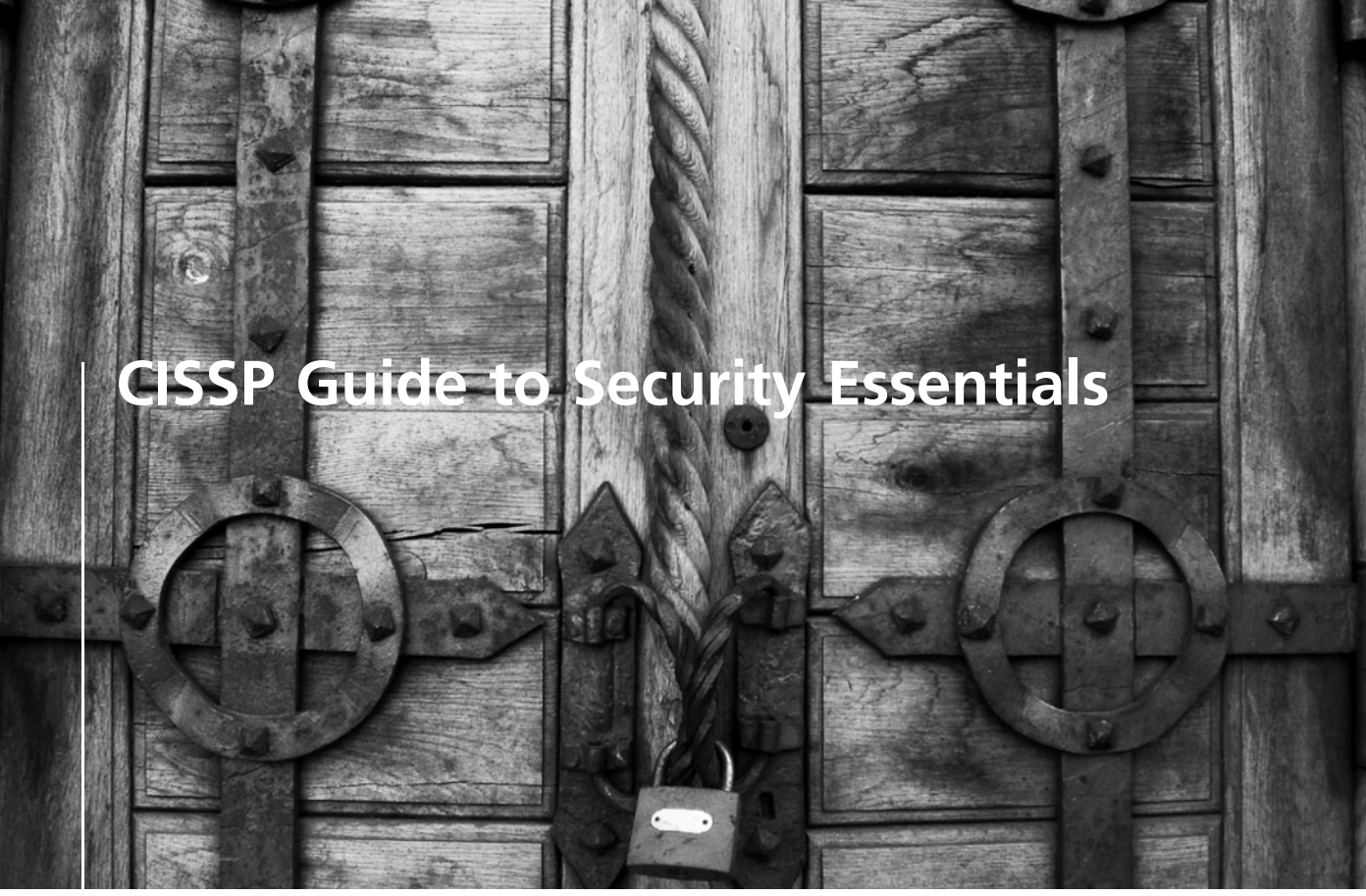
CISSP GUIDE TO SECURITY ESSENTIALS

PETER GREGORY

PREPARING TOMORROW'S INFORMATION SECURITY PROFESSIONALS

CISSP Guide to Security Essentials



CISSP Guide to Security Essentials

Peter Gregory

COURSE TECHNOLOGY
CENGAGE Learning

Australia • Brazil • Japan • Korea • Mexico • Singapore • Spain • United Kingdom • United States

COURSE TECHNOLOGY
CENGAGE Learning™

CISSP Guide to Security Essentials, Peter Gregory

Vice President, Career and Professional Editorial: Dave Garza

Executive Editor: Stephen Helba

Managing Editor: Marah Bellegarde

Senior Product Manager: Michelle Ruelos Cannistraci

Editorial Assistant: Sarah Pickering

Vice President, Career and Professional Marketing: Jennifer McAvey

Marketing Director: Deborah S. Yarnell

Senior Marketing Manager: Erin Coffin

Marketing Coordinator: Shanna Gibbs

Production Director: Carolyn Miller

Production Manager: Andrew Crouth

Content Project Manager: Andrea Majot

Art Director: Jack Pendleton

Cover photo: iStock.com

Production Technology Analyst: Tom Stover

Manufacturing Coordinator: Denise Powers

Compositor: PrePress PMG

© 2010 Course Technology, Cengage Learning

ALL RIGHTS RESERVED. No part of this work covered by the copyright herein may be reproduced, transmitted, stored or used in any form or by any means graphic, electronic, or mechanical, including but not limited to photocopying, recording, scanning, digitizing, taping, Web distribution, information networks, or information storage and retrieval systems, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the publisher.

For product information and technology assistance, contact us at
Cengage Learning Customer & Sales Support, 1-800-354-9706

For permission to use material from this text or product, submit all requests online at **cengage.com/permissions**
Further permissions questions can be emailed to **permissionrequest@cengage.com**

Library of Congress Control Number: 2009925212

ISBN-13: 978-1-435-42819-5

ISBN-10: 1-435-42819-6

Course Technology
20 Channel Center Street
Boston, MA 02210
USA

Cengage Learning is a leading provider of customized learning solutions with office locations around the globe, including Singapore, the United Kingdom, Australia, Mexico, Brazil, and Japan. Locate your local office at: **international.cengage.com/region**

Cengage Learning products are represented in Canada by Nelson Education, Ltd.

For your lifelong learning solutions, visit **course.cengage.com**

Visit our corporate website at **www.cengage.com**

Notice to the Reader

Some of the product names and company names used in this book have been used for identification purposes only and may be trademarks or registered trademarks of their respective manufacturers and sellers.

Microsoft and the Office logo are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Course Technology, a part of Cengage Learning, is an independent entity from the Microsoft Corporation, and not affiliated with Microsoft in any manner.

Any fictional data related to persons or companies or URLs used throughout this book is intended for instructional purposes only. At the time this book was printed, any such data was fictional and not belonging to any real persons or companies.

Course Technology, the Course Technology logo, and the Shelly Cashman Series® are registered trademarks used under license.

Adobe, the Adobe logos, Authorware, ColdFusion, Director, Dreamweaver, Fireworks, FreeHand, JRun, Flash, and Shockwave are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. All other names used herein are for identification purposes only and are trademarks of their respective owners.

Course Technology, a part of Cengage Learning, reserves the right to revise this publication and make changes from time to time in its content without notice.

The programs in this book are for instructional purposes only. They have been tested with care, but are not guaranteed for any particular intent beyond educational purposes. The author and the publisher do not offer any warranties or representations, nor do they accept any liabilities with respect to the programs.

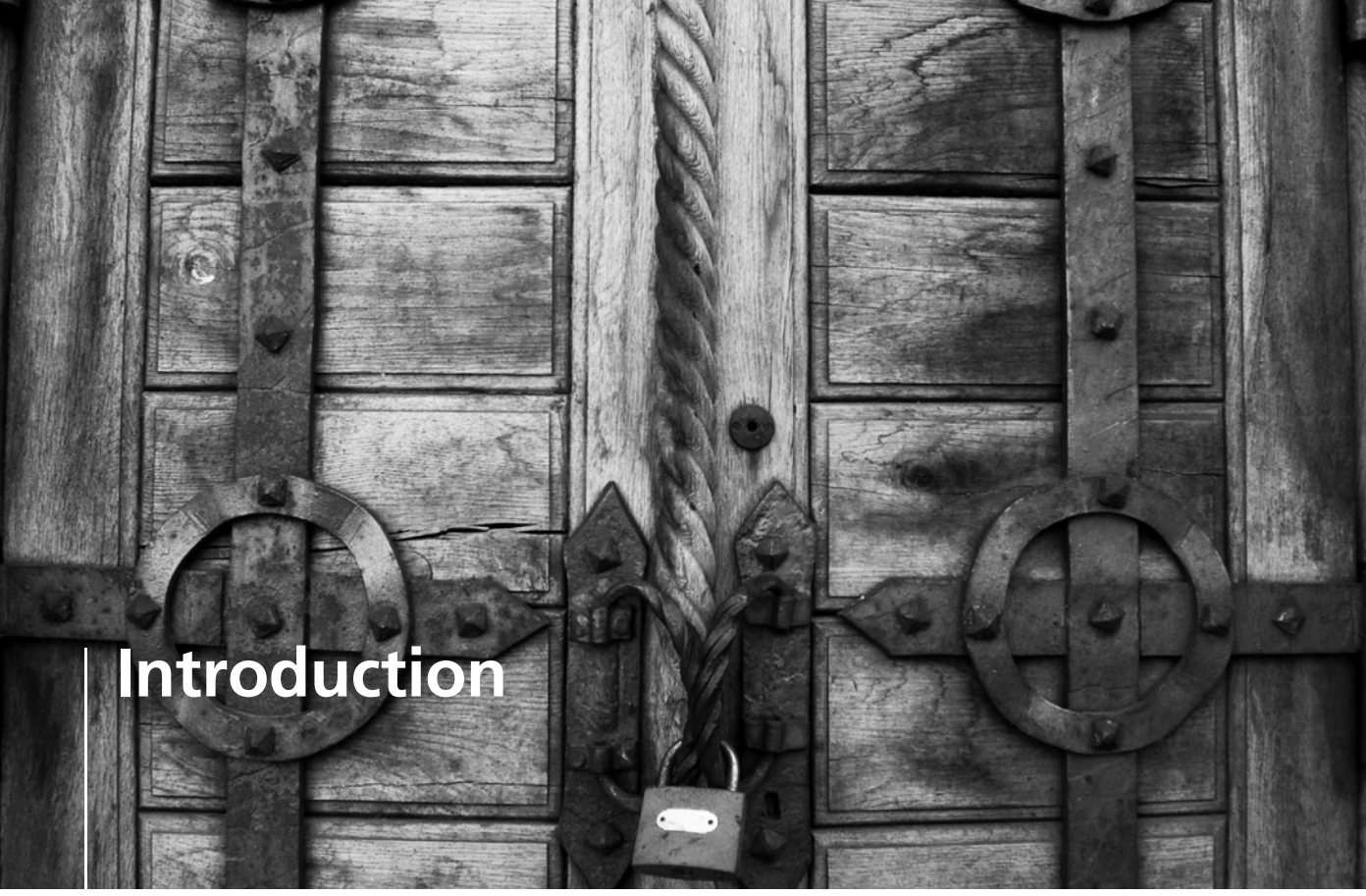
Printed in the United States of America
1 2 3 4 5 6 7 12 11 10 09

Brief Table of Contents

Table of Contents

CHAPTER 3

CHAPTER 4



Introduction

"If the Internet were a city street, I would not travel it in daylight," laments a chief information security officer for a prestigious university.

The Internet is critical infrastructure at the world's commerce. Cybercrime is escalating; once the domain of hackers and script kiddies, cyber-gangs and organized criminal organizations have discovered the business opportunities for extortion, embezzlement, and fraud that now surpasses income from illegal drug trafficking. Criminals are going for the gold, the information held in information systems that are often easily accessed anonymously from the Internet.

The information security industry is barely able to keep up. Cybercriminals and hackers always seem to be one step ahead, and new threats and vulnerabilities crop up at a rate that often exceeds our ability to continue protecting our most vital information and systems. Like other sectors in IT, security planners, analysts, engineers, and operators are expected to do more with less. Cybercriminals have never had it so good.

There are not enough good security professionals to go around. As a profession, information security in all its forms is relatively new. Fifty years ago there were perhaps a dozen information security professionals, and their jobs consisted primarily of making sure the doors were locked and that keys were issued only to personnel who had an established need for access. Today, whole sectors of commerce are doing virtually all of their business online, and other critical infrastructures such as public utilities are controlled online via the Internet. It's hard to find something that's not online these days. The rate of growth in the information security profession is falling way behind the rate of growth of critical information and infrastructures going online. This is making it all the more critical for today's and tomorrow's information security professionals to have a good understanding

of the vast array of principles, practices, technologies, and tactics that are required to protect an organization's assets.

The CISSP (Certified Information Systems Security Professional) is easily the most recognized security certification in the business. CISSP is also one of the most difficult certifications to earn, because it requires knowledge in almost every nook and cranny of information technology and physical security. The CISSP is a jack-of-all-trades certification that, like that of a general practitioner physician, makes us ready for any threat that could come along.

The required body of knowledge for the CISSP certification is published and updated regularly. This book covers all of the material in the published body of knowledge, with each chapter clearly mapping to each of the ten categories within that body of knowledge.

With the demand for security professionals at an all-time high, whether you are a security professional in need of a reference, an IT professional with your sights on the CISSP certification, or a course instructor, *CISSP Guide to Security Essentials* has arrived just in time.

Intended Audience

This book is written for students and professionals who want to expand their knowledge of computer, network, and business security. It is not necessary that the reader specifically target CISSP certification; while this book is designed to support that objective, the student or professional who desires to learn more about security, but who does not aspire to earn the CISSP certification at this time, will benefit from this book as equally as a CISSP candidate.

CISSP Guide to Security Essentials is also ideal for someone in a self-study program. The end of each chapter has not only study questions, but also Hands-On Projects and Case Projects that you can do on your own with a computer running Windows, MacOS, or Linux.

The structure of this book is designed to correspond with the ten domains of knowledge for the CISSP certification, called the Common Body of Knowledge (CBK). While this alignment will be helpful for the CISSP candidate who wants to align her study with the CBK, this is not a detriment to other readers. This is because the CBK domains align nicely with professional practices such as access control, cryptography, physical security, and other sensibly organized categories.

This book's pedagogical features will help all readers who wish to broaden their skills and experience in computer and business security. Each chapter contains several Hands-On Projects that guide the reader through several key security activities, many of which are truly hands-on with computers and networks. Each chapter also contains Case Projects that take the reader into more advanced topics to help them apply the concepts in the chapter.

Chapter Descriptions

Here is a summary of the topics covered in each chapter of this book:

Chapter 1, "Information Security and Risk Management," begins with the fundamentals of information and business security—security and risk management—by explaining how an organization's security program needs to support the organization's goals and objectives. The

chapter continues with risk management, security management and strategies, personnel security, and professional ethics.

Chapter 2, "Access Controls," discusses access control principles and architectures, and continues with descriptions of the types of attacks that are carried out against access control systems. The chapter also discusses how an organization can test its access controls to make sure they are secure.

Chapter 3, "Application Security," begins with a discussion of the types of application software, application models, and technologies. The chapter continues by exploring threats to software applications and countermeasures to deal with them. It explores how to secure the software development life cycle—the process used for the creation and maintenance of application software. The chapter discusses application environment and security controls, and concludes with a discussion of the security of databases and data warehouses.

Chapter 4, "Business Continuity and Disaster Recovery Planning," explores the concepts and practices in business continuity planning and disaster recovery planning. The chapter provides a lengthy discourse on a practical approach to running a BCP / DRP project. Next, the chapter describes several approaches to testing BCP and DRP plans, and how such plans are maintained over time.

Chapter 5, "Cryptography," begins with an introduction to the science of cryptography, the practice of hiding data in plain sight. The chapter continues with a discussion of the applications and uses of cryptography, and on the methodologies used by cryptographic algorithms. The chapter also includes a discussion of cryptography and key management.

Chapter 6, "Legal, Regulations, Compliance, and Investigations," starts with a discussion of the different types of computer crime and the various ways that computers are involved in criminal activity. The next discussion focuses on the types and categories of laws in the U.S. and other countries, with a particular focus on computer-related laws. The chapter continues with a discussion of security incident response, investigations, and computer forensics, and concludes with a discussion of ethical issues in the workplace.

Chapter 7, "Operations Security," introduces and discusses the broad topic of putting security controls, concepts, and technologies into operation in an organization. The specific topics discussed includes records management, backup, anti-virus, remote access, administrative access, resource protection, incident management, vulnerability management, change management, and configuration management. The chapter discusses resource protection, high-availability application architectures, and attacks and countermeasures for IT operations.

Chapter 8, "Physical and Environmental Security," begins with a discussion of site access controls for the physical protection of worksites that may include IT systems. The chapter discusses secure siting, which is the process of identifying risk factors associated with the location and features of an office building. The chapter provides an overview of fire prevention and suppression, theft prevention, and building environmental controls including electric power and heating, ventilation, and air conditioning.

Chapter 9, "Security Architecture and Design," discusses security models that have been developed and are still in use from the 1970s to the present. The chapter continues with a discussion of information system evaluation models including the Common Criteria.

The chapter discusses computer hardware architecture and computer software, including operating systems, tools, utilities, and applications. Security threats and countermeasures in the context of computer software are also explored.

Chapter 10, "Telecommunications and Network Security," is a broad exploration of telecommunications and network technologies. The chapter examines the TCP/IP and OSI protocol models, and continues with a dissection of the TCP/IP protocol suite. The chapter addresses TCP/IP network architecture, protocols, addressing, devices, routing, authentication, access control, tunneling, and services. The chapter concludes with a discussion of network-based threats and countermeasures.

Appendix A, "The Ten Domains of CISSP Security," provides a background on the CISSP certification, and then describes the ten domains in the CISSP Common Body of Knowledge.

Appendix B, "The (ISC)^2 Code of Ethics," contains the full text of the (ISC)^2 Code of Ethics, which every CISSP candidate is required to support and uphold. The Code of Ethics is a set of enduring principles to guide the behavior of every security professional.

Glossary, lists common information security and risk management terms that are found in this book.

Features

To aid you in fully understanding computer and business security, this book includes many features designed to enhance your learning experience.

- **Maps to the CISSP Common Body of Knowledge (CBK).** The material in this text covers all of the CISSP exam objectives. Aside from Information Security and Risk Management being addressed first in the book, the sequence of the chapters follows the ten CISSP domains.
- **Common Body of Knowledge objectives included.** Each chapter begins with the precise language from the (ISC)^2 Common Body of Knowledge for the respective topic in the CISSP certification. This helps to remind the reader of the CISSP certification requirements for that particular topic.
- **Chapter Objectives.** Each chapter begins with a detailed list of the concepts to be mastered within that chapter. This list provides you with both a quick reference to the chapter's contents and a useful study aid.
- **Illustrations and Tables.** Numerous illustrations of security vulnerabilities, attacks, and defenses help you visualize security elements, theories, and concepts. In addition, the many tables provide details and comparisons of practical and theoretical information.
- **Chapter Summaries.** Each chapter's text is followed by a summary of the concepts introduced in that chapter. These summaries provide a helpful way to review the ideas covered in each chapter.
- **Key Terms.** All of the terms in each chapter that were introduced with bold text are gathered in a Key Terms list with definitions at the end of the chapter, providing additional review and highlighting key concepts.
- **Review Questions.** The end-of-chapter assessment begins with a set of review questions that reinforce the ideas introduced in each chapter. These questions help you

evaluate and apply the material you have learned. Answering these questions will ensure that you have mastered the important concepts and provide valuable practice for taking the CISSP exam.

- **Hands-On Projects.** Although it is important to understand the theory behind network security, nothing can improve upon real-world experience. To this end, each chapter provides several Hands-On Projects aimed at providing you with practical security software and hardware implementation experience. These projects can be completed on Windows XP or Vista (and, in some cases, Windows 2000, MacOS, Linux). Some will use software downloaded from the Internet.
- **Case Projects.** Located at the end of each chapter are several Case Projects. In these extensive exercises, you implement the skills and knowledge gained in the chapter through real analysis, design, and implementation scenarios.
- **(ISC)^2 Code of Ethics.** The entire (ISC)^2 Code of Ethics is included at the end of this book. It is this author's opinion that the security professional's effectiveness in the workplace is a direct result of one's professional ethics and conduct.

Text and Graphic Conventions

Wherever appropriate, additional information and exercises have been added to this book to help you better understand the topic at hand. Icons throughout the text alert you to additional materials. The icons used in this textbook are described below.

The Note icon draws your attention to additional helpful material related to the subject being described.

Hands-On Projects in this book are preceded by the Hands-On icon and descriptions of the exercises that follow.

Case Project icons mark Case Projects, which are scenario-based assignments. In these extensive case examples, you are asked to implement independently what you have learned.

Companion CD-ROM

The accompanying CD includes 250 sample exam questions.

Information Security Community Site

The Information Security Community Site was created for students and instructors to find out about the latest in information security news and technology.

Visit www.community.cengage.com/security to:

- Learn what's new in information security through live news feeds, videos, and podcasts.
- Connect with your peers and security experts through blogs and forums.
- Download student and instructor resources, such as additional labs, instructional videos, and instructor materials.
- Browse our online catalog.

Instructor's Materials

The following additional materials are available when this book is used in a classroom setting. All of the supplements available with this book are provided to the instructor on a single CD-ROM (ISBN: 143542820X). You can also retrieve these supplemental materials from the Course Technology Web site, *www.course.com*, by going to the page for this book, and clicking the "Download Instructor Files & Teaching Tools" link.

Electronic Instructor's Manual—The Instructor's Manual that accompanies this textbook provides additional instructional material to assist in class preparation, including suggestions for lecture topics, suggested lab activities, tips on setting up a lab for the hands-on assignments, and solutions to all end-of-chapter materials.

ExamView Test Bank—This Windows-based testing software helps instructors design and administer tests and pretests. In addition to generating tests that can be printed and administered, this full-featured program has an online testing component that allows students to take tests at the computer and have their exams automatically graded.

PowerPoint Presentations—This book comes with a set of Microsoft PowerPoint slides for each chapter. These slides are meant to be used as a teaching aid for classroom presentations, to be made available to students on the network for chapter review, or to be printed for classroom distribution. Instructors are also at liberty to add their own slides to cover additional topics.

How to Earn and Maintain a CISSP Certification

In order to become CISSP certified, you must:

1. Select a test location and date from the schedule on the $(ISC)^2$ website, www.isc2.org.
2. Register for an examination by completing and returning an application and paying the registration fee.
3. Take and pass the CISSP certification exam.
4. Provide evidence of the required five years of work experience.
5. Submit a completed endorsement form.
6. Have a criminal record that is free of disqualifying criminal convictions.
7. Be in good standing in the information security industry.

Note that some candidates will be audited, in order to confirm the facts of their application, before the CISSP certification is issued.

You will also be required to sign an agreement of support of the (ISC)^2 code of ethics. Every CISSP is required to support the code of ethics; violations may result in the loss of your certification.

Once you earn your CISSP certification, you are required to earn CPE credits in order to retain your certification. You are required to complete 120 CPE credits every three years, with no less than 20 CPE credits each year of your certification cycle. (ISC)^2 recognizes that security practices and technologies constantly change, which is why staying current is a requirement for keeping your CISSP. You will also be required to pay an annual fee to maintain your certification.

You are encouraged to volunteer your time and talent in the CISSP community. Opportunities include proctoring CISSP exams, writing CISSP exam questions, public speaking, at (ISC)^2 and other events, teaching, mentoring new certification candidates, writing articles, and more. More information can be found on the (ISC)^2 website at www.isc2.org.

For more information about the CISSP certification, visit the (ISC)^2 website at www.isc2.org. A document called the *CISSP Candidate Bulletin of Information* is a helpful document that explains the entire certification process. You will be required to register on the (ISC)^2 website in order to receive a copy of the document. You may also contact (ISC)^2 by phone at (703) 891-6781.

Photo and Image Credits

Figure 2-4 Courtesy of xkcd.com

Figure 2-6 Image copyright, 2009. Used under license with istockphoto.com

Figure 3-5 Redrawn with permission from S. Staniford, V. Paxon, and N. Weaver, "How to own the Internet In Your Spare Time, "Proc. USENIX Security Symposium 2002.

Figure 4-1 Courtesy of US Geological Survey

Figure 6-1 Copyright 2002 Carnegie Mellon University with special permission from the Software Engineering Institute

Figure 8-3 Courtesy of Rebecca Steele

Figure 8-4 Courtesy of Rebecca Steele

Figure 8-5 Image copyright, 2009. Used under license from istock.com

Figure 8-6 Courtesy of U.S. Army Research Laboratory

Figure 8-8 Image copyright, 2009. Used under license from istock.com

Figure 8-9 Image copyright, 2009. Used under license from istock.com

Figure 8-12 Courtesy of Delta Scientific

Figure 9-2 Courtesy of Rebecca Steele

Figure 9-3 Courtesy of Rebecca Steele

Figure 9-4 Courtesy of Rebecca Steele

Figure 10-2 Courtesy of Rebecca Steele

Figure 10-3 Courtesy of Rebecca Steele

The illustration in Figure 6-1 is reproduced from "Cyberterrorism" by Tim Shimeall, www.cert.org/archive/ppt/cyberterror.ppt, Copyright 2002 Carnegie Mellon University with special permission from the Software Engineering Institute.

ANY CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL CONTAINED HEREIN IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

The Software Engineering Institute and Carnegie Mellon University do not directly or indirectly endorse this publication.

Acknowledgments

First, I want to thank my wife and best friend, Rebekah. Without her patience and support, writing this book could not have been possible.

It takes a team of professionals to produce a teaching book. Those with whom I worked directly are mentioned here.

Several individuals at Cengage Learning have also been instrumental in the production of this book. First, Executive Editor Steve Helba established the scope and direction for this book. Senior Product Manager Michelle Ruelos Cannistraci managed the author through the entire writing, reviewing, and production process. Next, Content Project Manager Andrea Majot kept track of the details as the author sent in chapter files, images, and other materials. Associate Project Manager Marie Desrosiers assisted in keeping people and content organized. Certainly there were others: editors, compositors, graphic artists, who were also involved in this book project. Heartfelt thanks to all of you.

Special recognition goes to the book's technical reviewers. These are industry and academic subject matter experts who carefully read through the manuscript to make sure that it is both technically accurate and also well organized, with accurate and understandable descriptions and explanations. This book's technical reviewers are:

- Dr. Barbara Endicott-Popovsky, the Director for the Center of Information Assurance and Cybersecurity at the University of Washington, designated by the NSA as a Center for Academic Excellence in Information Assurance Education.
- Michael Simon, a leading expert in computer security, information assurance, and security policy development. Mike and I have also written two books together.
- Jim Drennan at Pensacola Junior College Center for Information and Engineering Technology, who provided valuable and thoughtful feedback in several important areas.

- Faisal Abdullah at Lewis University also provided valuable information that prompted me to produce additional content.

Special thanks to Kirk Bailey for his keen insight over the years and for fighting the good fight.

I am honored to have had the opportunity work with this outstanding and highly professional group of individuals at Cengage Learning, together with the reviewers and others of you who never compromised on the pursuit of excellence.

About the Author

Peter H. Gregory, CISA, CISSP, DRCE, is the author of twenty books on information security and technology, including *IT Disaster Recovery Planning For Dummies, Biometrics For Dummies, Securing the Vista Environment,* and *Solaris Security*. He has spoken at numerous security conferences, including RSA, SecureWorld Expo, InfraGard, and the West Coast Security Forum.

Peter is the security and risk manager at a financial management services firm in Seattle. He is the lead instructor and advisory board member for the University of Washington's certificate program in information security, and an advisory board member and guest lecturer for the University of Washington's certificate program in information assurance. He is on the board of directors for the Washington State chapter of InfraGard, a graduate of the FBI Citizens Academy, and is active in the FBI Citizens Academy Alumni Association.

In his free time he enjoys the outdoors in Washington State with his wife and family.

This page intentionally left blank

Lab Requirements

To the User

This book contains numerous hand-on lab exercises, many of which require a personal computer and, occasionally, specialized software.

Information and business security is not just about the technology; it's also about people, processes, and the physical facility in which all reside. For this reason, some of the labs do not involve the exploration of some aspect of computers or networks, but instead are concerned with business requirements, analysis, or critical evaluation of information. But even in these non-technical labs, a computer with word processing, spreadsheet, or illustration software will be useful for collecting and presenting information.

Hardware and Software Requirements

These are all of the hardware and software requirements needed to perform the end-of-chapter Hands-On Projects:

- Windows XP Professional (in some projects, Windows 2000, MacOS, or a current Linux distribution are sufficient)
- An Internet connection and Web browser (e.g., Firefox or Internet Explorer)
- Anti-virus software

Specialized Requirements

The need for specialized hardware or software is kept to a minimum. However, the following chapters do require specialized hardware or software:

- Chapter 2: Zone Labs' Zone Alarm firewall
- Chapter 3: Secunia Personal Software Inspector (PSI), IBM/Watchfire AppScan
- Chapter 10: Notebook or desktop computer with Wi-Fi NIC compatible with the Netstumbler tool

Free Downloadable Software is Required in the Following Chapters

Chapter 2:

- Zone Labs' Zone Alarm firewall
- WinZip version 9 or newer

Chapter 3:

- Secunia Personal Software Inspector (PSI)
- Microsoft Threat Analysis & Modeling tool

Chapter 5:

- TrueCrypt
- GnuPG
- Gifshuffle
- WinZip version 9 or newer

Chapter 9:

- Microsoft Process Explorer
- Cyberkit

Chapter 10:

- Wireshark
- SuperScan
- Netstumbler

chapter 1

Information Security and Risk Management

Topics in this Chapter:

- How Security Supports Organizational Mission, Goals and Objectives
- Risk Management
- Security Management
- Personnel Security
- Professional Ethics

The *International Information Systems Security Certification Consortium* (ISC)^2 *Common Body of Knowledge* (CBK) defines the key areas of knowledge for Information Security and Risk Management in this way:

Information Security and Risk Management entails the identification of an organization's information assets and the development, documentation, and implementation of policies, standards, procedures and guidelines that ensure confidentiality, integrity, and availability. Management tools such as data classification, risk assessment, and risk analysis are used to identify the threats, classify assets, and to rate their vulnerabilities so that effective security controls can be implemented.

Risk management is the identification, measurement, control, and minimization of loss associated with uncertain events or risks. It includes overall security review, risk analysis; selection and evaluation of safeguards, cost benefit analysis, management decision, safeguard implementation, and effectiveness review.

The candidate will be expected to understand the planning, organization, and roles of individuals in identifying and securing an organization's information assets; the development and use of policies stating management's views and position on particular topics and the use of guidelines, standards, and procedures to support the policies; security awareness training to make employees aware of the importance of information security, its significance, and the specific security-related requirements relative to their position; the importance of confidentiality, proprietary and private information; employment agreements; employee hiring and termination practices; and risk management practices and tools to identify, rate, and reduce the risk to specific resources.

Key areas of knowledge:

- *Understand and document the goals, mission, and objectives of the organization*
- *Establish governance*
- *Understand concepts of availability, integrity, and confidentiality*
- *Apply the following security concepts in planning: defense in depth, avoid single paths of failure*
- *Develop and implement security policy*
- *Define the organization's security roles and responsibilities*
- *Secure outsourcing*
- *Develop and maintain internal service level agreements*
- *Integrate and support identity management*
- *Understand and apply risk management concepts*
- *Evaluate personnel security*
- *Develop and conduct security education, training, and awareness*
- *Understand data classification concepts*
- *Evaluate information system security strategies*

- *Support certification and accreditation efforts*
- *Design, conduct, and evaluate security assessments*
- *Report security issues to management*
- *Understand professional ethics*

Even though this domain is positioned as number 5 in the Certified Information Systems Security Professional (CISSP) common body of knowledge, it is placed first in this book because all security activities should take place as a result of security and risk management.

Organizational Mission, Objectives, and Goals

In order to be able to protect an organization's **assets**, it is first necessary to understand several basic characteristics of the organization, including its goals, mission, and objectives. All are statements that define what the organization desires to achieve and how it will proceed to achieve them. These three terms are described in more detail here.

Mission

The mission of an organization is a statement of its ongoing purpose and reason for existence. An organization usually publishes its mission statement, so that its employees, customers, suppliers, and partners are aware of the organization's stated purpose. Some example mission statements:

> *"Promote professionalism among information system security practitioners through the provisioning of professional certification and training."*—(ISC)²

> *"Empower and engage people around the world to collect and develop educational content under a free license or in the public domain, and to disseminate it effectively and globally."*—Wikimedia Foundation

> *"Help civilize the electronic frontier; to make it truly useful and beneficial not just to a technical elite, but to everyone; and to do this in a way which is in keeping with our society's highest traditions of the free and open flow of information and communication."*—Electronic Frontier Foundation

An organization's security professionals need to be aware of their organization's mission, because it will, in part, influence how we will approach the need to protect the organization's assets.

Objectives

The objectives of an organization are statements of activities or end-states that the organization wishes to achieve. Objectives support the organization's mission and describe how the organization will fulfill its mission.

Objectives are observable and measurable. People can determine whether the organization met its objectives or not. Also, objectives do not necessarily specify how they will be completed, or by whom.

Sample organization objectives include:

"Obtain ISO 27001 certification by the end of third quarter."

"Reduce development costs by twenty percent in the next fiscal year."

"Complete the integration of CRM and ERP systems by the end of November."

Security personnel need to know the organization's objectives and be involved in their fruition, so that the organization can achieve its objectives with the lowest reasonable level of risk.

Goals

While objectives describe desired end-states for an organization, goals specify specific accomplishments that will enable the organization to meet its objectives.

Security Support of Mission, Objectives, and Goals

Security professionals in an organization ought to be concerned with the reduction of risk through the proper activities and controls that protect assets and activities. We need to be keenly aware of our organizations' mission, objectives, and goals, so that we can become involved in the key activities that the organization is undertaking.

Involvement and influence in an organization's key activities requires the support of senior management. This support comes in the form of priorities and resources that permit security professionals to be closely involved with key activities. This is discussed in greater detail later in this chapter in the section, "Security Management."

Risk Management

Risk management is the process of determining the maximum acceptable level of overall risk to and from a proposed activity, then using risk assessment techniques to determine the initial level of risk and, if this is excessive, developing a strategy to ameliorate appropriate individual risks until the overall level of risk is reduced to an acceptable level. In the vernacular this means, find the level of risk (associated with a given activity or asset) and do something about it if needed.

Two basic steps are performed in risk management: risk assessment and risk treatment. Risk assessment is used to identify risks, and risk treatment is used to manage the identified risks. These are discussed in the remainder of this section.

NIST 800-30, *Risk Management Guide for Information Technology Systems*, is an outstanding, high quality standard for risk management. This document was developed by the U.S. National Institute of Standards and Technology, which develops all of the security standards for the U.S. federal government.

Risk Assessment

Risk assessments are activities that are carried out to discover, analyze, and describe risks. Risk assessments may be qualitative, quantitative, or a combination of these.

Internal audit is related to risk assessment; internal audit is discussed in a separate section in this chapter.

Qualitative Risk Assessment

A qualitative risk assessment occurs with a pre-defined scope of assets or activities. Assets can, for example, consist of software applications, information systems, business equipment, or buildings. Activities may consist of activities carried out by an individual, group, or department.

A qualitative risk assessment will typically identify a number of characteristics about an asset or activity, including:

- **Vulnerabilities**. These are weaknesses in design, configuration, documentation, procedure, or implementation.
- **Threats**. These are potential activities that would, if they occurred, exploit specific vulnerabilities.
- **Threat probability**. An expression of the likelihood that a specific threat will be carried out, usually expressed in a Low-Medium-High or simple numeric (1–5 or 1–10) scale.
- **Countermeasures**. These are actual or proposed measures that reduce the risk associated with vulnerabilities or threats.

Here is an example. A security manager is performing a qualitative risk assessment on the assets in an IT environment. For each asset, the manager builds a chart that lists each threat, along with the probability of realization. The chart might resemble the list in Table 1.1.

This is an oversimplified example, but sometimes qualitative risk analysis won't be much more complicated than this—although a real risk analysis should list many more threats and countermeasures.

Threat	Impact	Probability	Countermeasure	Probability
Flooding	H	L	Water alarms	L
Theft	H	L	Key card, video surveillance, guards	L
Earthquake damage	M	M	Lateral rack bracing; attach all assets to racks	L
Logical intrusion	H	M	Network-based intrusion detection system; host-based intrusion detection system	L

Table 1-1 Risk assessment chart

Quantitative Risk Assessment

A quantitative risk assessment can be thought of as an extension of a qualitative risk assessment. A quantitative risk assessment will include the elements of a qualitative risk assessment but will include additional items, including:

- **Asset value**. Usually this is a dollar figure that may represent the replacement cost of an asset, but could also represent income derived through the use of the asset.

- **Exposure factor (EF)**. The proportion of an asset's value that is likely to be lost through a particular threat, usually expressed as a percentage. Another way to think about exposure factor is to consider the *impact* of a specific threat on an asset.
- **Single loss expectancy (SLE)**. This is the cost of a single loss through the realization of a particular threat. This is a result of the calculation:

$$\text{SLE} = \text{asset value (\$)} \times \text{exposure factor (\%)}$$

- **Annualized rate of occurrence (ARO)**. This is the probability that a loss will occur in a year's time. This is usually expressed as a percentage, which can be greater than 100% if it is believed that a loss can occur more than once per year.
- **Annual loss expectancy (ALE)**. This is the yearly estimate of loss of an asset, calculated as follows:

$$\text{ALE} = \text{ARO} \times \text{SLE}$$

Let's look at an example: an organization asset, an executive's laptop computer, that is worth $4,000. The asset value is $4,000.

Now we will calculate the exposure factor (EF), which is the proportion of the laptop's value that is lost through a particular threat. The threat of theft will, of course, result in the entire laptop's value to be lost. For theft, EF = 100%. For sake of example, let's add another threat, that of damage, if the executive drops the laptop and breaks the screen. For that threat, the EF = 50% (presuming a $2,000 repair bill to replace the LCD screen).

For theft, the single loss expectancy (SLE) is $4,000 × 100% = $4,000. For damage, the SLE is $4,000 × 50% = $2,000.

Now we need to calculate how often either of these scenarios might occur in a single year. For theft, let us presume that there is a 10% probability that this executive's laptop will be stolen (he's a popular individual). Thus, the ARO = 10%. This particular executive is really clumsy and drops his laptop computer a lot, so the ARO for that threat is 25%.

The annual loss expectancy (ALE) for theft is 10% × $4,000 or $400.

The ALE for damage is 25% × $2,000 = $500.

This all means that the organization will lose $900 ($400 for theft and $500 for damage) each year in support of the executive's laptop computer. Knowing this will help management make more intelligent spending decisions for any protective measures that they feel will reduce the probability or impact of these and other threats. This is discussed in the next section on countermeasures.

Quantifying Countermeasures

Annual loss expectancy (ALE) is the cost that the organization is likely to bear through the loss of the asset. Because ALE is expressed in dollars (or other local currency), the organization can now make decisions regarding specific investments in countermeasures that are designed to reduce the risk. The risk analysis can be extended to include the impact of countermeasures on the overall risk equation:

- **Costs of countermeasures**. Each countermeasure has a specific cost associated with it. This may be the cost of equipment, software, or labor costs.

- **Changes in exposure factor**. A specific countermeasure may have an impact on a specific threat. For example, the use of an FM-200-based fire extinguishment system will mean that a fire in a business location will cause less damage than a sprinkler-based extinguishment system.
- **Changes in single loss expectancy**. Specific countermeasures may influence the probability that a loss will occur. For instance, the introduction of an anti-virus network appliance will reduce the frequency of malware attacks.

Geographic Considerations Organizations can take quantitative risk analysis a step or two further by calculating SLE, ALE, and ARO values in specific geographic locations. This is useful in organizations with similar assets located in different locations where the probability of loss or the replacement cost of these assets varies enough to matter.

Specific Risk Assessment Methodologies The risk assessment steps described in this section are intentionally simplistic, with the intention of illustrating the concepts of identifying the value of assets and by using formulas to arrive at a quantitative figure that represents the probable loss of assets in a year's time. For some organizations, this simple approach may be sufficient. On the other hand, there are several formal approaches to risk assessment that may be suitable for larger or more complex efforts. Among these approaches are:

- **OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)**. Developed by Carnegie Mellon University's Software Engineering Institute (SEI), OCTAVE is an approach where analysts identify assets and their criticality, identify vulnerabilities and threats, evaluate risks, and create a protection strategy to reduce risk.
- **FRAP (Facilitated Risk Analysis Process)**. This is a qualitative risk analysis methodology that can be used to pre-screen a subject of analysis as a means to determine whether a full blown quantitative risk analysis is needed.
- **Spanning Tree Analysis**. This can be thought of as a visual method for identifying categories of risks, as well as specific risks, using the metaphor for a tree and its branches. This approach would be similar to a *Mind Map* for identifying categories and specific threats and/or vulnerabilities.
- **NIST 800-30, Risk Management Guide for Information Technology Systems**. This document describes a formal approach to risk assessment that includes threat and **vulnerability** identification, control analysis, impact analysis, and a matrix depiction of risk determination and control recommendations.

Risk Treatment

When a qualitative or quantitative risk assessment has been performed, an organization's management can begin the process of determining what steps, if any, need to be taken to manage the risks identified in the risk assessment. The four general approaches to risk treatment are:

- Risk acceptance
- Risk avoidance
- Risk reduction

- Risk transfer

It is important to remember that the objective of risk treatment is not to eliminate risk—often risk cannot be eliminated, but only managed.

Risk Avoidance Generally the most extreme form of risk treatment, in **risk avoidance** the associated activity that introduces the risk is discontinued. For instance, an organization performs a risk analysis of an Internet-based shopping cart application, and then decides to abandon the use of the application altogether. This is risk avoidance.

Risk Reduction **Risk reduction**—also known as **risk mitigation**—involves the use of countermeasures to reduce the risks initially identified in the risk analysis. Examples of risk reduction in information systems include firewalls, intrusion detection systems, and DMZ networks.

Risk Acceptance In a typical risk assessment, there will be many identified risks, typically ranked as high, medium, and low risk. Management may choose to forego mitigation of all of the risks ranked low, in other words leaving things as they are and accepting the stated risks. This is known as **risk acceptance**.

Risk Transfer **Risk transfer** typically involves the use of insurance as a means for mitigating risk. For instance, a risk analysis on the use of laptop computers may identify theft as one risk. While the organization may mitigate the risk through the use of cable locks, it may transfer part of the risk to an insurance company. Note that risk transfer usually involves a cost (insurance premiums) that should be considered in a quantitative risk analysis.

Residual Risk In any particular risk situation, generally only some of the risk can be avoided, reduced, or transferred. There is always some remaining risk, called **residual risk**. Typically this risk must be accepted, unless management can enact another round of analysis and a fresh set of countermeasures to avoid, reduce, or transfer the risk. But even then, there will be some "leftover" risk, called *residual risk*.

Security Management Concepts

Several concepts and terms are used in the **security management** profession. When security professionals are discussing the measures needed to protect assets in the organization, the following terms are commonplace:

- Security controls
- CIA Triad
- Defense in depth
- Single points of failure
- Fail open, fail closed, fail soft
- Privacy

The ISO 27001 standard, "Information Technology—Security Techniques—Information Security Management Systems—Requirements," is an outstanding standard for information security management. Originally developed as British Standard 7799, the standard was adopted by the International Standards Organization (ISO) in 2000. ISO 27001 was later updated in 2005. ISO 27001 is a top-down process approach to security management that, when properly implemented, will result in continuous improvement in security management within an organization.

Security Controls

Security controls are the measures that are taken to enforce **security policy** and reduce risk. The types of controls used are detective, deterrent, preventive, corrective, recovery, and compensating. These controls are discussed in detail in Chapter 3, "Application Security."

The CIA Triad

The core principles of information security are *confidentiality*, *integrity*, and *availability*, often coined as **CIA**. All other concepts and activities in information security are based on these principles. The CIA Triad is depicted in Figure 1-1.

Confidentiality The principle of **confidentiality** asserts that information and functions can be accessed only by properly authorized parties.

Private information about citizens has resulted in the proliferation of information systems operated by both government and industry. Typically, a personal "profile" containing many items of basic information is established when an individual begins a relationship with an organization. This relationship is started when a person makes a purchase, registers to vote, renews a driver's license, pays taxes, or consults a physician. Even if the purpose or the duration of the relationship is brief, often the information will remain on the organization's information systems for an extended period of time, often for many years.

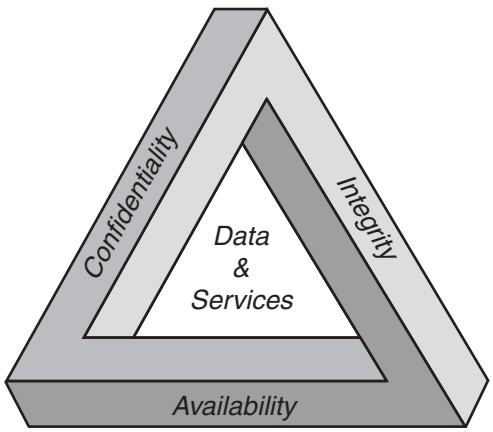


Figure 1-1 The CIA Triad

Source: Course Technology/Cengage Learning

Individuals expect that their confidential information will not be disclosed to unauthorized parties and that it will be properly protected. However, we have come to expect that some organizations will not handle information properly, resulting in an unauthorized disclosure that, in its worst case, could result in an attempted identity theft or financial fraud carried out against the persons whose information was compromised.

Integrity The principle of **integrity** asserts that information and functions can be added, altered, or removed only by authorized persons and means.

The general expectation of information systems is that information will be properly and accurately introduced into a system, and throughout its lifetime the information will remain accurate. While the principle of confidentiality states that only authorized parties will be able to view information, the principle of integrity assets that only authorized parties will be able to modify information. Integrity is achieved through role-based access control, which is the generic name for a mechanism that controls the actions performed by individuals. In the context of information stored in a database of tables consisting of tables, rows, and fields, the concept of integrity will govern which individuals are able to modify which tables, rows, and fields in a database.

In data security, the need for integrity encompasses software, systems, and the people who design, build, and operate them. Software must operate properly, particularly when a program is accessing and modifying data. Systems must be properly configured so that the data that resides on them is managed and updated correctly. The people who design, build, and operate software and systems must be properly trained on the technologies that they are using, and they must also adhere to a code of professional ethics that guides their behavior and decision-making.

Availability The principle of **availability** asserts that systems, functions, and data must be available on-demand according to any agreed-upon parameters regarding levels of service. In other words, systems should generally be available and running properly when they are supposed to be available.

Availability is multi-faceted and involves many separate safeguards and mechanisms to ensure that systems and data are available when needed. These safeguards range from firewalls and anti-virus software to resilient architectures to disaster recovery planning. *Availability* covers nearly all of the aspects of data security that directly or indirectly protect a system from harm.

Defense in Depth

The term **defense in depth** implies a *layered defense* consisting of two or more protective methods that protect some asset. Some of the characteristics of defense in depth are:

- **Heterogeneity**. A good defense in depth mechanism contains different types of protective mechanisms. For example, two layers of firewalls of different brands.
- **Entire protection**. Each layer of the defense fully protects an asset against the type of threat that the defense is designed to block. For example, anti-virus on an e-mail server and also on end-user workstations.

The classic example of a good defense in depth is the medieval castle's defenses that include a drawbridge, a moat, a moat monster, archers, soldiers to pour boiling oil, and so on. These defenses are all different from one another but are all designed to protect the castle (and its assets) from attack from outsiders.

The objective of a defense in depth is to reduce the probability that a threat can act upon an asset. This occurs in two ways:

- **Single vulnerability**. If one of the components of a defense in depth had an exploitable vulnerability, chances are that another layer in the defense will not have the same vulnerability.
- **Single malfunction**. If one of the components of a defense in depth malfunctions, chances are that another layer in the defense will not malfunction.
- **Fail open**. If one of the components in a defense in depth fails open, the other component(s) will continue to operate and protect the asset.

Single Points of Failure

A **single point of failure** is the characteristic of a component in a system if the failure of the component will result in the failure of the entire system.

Single points of failure are generally discussed only in a system that is designed for resilience and that contains redundant components. A single point of failure in such a system would be the portion of the system where redundancy does not exist.

For example, the firewall in Figure 1-2 would be a single point of failure. If the firewall fails, the system will be unreachable. The firewall is a single point whose failure will cause the failure of the entire system.

Fail Open, Fail Closed, Fail Soft

The concepts of *fail open*, *fail closed*, and *fail soft* are related to what happens to the protection in the event of a failure of a security control.

When a security control fails, generally one of two things happens: either the control blocks all access, or it permits all access. If the control fails and it blocks all access, it is said to **fail closed**. Another term for fail closed is **fail safe**.

If the control fails and permits all access, it **fails open**.

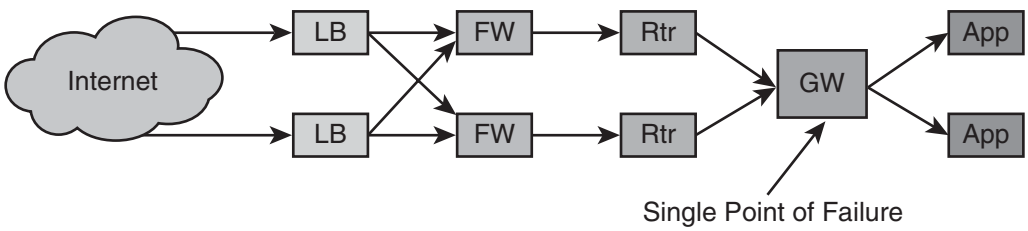


Figure 1-2 Single point of failure in an otherwise resilient environment

Source: Course Technology/Cengage Learning

A system can take action during an adverse situation such as a hardware failure. **Fail soft** is the process of shutting down non-essential components on a system, thereby freeing up resources so that critical components can continue operating.

Generally speaking it is more desirable for a control to fail closed than to fail open. This, however, is dependent upon the objective and design of the entire system.

An example of undesirable fail open is a doorway controlled by a key card access system that can be bypassed if the key card system fails. A desirable fail open would be the automatic opening of security doors to facilitate personnel exiting in case of fire.

Most security controls fail closed. For example, if a key card system fails, personnel cannot enter or move about the premises. If an application server is unable to access an LDAP authentication server, then no users can log on to the application.

Privacy

Merriam Webster dictionary defines **privacy** as "freedom from unauthorized intrusion." The practice of privacy in business refers to the protection of individuals' private information so that it is used only for intended and agreed-upon purposes and protected from unauthorized disclosure.

Personally Identifiable Information

Personally identifiable information (PII) refers to the items that comprise a person's identity, usually including:

- Full name
- National identification number (in the U.S., social security number)
- Telephone number
- Driver's license number
- Passport number
- Residential address
- Bank account numbers
- Credit card numbers

In many locales, organizations are required to protect many of these items, and sometimes others, from unauthorized disclosure. Most often this requirement is in the form of laws and regulations intended to curb the proliferation of this information to others.

Security Management

Security management is primarily concerned with strategic level activities that influence the operation of systems and the behavior of employees. Security management will involve several key activities, including:

- Executive oversight
- Governance
- Policy, guidelines, standards, and procedures

- Roles and responsibilities
- Service level agreements
- Security outsourcing
- Data classification and protection
- Certification and accreditation
- Internal audit

Security Executive Oversight

The support and oversight by executives of security-related activities is vital to the viability of a security program in an organization. Several activities are related to this oversight, including:

- **Support of policies**. Executive support is needed to ensure that security policies and other policies are taken seriously by all members of the organization. Support should come in the form of communication (memos stating that adherence to policy is a required condition of employment) and leadership by example.
- **Allocation of resources**. Executives control the allocation of resources in an organization, primarily through budgeting and staffing levels. In order for a security program to be effective, executives must allocate sufficient resources to security.
- **Support of risk**. One of the primary activities in a security management function is the performance of risk assessments, which result in the treatment of identified risks. Executives need to visibly accept the disposition of risks as documented in risk assessments whether risks are accepted, transferred, mitigated, or avoided.

Security Governance

The IT Governance Institute in its *Board Briefing on IT Governance, 2nd Edition*, defines security **governance** this way:

> *"Security governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly."*

In other words, strategy, objectives, and risks are developed and executed in a top-down manner. In a governance model, executive management is in control of the activities intended to protect organization assets from known threats. Usually this translates into a series of activities that include:

- **Steering committee oversight**. A group of executives are regularly briefed on activities related to security and risk management. Discussions about incidents and events take place, changes to policies are made, and decisions and opinions are solicited.
- **Resource allocation and prioritization**. Executives allocate resources to security-related activities, in order that required activities may be carried out.
- **Status reporting**. Information about events, trends, issues, and other security related matters are collected and sent upwards through meaningful status reports that provide feedback on decisions, strategic direction, and overall effectiveness of the security program.

- **Decisions**. Decisions made at the steering committee level (and at lower levels) are sent downwards to appropriate levels to be carried out by managers and staff members.

Security Policy, Guidelines, Standards, and Procedures

An organization that desires to manage security in a formal way needs to make several statements about the behavior (human, information system, and so on) that is acceptable and unacceptable and how such behavior should be carried out. This is accomplished through a hierarchy of documents, which are:

- Policies
- Requirements
- Guidelines
- Standards
- Procedures

Policies Security **policy** provides constraints of behavior for an organization's personnel as well as its information systems and other machinery. Put another way, security policy specifies the activities that are required, limited, or forbidden in an organization.

An example policy is, *Information systems should be configured to require good security practices in the selection and use of passwords*.

Policy Standards The international standard, ISO 27002:2005, *Information technology—Security techniques—Code of practice for information security management*, is a well known framework on which an organization can build its security policy. The sections in the standard are:

- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance with legal requirements and policies

The SANS organization has a well known security policy model in the *SANS Security Policy Project* found at http://www.sans.org/resources/policies/. Here the reader can find articles on policies, standards, and guidelines, example policies, and whitepapers on the development of security policy.

Policy Effectiveness An organization that enacts policies should take steps to ensure that its policies are effective. Policy effectiveness requires a top-down approach. To be effective, a security policy must be:

- Approved by senior management
- Communicated to employees
- Periodically reviewed
- Assessed for effectiveness

Security policy must reflect and support the mission, objectives and goals of an organization. If the organization is risk-averse (for whatever reason, which doesn't matter), then its security policy should support this risk aversion appropriately. If the organization has a greater appetite for risk, then its security policy should reflect this also.

Requirements

The term **requirements** usually refers to characteristics of an information system or business process. Typically, a set of requirements will be created when a new information system is being developed or purchased. The requirements will help the organization make suitable selection, design, or configuration decisions.

Requirements should reflect security policy; if security policy says, "a system shall not do thus-and-so", then a corresponding requirement should make the same or similar assertion. The goal of security requirements is to constrain a system or process so that, when implemented, it complies with the organization's security policy.

An example requirement is, *Information systems must enforce password quality standards and must be able to reference a central authentication service, either LDAP or Active Directory.*

Guidelines

Whereas security policy defines *what* should be done (or not done), **guidelines** provide information on *how* policy can be implemented. An organization can choose to make guidelines binding statements that must be adhered to, or they can be suggestions or ideas on how specific policies may be implemented. Which approach is adopted is up to the organization.

For example, if a security policy states that *personnel access to business facilities shall be controlled*, guidelines can suggest that keycard systems with PIN pads be used at building entrances and within sensitive areas inside buildings.

An example guideline is, *Users should choose a password that is easy for the user to remember, but hard for others to guess. The types of passwords that should be avoided include: employee, spouse or pet names, significant anniversaries, common words such as "password," words related to work functions, and other easily guessed words. Passwords must not be written down unless they are locked in a desk or file cabinet at all times or carried on the user's person.*

Standards

Standards are statements that specify *what* shall be used to support security policies and guidelines. Typically, standards will comprise the following:

- **Product standards**. These are specific names of products that shall be used to support a policy.

- **Process standards**. These may cite process templates, names, or methodologies.
- **Technology standards**. This includes the use of technology standards such as TCP/IP or OSPF, computer languages, and so on.
- **Reference configurations**. These include server build specs, router configurations, software configurations, and so on.
- **Reference architectures**. These include schematics for building networks, specifications for integrating applications, and so on.

It is expected that standards will change far more frequently than policies and guidelines.

An example standard is: *Minimum password length is 8 characters. Passwords must consist of lower case, upper case, and numeric characters. Passwords must expire after no more than 90 days. Accounts must automatically lock if a user has entered an incorrect password more than three times in ten minutes; accounts must be unlocked by an access administrator, or may be automatically unlocked one hour after the last logon attempt. Users may not use any of the previous 10 passwords used.*

Procedures **Procedures** are the instructions that specify *how* tasks are to be performed. True to the hierarchical form, procedures must support policies, guidelines, and standards.

The purpose of a procedure is to ensure the consistent and methodical completion of repetitive tasks. Consistency builds quality and reduces incidents, which allows the organization to operate more efficiently and at greater levels of service.

Security Roles and Responsibilities

Management should define security roles and responsibilities in the organization. This includes not only the roles and responsibilities of dedicated security personnel, but of all employees in the organization. Roles and responsibilities should be formally defined in two places:

- **Security policy**. General and specific expectations of security staff and other employees should be defined in the organization's security policy.
- **Job descriptions**. Individual job descriptions of security staff and other employees should define specific security-related roles and responsibilities.

The roles and responsibilities that need to be defined include:

- **Ownership of assets**. Individual assets and groups of assets need to have designated owners who are responsible for their operation and protection.
- **Access to assets**. The owners of assets should be designated as the persons who decide who may access or use those assets. A higher level of management may be responsible for approving non-standard access to assets.
- **Use of assets**. All employees should be explicitly designated as responsible for their individual use of assets.
- **Managers**. Managers should be designated as being responsible for the behavior of employees under their control.

Service Level Agreements

A **service level agreement** (**SLA**) is a formally defined level of service provided by an organization. Within the context of security management, SLAs may be defined for many activities, including:

- **Security incident response**. A security team may be required to mobilize within a stated period of time when a security incident has been called.
- **Security alert delivery**. Security alerts, which may be bulletins of threats or vulnerabilities, may need to be delivered to recipients within a stated period of time.
- **Security investigation**. A security investigator may be required to respond to a call for assistance within a stated period of time.
- **Policy and procedure review**. A security team may be required to periodically review policies, procedures, and other documents at regular intervals.

SLAs can be defined for other tactical activities performed by security management and staff.

Secure Outsourcing

Outsourcing is the subcontracting of a business process to a third-party company. Organizations outsource many different functions for a variety of reasons, including:

- Redirecting energy on the organization's core competencies
- Controlling the efficient use of capital and other resources

There are some risks associated with the outsourcing of business processes to third parties, including:

- **Control of confidential information**. An organization will need to equip the outsourcer with the information required to perform its functions properly. Because this information is now out of its direct control, protection of that information is now entirely dependent upon the outsourcer's actions.
- **Loss of control**. Organizations that outsource functions to third parties give up a measure of control to that organization.
- **Accountability**. While the organization has outsourced functions to a third party and is at the complete mercy to the third party's integrity, the organization is still completely accountable for the actions performed by the outsourcer.

Data Classification and Protection

Organizations store, transmit, and manage a wide variety of types of information, ranging from personnel and payroll records to computer source code to content on public facing web sites. Information security professionals who are responsible for protecting this information need to decide what measures are required to protect the data. Data of widely varying levels of sensitivity exists in many forms; while it is possible to develop criteria for protecting every set of data in the organization, this approach scales poorly.

Data classification is the undertaking of developing levels of sensitivity for information, and assigning those levels for the purpose of establishing appropriate modes of protection for those datasets. This orderly system of assigning classification levels is preferable to a chaotic environment where information is protected in an ad hoc style.

A formal data classification program consists of several parts, which are:

- Sensitivity levels
- Marking procedures
- Access procedures
- Handling procedures

Sensitivity Levels In a data classification program, a set of **sensitivity levels** is established, which reflects the nature of data that is used in the organization. Such a set of sensitivity levels could be, for example:

- Top Secret
- Secret
- Confidential
- Public

Most organizations don't have more than four or five levels, since each level generally will have it own sets of marking and handling procedures. The more levels there are, the more complicated the classification program will be. Pragmatically, establishing too many levels will introduce too much complication, increase the likelihood of errors, while providing only marginally more security than a simpler program.

Because information classification and handling is largely a human-driven and -operated process, it is preferable to use a simpler scheme of classification levels that will reduce ambiguity and errors.

Information Labeling **Labeling**, or **marking**, is the process of affixing a word, symbol, or phrase on a set of data. The purpose of labeling is to make other readers aware of the level of classification on a set of data. When others are aware of the classification level of a particular set of data, they are more apt to be aware of the classification level and handle the data properly.

Using the example of the four levels of classification above, here are some sample labels that can be affixed to human-readable documents shown in Table 1.2.

Marking is not as simple as it may first appear. While it can be relatively simple to mark a document or report with a header or footer containing a classification word or phrase, or affix a classification label on a backup tape, effectively labeling stored or transmitted data is not so clear-cut. Other situations include:

- **On-screen labeling.** Software programs that display classified information can include on-screen labeling.
- **Data transmission.** Devices that transmit classified information can have labels affixed to them; further, administrative interfaces (used by network or systems engineers) can have a label displayed at login time. Cabling used to transmit classified information can be labeled or color-coded.

Level	Label
Top Secret	"COMPANY Top Secret" in at least 48 pt type on cover page. "COMPANY Top Secret: for registered personnel only" in at least 24 pt type on every page.
Secret	"COMPANY Secret: for authorized personnel only with a business need-to-know" in at least 20 pt type on every page.
Confidential	"COMPANY Confidential: for employees and customers only" in at least 14 pt type on every page.
Public	"COMPANY Approved for Public Use" on every page.

Table 1-2 Sample classification labels

Handling Once classified information is introduced into an organization, it needs to be handled properly in every type of situation. Handling guidelines need to be developed for each level of classification, for each possible type of activity, including these listed here and possibly several more:

- **Computer storage**. Classification guidelines can include which systems (or classes of systems) are permitted to store the data and under what specific conditions.
- **Computer access control**. Classification guidelines may include business rules about which personnel (individuals, groups, departments, roles, security clearance level, etc.) may access classified information.
- **Backup tape and other portable media**. Classification guidelines will determine when and how data at different classification levels may be written to various types of portable media. For instance, data at the highest levels of secrecy might be forbidden from most or all portable media, and at other levels, encryption may be required.
- **Network transmission**. Classification guidelines should specify if and how data at various classification levels may be transmitted over networks. Of course there are different types of networks (internal, external, and perhaps physically separate high-secrecy networks), so this guideline alone will probably be multidimensional.
- **E-mail transmission**. Classification guidelines may determine which classification levels permit e-mail to be used to transmit classified information to another person. Like network transmission, e-mail transmission will probably contain conditions such as encryption, internal vs. external recipients, and so on.
- **Facsimile**. Classification guidelines should address whether information at different classification levels can be faxed and, if so, what conditions should be imposed, such as confirming that the sender's and recipient's fax machines will be attended throughout the transmission.
- **Printing**. Classification guidelines should address the conditions under which information at various classification levels may be printed.
- **Mailing/shipping/courier**. Classification guidelines need to address whether and how classified information may be mailed or shipped. Possible conditions include lockbox, registered, insured, and double-sealed packages.
- **Carrying**. Classification guidelines need to include guidance on the safeguards that individuals need to take when carrying classified information.

- **Hardcopy storage.** Classification guidelines should address how hardcopies of classified information must be stored. Some levels may require double-locking (stored in a locked desk or cabined in a locked office), for instance.

Destruction **Classification** guidelines need to include information on the proper disposal of classified information. **Destruction** procedures—steps to ensure that information is discarded in a way that renders it non-retrievable—need to include every type of media and likely context.

For example, media destruction procedures should include proper disposal of hardcopy documents. In the workplace there are sure to be shredders or secure document disposal bins, but what about staff members who work primarily in home offices? And how does someone on extended travel safely dispose of a classified document?

Certification and Accreditation

Certification and accreditation are the activities associated with the evaluation of a system against a set of standards or policies. These activities are carried out as part of a formal approval process for initiating or continuing the use of a system.

- **Certification** is the process of evaluating a system against a set of formal standards, policies, or specifications.
- **Accreditation** is the formal approval for the use of a certified system, for a defined period of time (and possibly other conditions).

Internal Audit

In the context of information security, **internal audit** is the activity of self-evaluation of controls and policies to measure their effectiveness.

In order to be effective itself, the internal audit function must be objective. This means that the staff members performing internal audit activities should not be a part of the department or division that they are examining. Instead, internal audit should report to a dissociated part of the organization such as Legal.

Internal audit should follow a formal methodology that will further the objectivity and quality of the examination of security controls. One of the most widely recognized methodologies is the Standards and Practices of internal auditing from The Institute of Internal Auditors, available at www.theiia.org.

Security Strategies

Management is responsible for developing the ongoing strategy for security management. The development and changes to the security strategy will be based upon the results of past events, including:

- **Incidents.** If any security incidents have occurred, the facts uncovered in the handling of the incident, as well as its root cause, may prompt management to make changes.
- **Performance of SLAs.** If the performance of SLAs is below expectations, management may make changes to improve this.

- **Certification and accreditation.** The outcomes of recent certifications and accreditations may provide cause for strategic changes.
- **Internal audit.** The results of internal audits may prompt management to make changes to audited processes or to the audit process itself.

Strategic changes should be made in consultation with executive management and through the governance function described earlier in this section.

Personnel Security

The "cradle-to-grave" approach to employment is largely a thing of the past. In most organizations and industries, people are changing jobs as frequently as every three to five years. This can mean that some organizations are replacing as much as a third of their personnel every year. Consequently, organizations have a lot of staff members that they don't really know all that well. And because most organizations rely heavily on their information systems for many key business processes, they are entrusting the ongoing integrity and viability of the business on people they don't really know all that well.

With long-term employees comes a high level of comfort and trust. But in businesses with higher employee turnover, employers need to replace the trust with additional up-front due diligence, in the form of more formal hiring practices and **background verifications**.

Another area of risk lies in the fact that employers are entrusting their employees with access to a great deal of information. Most information systems lack sufficiently detailed access controls, resulting in employees having access to a lot more information than they really need. This increases the risk of damage to the business if an employee makes an error in judgment or is careless. Employers, then, need to provide formal training to its staff on the proper use of organization information systems and handling of information.

These topics are addressed in this section.

Hiring Practices and Procedures

The near-universal practice among organizations is the use of written agreements that employers and employees sign at various stages of the employment relationship.

Non-Disclosure Agreement

As soon as an employer and an employment candidate are discussing potential employment, an employer can require the candidate to sign a **non-disclosure agreement** (**NDA**). This agreement will require that the candidate not discuss any details about the organization with any other party.

The advantage of the pre-employment NDA is that the employer will have some written assurance that the candidate will not share any secrets shared during interviews. While an **employment agreement** will certainly have a non-disclosure clause in it, a separate pre-employment NDA provides some protection from disclosure by those individuals who the organization does not hire.

Consent to Background Verification

As the pre-employment relationship advances, an employer that is considering making an offer of employment to a candidate will, in most

jurisdictions, be required to obtain a signed consent to obtain background information from the candidate. In this simple form, the candidate is providing basic identifying information (e.g., full name, aliases, date of birth, country of citizenship, social/insurance number), together with a written consent for the employer to obtain background information.

The consent form may also contain a clause that states that the employer may refuse employment, terminate employment, and even turn the candidate over to law enforcement authorities if the candidate provides false or misleading information or is found to have an undesirable background.

The employer may also use information obtained from the employment application form to confirm certain aspects of a candidate's background.

Background Verification In regions of the world with higher rates of crime, an organization runs a real risk of hiring someone with a criminal record. An organization that is considering hiring a candidate should complete a **background verification** to validate the truthfulness of the candidate's claims and to investigate the candidate's potential criminal background. The following checks may be included in a background check:

- Confirmation of citizenship and of the candidate's legal right to employment
- Confirmation of employment history
- Confirmation of education background
- Confirmation of professional certifications and licenses
- Investigation on potential criminal history
- Investigation of credit history, important for positions involving financial management responsibility
- Investigation of potential ties with terrorist or criminal organizations

Offer Letter An organization intent upon hiring a candidate will next issue an offer of employment, or **offer letter**, which usually contains:

- Position title and description
- Start date
- Compensation
- Name of manager

The offer letter should tie together the other elements of the hiring process, including non-disclosure, background check, non-compete, and the requirement that the candidate always abide by security policy and other policies.

Non-Compete In some locales, an organization can also restrict an employee's ability to change employers to work for a competitor. Organizations intent on enforcing non-compete are concerned with the protection of their intellectual property and other insider information. A **non-compete agreement** is a legal agreement that specifies terms and conditions related to the possibility of an employee accepting employment with a competing organization in the future.

Intellectual Property Agreement An **intellectual property agreement** guarantees that the organization owns all intellectual property (IP) that may be created by an employee. Often this includes IP that an employee may create while working on his or her own time using his or her own resources.

Employment Agreement Sometimes an organization and a new employee will sign an **employment agreement** that defines terms and conditions of the employment relationship. Generally, employment agreements are limited to executives, but are also used when hiring licensed professionals like teachers or doctors. Where labor unions are used to manage employer-employee relationships, employment agreements often represent an entire segment of the organization's workforce.

Employee Handbook Many organizations have an **employee handbook**, a formal document that describes the terms and conditions of employment, including but not limited to:

- Working hours and locations
- Expected behavior
- Benefits
- Paid and unpaid leave
- Policies, including security policy
- Acceptable use of organization assets, including workstations and other information systems

In many situations, employees are required to sign the employee handbook, which provides a written attestation that the employee understands all of the terms and conditions of employment and of the organization's principal policies.

Formal Job Descriptions Many organizations have developed formal **job descriptions**, which are formal documents that typically include:

- Job title
- Pay range
- Description of duties
- Description of responsibilities
- Required experience

Often, organizations include adherence to policies in the list of responsibilities. This further strengthens the organization's message that all policies, including security policies, are taken seriously.

Termination

Various circumstances lead to a separation of employment, which are either employee-initiated or employer-initiated. Regardless of the cause, organizations need to perform certain critical tasks upon **termination** of an employee, including:

- Terminate access to all information systems and networks
- Change administrative passwords that may be known to the employee

- Recover all organization-owned assets
- Have incoming e-mail for the terminated employee routed to a designated person or group

Some termination situations call for an urgent mobilization of curtailment of access by the terminated employee, to prevent the former employee from accessing information systems for the purpose of causing harm to the organization. At times the organization will need to take additional steps, including:

- A review of all recent activities related to the terminated employee
- Code reviews of software source code that the terminated employee had access to

These reviews may be needed, on the chance that the employee sensed the termination was imminent and had reason to damage information systems.

Work Practices

Several practices, when put into place, will reduce behavioral-based risk in an organization. These practices are:

- Separation of duties
- Job rotation
- Mandatory vacations

Separation of Duties The principle of **separation of duties** (sometimes known as *segregation of duties*) states that important tasks should require more than one person to complete. A group of two or more employees are less likely to carry out an unauthorized task. Examples of tasks that should employ separation of duties include:

- Payment requests
- Requests for privileged access

In these examples, no single individual should be able to perform these duties. Instead, strictly controlled processes should be established that require at least two individuals (and not just *any* two, but two designated persons or roles) should be required to perform these functions.

Job Rotation Personnel in sensitive roles may, after extended intervals, be tempted to collusion for personal gain and other unauthorized activities. When employers occasionally rotate personnel through various roles, especially when unannounced, employees are less likely to perform these "extra" activities. This practice is known as **job rotation**. Enacting this can be difficult in smaller organizations that have only single individuals in various roles.

Mandatory Vacations While it is laudable that some employees are so loyal to their employers that they wish to never leave their posts, mandatory vacations provide something akin to short-term job rotation that can sometimes helps an organization spot irregularities that may be a sign of unauthorized activities. When mandatory vacations are institutionalized, employees are less likely to carry out prohibited activities that could be detected during their absence.

Security Education, Training, and Awareness

In order to adequately protect its assets, organizations need their employees to exercise good judgment and be keen to irregularities that could be signs of trouble. But because this new "21st century digital common sense" is not yet common, organizations need to take time to teach its employees the "do's" and "don'ts" of information security. This formal education is known as **security awareness training** and needs to be strategic, formal, and presented in a variety of ways, including:

- **Security content in new-hire paperwork**. This includes the employee handbook and documents that a new employee is required to sign upon hire. This is covered earlier in this chapter in the section, "Hiring practices and procedures."
- **Security content in day-one orientation**. New employees need to be made aware of key security policies on their first day of hire.
- **Security training**. Soon after starting employment, new employees should be enrolled in more comprehensive security awareness training, which may take the form of classroom or web-based training.
- **Specialized training**. Employees in some job categories may be required to attend additional specialized training, including:
  - Secure programming for software developers
  - Fraud prevention for finance department employees
  - Network and system protection for network and system engineers
- **Other messaging**. In addition to training, messages of other forms need to be periodically made available to employees, including:
  - E-mail
  - Posters and flyers
  - Promotions
  - Voice-mails
  - Incentive programs
- **Testing**. In addition to providing educational material on security and asset protection, many employers also test employees to assess their knowledge. Employees may even be required to attain a minimum test score or be required to repeat security training.

Professional Ethics

The Merriam Webster dictionary defines **ethics** as "the discipline dealing with what is good and bad and with moral duty and obligation." It defines *professional ethics* as "the principles of conduct governing an individual or a group." From these two definitions, we understand that security professionals' behavior should reflect a high level of morality, integrity, and responsibility.

Security professionals are expected to lead by example. Security professionals should abide by security policies that they expect other employees to follow. In a real sense, security professionals are like law enforcement and should be held to an even higher standard than the rank-and-file.

Many professional organizations have published a code of ethical standards that members are required to uphold. (ISC)², the governing body of the CISSP certification, has a comprehensive code of ethics that all security professionals, CISSP or not, should adopt as their own.

Each CISSP certification holder is required to support the (ISC)² Code of Ethics, which appears in Appendix B.

Chapter Summary

- An organization's security program should support the organization's mission, objectives, and goals.
- *Risk management* is the process of determining the acceptable level of risk and the use of risk assessment and mitigation to reduce risk to an acceptable level.
- The core principles of information security are *confidentiality*, *integrity*, and *availability*.
- *Defense in depth* is a technique of using a layered defense to protect an asset.
- A *single point of failure* is the characteristic of a component in a system if the failure of the component will result in the failure of the system.
- *Fail open* is the characteristic of a control to permit all accesses when the control fails. *Fail closed* is the characteristic of a control to block all access when the control fails.
- *Privacy* is related to the protection of private information associated with private citizens.
- Executive oversight is needed for the support of policies, allocation of resources, and support of risk.
- *Security governance* is the set of responsibilities and practices related to the development of strategic direction and risk management.
- *Security policies* specify the required characteristics of information systems and the required conduct of employees.
- *Security requirements* specify required characteristics of information systems and processes, and are usually used during systems development and acquisitions.
- *Guidelines* are statements that specify how security requirements may be carried out.
- *Standards* specify the types of systems, tools, technologies, configurations, and architectures used in an organization.
- *Procedures* are the step-by-step instructions used to perform tasks.
- Security-related roles and responsibilities are defined in security policies and job descriptions.
- Security roles and responsibilities define the ownership, access, and use of assets, and the general responsibilities of managers and employees.

- *Service level agreements (SLAs)* are formal statements that specify levels of service provided by a service organization.
- An organization that outsources business processes needs to ensure that its intellectual property is adequately protected.
- A data classification and protection policy defines levels of sensitivity for business information, as well as handling procedures for each level of sensitivity.
- *Certification* is the process of evaluating a system against a set of evaluation criteria. *Accreditation* is the act of permitting the use of a certified system.
- Internal audit is the activity of evaluating security controls and policies to measure their effectiveness.
- Management is responsible for the development of security strategies, in order to maintain and improve security-related activities in the organization.
- An organization's hiring process should include the use of non-disclosure, employment, non-compete, intellectual property, and acceptable use agreements, as well as background checks.
- An *employee handbook* should highlight all terms and conditions of employment.
- Job descriptions should explain all responsibilities and requirements for each position in the organization.
- Upon termination of employment, the organization should retrieve all assets issued to the terminated employee and immediately rescind the employee's access to all information systems.
- Sound work practices include separation of duties, job rotation, and mandatory vacations.
- A security education, training, and awareness program should keep employees regularly informed of their expectations.
- Security professionals should adhere to a strict code of professional conduct and ethics.

Key Terms

Accreditation The process of formally approving the use of a system.

Annual loss expectancy (ALE) The yearly estimate of loss of an asset, calculated as: ALE = ARO × SLE.

Annualized rate of occurrence (ARO) The probability that a loss will occur in a year's time.

Asset An object of value to the organization. An asset may be a physical object such as a computer, or it can be information.

Availability The concept that asserts that information systems can be accessed and used when needed.

Background verification The process of verifying an employment candidate's employment, education, criminal, and credit history.

Certification The process of evaluating a system against a specific criteria or specification.

CIA Confidentiality, Integrity, and Availability.

Classification See *Data classification*.

Confidentiality The concept of information and functions being protected from unauthorized access and disclosure.

Countermeasure A control or means to reduce the impact of a threat or the probability of its occurrence.

Data classification The process of assigning sensitivity levels to documents and data files in order to assure their safekeeping and proper handling.

Defense in depth A strategy for protecting assets that relies upon several layers of protection. If one layer fails, other layers will still provide some protection.

Destruction The process of discarding information in a way that renders it non-retrievable.

Employee handbook A formal document that defines terms and conditions of employment.

Employment agreement A legal agreement that specifies terms and conditions of employment for an individual employee or group of employees.

Ethics The discipline of dealing with a code of professional behavior.

Exposure factor (EF) The proportion of an asset's value that is likely to be lost through the realization of a particular threat.

Fail closed The characteristic of a security control—upon failure, it will deny all access.

Fail open The characteristic of a security control—upon failure, it will permit all access.

Fail safe See *Fail closed*.

Fail soft The process of shutting down non-essential components on a system, thereby freeing up resources so that critical components can continue operating.

Governance The entire scope of activities related to the management of policies, procedures, and standards.

Guideline Information that describes how a policy may be implemented.

Integrity The concept of asserting that information may be changed only by authorized persons and means.

Intellectual property agreement A legal agreement between an employee and an organization that defines ownership of intellectual property (IP) that the employee may develop during employment.

Internal audit The activity of self evaluation of controls and policies to measure their effectiveness.

Job description A formal document that defines a particular job title, responsibilities, duties, and required experience.

Job rotation The practice of rotating personnel through a variety of roles in order to reduce the risk of unauthorized activities.

Labeling The process of affixing a sensitivity identifiers to a document or data file.

Marking See *Labeling*.

Non-compete agreement A legal agreement that stipulates terms and conditions regarding whether the employee may accept employment with a competing organization in the future.

Non-disclosure agreement (NDA) A legal agreement that requires one or both parties to maintain confidentiality.

Offer letter A formal letter from an organization to an employment candidate that offers employment under a basic set of terms.

Personally identifiable information (PII) Items associated with an individual such as name, passport number, driver's license number, and social insurance number.

Policy An official statement that establishes plans, boundaries, and constraints on the behavior of information systems and employees.

Privacy The protection of sensitive information associated with individuals.

Procedure Step-by-step instructions for performing a task.

Requirements Statements of necessary characteristics of an information system.

Residual risk The risk that remains after countermeasures are applied.

Risk acceptance A form of risk treatment where an identified risk is accepted as-is.

Risk assessment The process of examining a system or process to identify potential risks.

Risk avoidance A form of risk treatment where the activity associated with an identified risk is discontinued, thereby avoiding the risk.

Risk management The strategic activities related to the identification of risks through risk assessment and the subsequent treatment of identified risks.

Risk mitigation *See* Risk reduction

Risk reduction A form of risk treatment where an identified risk is reduced through countermeasures.

Risk transfer A form of risk treatment where an identified risk is transferred to another party, typically through an insurance policy.

Security awareness training A formal education program that teaches security principles and expected behavior to employees.

Security management Activities related to the development and implementation of security policies and controls.

Security policy A branch of organizational policy that defines security-related controls and behaviors.

Sensitivity level A category of information sensitivity in an information classification scheme.

Separation of duties The work practice where high risk tasks are structured to be carried out by two or more persons.

Service Level Agreement (SLA) Formal statements that specify levels of service provided by a service organization.

Single Loss Expectancy (SLE) The cost of a single loss through the realization of a particular threat. This is a result of the calculation, SLE = asset value × exposure factor (EF).

Single point of failure A component in a system that lacks a redundant or backup counterpart; the failure of the component will cause the failure of the entire system.

Standard A statement that specifies the brand, model, protocol, technology, or configuration of a system.

Termination The cessation of employment for an employee.

Threat A potential activity that would, if it occurred, exploit a vulnerability in a system.

Vulnerability A weakness in a system that may permit the realization of a threat.

Review Questions

1. An organization that needs to understand vulnerabilities and threats needs to perform a:
   a. Penetration test
   b. Threat analysis
   c. Qualitative risk assessment
   d. Quantitative risk assessment
2. A risk manager has performed a risk analysis on a server that is worth $120,000. The risk manager has determined that the Single Loss Expectancy is $100,000. The Exposure Factor is:
   a. 83%
   b. 1.2
   c. 80%
   d. 120%
3. A risk manager has performed a risk analysis on a server that is worth $120,000. The Single Loss Expectancy (SLE) is $100,000, and the Annual Loss Expectancy (ALE) is $8,000. The Annual Rate of Occurrence (ARO) is:
   a. 12.5
   b. 92%
   c. 8
   d. 8%
4. A risk manager needs to implement countermeasures on a critical server. What factors should be considered when analyzing different solutions?
   a. Original annualized loss expectancy (ALE)
   b. Annualized Loss Expectancy (ALE) that results from the implementation of the countermeasure
   c. Original Exposure Factor (EF)
   d. Original Single Loss Expectancy (SLE)

5. The general approaches to risk treatment are:
   a. Risk acceptance, risk avoidance, and risk reduction
   b. Risk acceptance, risk reduction, and risk transfer
   c. Risk acceptance, risk avoidance, risk reduction, and risk transfer
   d. Risk analysis, risk acceptance, risk reduction, and risk transfer
6. CIA refers to:
   a. Confidence, Integrity, and Audit of information and systems
   b. Confidentiality, Integrity, and Assessment of information and systems
   c. Confidentiality, Integrity, and Availability of information and systems
   d. Cryptography, Integrity, and Audit of information and systems
7. A recent failure in a firewall resulted in all incoming packets being blocked. This type of failure is known as:
   a. Fail open
   b. Access failure
   c. Circuit closed
   d. Fail closed
8. The definition of PII:
   a. Is name, date of birth, and home address
   b. Is name, date of birth, home address, and home telephone number
   c. Is name, date of birth, and social insurance number
   d. Varies by jurisdiction and regulation
9. The statement, "All financial transactions are to be encrypted using 3DES" is an example of a:
   a. Procedure
   b. Guideline
   c. Standard
   d. Policy
10. The purpose of information classification is:
    a. To establish procedures for safely disposing of information
    b. To establish procedures for the protection of information
    c. To establish procedures for information labeling
    d. To establish sensitivity levels for information
11. An organization is concerned that its employees will reveal its secrets to other parties. The organization should implement:
    a. Document marking
    b. Non-disclosure agreements

c. Logon banners
d. Security awareness training

12. The purpose of a background verification is to:
    a. Obtain independent verification of claims on an employment application
    b. Determine if the applicant should be hired
    c. Determine if the applicant is suitable for the job description
    d. Determine the applicant's honesty
13. When an employee is terminated from employment, the employee's access to computers should be terminated:
    a. At the next monthly audit
    b. At the next quarterly audit
    c. Within seven days
    d. Within one day
14. Security awareness training should be:
    a. Mandatory for information workers only
    b. Optional
    c. Provided at the time of hire and annually thereafter
    d. Provided at the time of hire
15. Management in an organization regularly reassigns employees to different functions. This practice is known as:
    a. Job rotation
    b. Reassignment
    c. Separation of duties
    d. Due diligence

Hands-On Projects

Project 1-1: Defense in Depth Network Design

In this project you will design a new network infrastructure for a five-hundred employee law firm. The design of the network should incorporate several elements that demonstrate a defense in depth architecture.

The design of the network should incorporate protection against the following threats:

- Malicious software
- Phishing
- Spam

- Leakage of intellectual property
- Non company-owned devices on the internal network
- Rogue access points

For each type of threat, indicate the controls or features in the architecture that reduce or eliminate the threat.

This project is not so much about network technology as it is about the concept of defense in depth. Do not worry about whether you have incorporated the latest or the most precisely correct technologies in your design.

Project 1-2: Data Sensitivity Procedures

In this project you will develop data sensitivity procedures.

1. Develop a matrix with three columns, one for each of three levels of increasing sensitivity. Choose easily understood titles for each level.
2. The rows of the matrix should consist of various data handling activities including:
   - E-mail
   - FAX
   - Courier
   - Laptop computer
   - Hard copy
3. The cells of the matrix should specify whether the activity is permitted (for instance, if the most sensitive documents are permitted to be faxed) and, if so, under what conditions.
4. Opine on the matter of the number of sensitivity levels: how few or how many are needed, and how realistic is it to expect employees in an organization to be able to understand the classification levels and the procedures for protecting information at each level.

Project 1-3: Security Awareness Training

In this project you will develop a security awareness training plan for a 1000-employee company. You are to determine:

1. What training new-employees should receive upon hire.
2. What written materials should be issued to new employees.
3. What materials should be available on an intranet site.
4. What types of security awareness messages that should be issued to employees.

5. What specialized training should be available to IT personnel.
6. What recordkeeping for training should take place.

Case Projects

Case Project 1-1: Qualitative Risk Assessment

As a consultant with the Risk Analysis Consulting Co., you have been asked to perform a qualitative risk assessment for the TRC Chemical Company.

TRC Chemical has a large outside sales force, numbering in the hundreds. Most of these employees use their own home computers (70% laptops, 30% desktops) to conduct TRC Chemical business. You have been asked to assess the risks associated with the use of home computers versus company-owned and -managed computers.

Case Project 1-2: Quantitative Risk Assessment

As a consultant with the Risk Analysis Consulting Co., you have completed a qualitative risk assessment regarding the risks associated with using non company-owned computers to conduct company business. Your customer, TRC Chemical, is pleased with the results of the qualitative risk assessment and wants to see hard numbers to see whether it can justify the capital and expense burden of equipping the sales force with company-owned computers, based upon risk mitigation alone.

In your risk assessment, make best-estimates on the value of information and costs associated with purchasing and supporting company-owned computers.

Case Project 1-3: Segregation of Duties Matrix

As a consultant with the Risk Analysis Consulting Co., you have been asked to help the BBX Internet Stock Trading Company develop a viable segregation of duties for the management of its online software and supporting infrastructure.

The activities that BBX is concerned with include:

- Request and assignment of privileged access at the network, operating system, database, and application layers
- Setup of new customers
- Changes to audit alert settings

For each of the activities listed above, develop a segregation of duties matrix where different parts of each process are performed by different individuals.

Things to consider:

- Separate the activity of requesting an action from performing the action.
- Add an activity of confirming correct completion of the action.
- Include any recordkeeping for the action so that an auditor can examine the action after-the-fact to see if the action was appropriately carried out.

chapter 2

Access Controls

Topics in this Chapter:

- Identification and Authentication
- Centralized Access Control
- Decentralized Access Control
- Access Control Attacks
- Testing Access Controls

Access control is the general term in information technology that encompasses the various methods used to control who (and what) is permitted to access specific information and perform specific functions.

The (ISC)^2 *Common Body of Knowledge* (CBK) defines the key areas of knowledge for Access Control in this way:

Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It permits management to specify what users can do, which resources they can access, and what operations they can perform on a system.

The candidate should fully understand access control concepts, methodologies and implementation within centralized and decentralized environments across the enterprise's computer systems. Access control techniques, detective and corrective measures should be studied to understand the potential risks, vulnerabilities, and exposures.

Key areas of knowledge:

- *Control access by applying the following concepts/methodologies/techniques*
- *Identify, evaluate, and respond to access control attacks (e.g., Brute Force, Dictionary, Spoofing, Denial of Service)*
- *Design, coordinate, and evaluate penetration test(s)*
- *Design, coordinate, and evaluate vulnerability test(s)*

Controlling Access to Information and Functions

Computer systems, databases, and storage and retrieval systems contain information that has some monetary or intrinsic value. After all, the organization that has acquired and set up the system has expended valuable resources to establish and operate the system. After undergoing this effort, one would think that the organization would wish to control who can access the information that it has collected and stored.

Access controls are used to control access to information and functions. In simplistic terms, the steps undertaken are something like this:

1. Reliably identify the subject
2. Find out what information the subject wishes to access
3. Determine whether the subject is allowed to access the information
4. Permit (or deny) the subject's access to the information
5. Repeat

The actual practice of access control is far more complex than these five steps. This is due primarily to the high-speed, automated, complex, and distributed nature of information systems. Even in simple commercial environments, information often exists in many forms and locations, and yet these systems must somehow interact and quickly retrieve and render the desired information, without violating any access rules that are in place. These same systems must

also be able to quickly distinguish "friendly" accesses from hostile and unfriendly attempts to access—or even alter—this same information. The remainder of this chapter examines these topics in detail.

Identification and Authentication

Whenever a person, a program, or another computer wants to contact an information system for the purpose of adding information, retrieving information, or performing some function, the information system being contacted first wants to identify the person or object that is making the contact. There are two primary reasons that the contacted information system does this:

- So that the contacted information system can associate any accesses or transactions with the identity of the requesting person or system. Systems and applications usually have transaction logs or audit logs that list the events that took place, and such logs almost always associate events with the persons who performed them.
- So that the contacted information system can verify that the requested activity is permitted.

The two principle terms that need to be defined are: identification and authentication.

- **Identification** is the *unproven* assertion of an identity.
- **Authentication** is the assertion of an identity that is confirmed through some means such as a **password** (a secret word or phrase).

Information systems often use *levels* of identification and authentication when interacting with users. Here is an example: a web site distinguishes new visitors from returning visitors through the use of cookies. The web site prompts the user for a password before the user is permitted to view sensitive information such as an account profile or an order history. The web site may prompt the user again before approving a transaction such as a purchase, to ensure that the user performing the transaction is the same person who provided a userid and password earlier.

Authentication Methods

While most information systems authenticate users through a userid and password, there are other methods in wide use. Conceptually, information systems authenticate users by challenging the user in one of three ways:

- **What the user *knows*.** This method requires the user to input information that the user has committed to memory or has written down. Typically this consists of a userid and password or a userid and **personal identification number** (**PIN**). The weakness with this type of authentication is that the information that the user knows can be guessed by others, or it may be written down and subsequently discovered by other persons. The advantage of this type of authentication is that it is usually inexpensive and easy to implement.
- **What the user *has*.** This form of authentication relies on something that the user has in his or her possession. This type of authentication is often called **two-factor authentication** or **strong authentication** because it relies on two factors: what the user *knows* and what the user *has*. Examples of two-factor authentication include **smart card**, **token**, and USB key (described in more detail later in this section). In order to log in to an information system, the user must know information such as a userid and password, and the user must also have the physical object (the token, USB key, or smart card) in his possession and use it properly. The disadvantage of this type of authentication is that it's more costly to implement, and users sometimes lose their devices.

Sometimes, users store their authentication devices with their notebook computers, and when the notebook computer is stolen, the authentication device is stolen along with it. The advantage of strong authentication is that the information system is much more difficult to break into without possession of the authentication device.

- **What the user *is***. This type of authentication involves some form of **biometric** device, used to measure a characteristic of the user's body such as a fingerprint, hand scan, signature, iris scan, facial scan, and so on. This type of authentication is also considered **two-factor authentication** or **strong authentication** because it relies on what the user *knows* and what the user *is*. The intention of biometrics is to ensure that only the designated person will be able to access an information system, even if a user's userid and password have been compromised.

Strong authentication and biometrics are described in more detail later in this chapter.

How Information Systems Authenticate Users Most information systems authenticate users by requesting their userid and password. This is usually done through an interactive dialog that the information system presents to the user on a screen. The user types in his userid in the spaces provided, like the login dialog shown in Figure 2-1.

Figure 2-1 User login screen

Source: Course Technology/Cengage Learning

After the system accepts the user's credentials, the system verifies the userid and password by looking up the information in one of several ways, including:

- Looking up the userid and password in a stored file or database table
- Making a request to an authentication service that may be present on the same system, or to a centralized authentication service elsewhere on the network

If the userid and password match, then the system permits the user to perform whatever permitted functions have been configured for that user. If the userid and password do not match, the system will display a message that tells the user that the userid or password were incorrect.

How a User Should Treat Userids and Passwords A user's userid may be known to other persons. For instance, in an e-mail system, a user's userid may be their e-mail address. In many cases, userids must be known so that user interaction may take place.

While userids are usually well-known, users are always required to keep their passwords secret. When a user keeps his password a secret, other users are unable to use that user's account. This and other issues related to authentication are discussed later in this chapter.

How a System Stores Userids and Passwords Because passwords are supposed to be secret, they must be stored with a greater degree of protection than other information. Generally, a password is stored in an **encrypted** (a reversible process of scrambling the data to make it unreadable) or **hashed** (a process similar to encryption that is irreversible) form, so that someone (such as a database administrator), who has access to the information where passwords are stored, will not be able to see users' passwords. The preferred method for storing passwords is hashing, a method for storing information that makes it impossible for anyone to know the password.

Hashing is a cryptographic algorithm where the bits in the password are subjected to a mathematical algorithm that transforms the cleartext password into ciphertext. The system stores only the ciphertext. Then, when a user logs in to the system, the system hashes the password that the user typed in and compares it to the stored hash. If the two hashes are equal, then we know that the user typed in the password correctly. If the two hashes are not equal, then the user typed in the wrong password.

Strong Authentication Authentication that relies only upon a userid and password is too weak for many environments that store or manage sensitive information. Because a userid and password can be compromised, organizations often employ some method of *strong authentication* that relies upon more than just what users know. The two general types of strong authentication are two-factor authentication and biometrics.

Two-Factor Authentication **Two-factor authentication** involves the use of information that the user *knows*, such as a userid and password, and also upon something the user *has*, such as a smart card or token (described later in this section). It is considerably more difficult for an intruder to break in to an environment's authentication when two factor authentication is used. This is because the intruder, in addition to knowing a userid and password, must also have in his possession the hardware device that is also required for a user to successfully authenticate.

Here is a physical world analogy: personnel are required to key in a six-digit key code to enter a building. This is functionally similar to entering a userid and password in an information system. But if personnel are also required to insert a smart card to enter the building, this would be similar to a two-factor authentication for an information system. While an intruder may learn an employee's key code, the intruder would have to also obtain the employee's smart card in order to successfully enter the facility.

The preceding analogy simplifies access controls somewhat. The example does not, for instance, discuss whether an intruder can gain access to the facility by breaking in and bypassing the entry controls altogether. These are also concerns for information systems, where intruders can attempt to bypass security controls and use other means to gain illicit entry.

There are several types of two-factor authentication, including:

- **Digital certificate**. A user's workstation contains a digital certificate that must be present for the user to log in. The certificate can be constructed with elements that identify both the user and the workstation, so that the certificate cannot function in any other workstation. Like other types of two factor authentication, the user is also required to furnish a userid and password.
- **Smart card**. A credit card-sized plastic card that contains a microchip that stores a digital certificate or other identifying information.
- **Password token**. A small fob device that displays a passcode that changes periodically, usually every minute. When the user logs on, he must supply a userid, password, and the passcode that is present on the token.
- **USB token**. A small USB key contains a digital certificate or other information. The token must be inserted into a USB port on the workstation to permit the user to log on. The user is still required to furnish a userid and password.

The distinct advantage of two-factor authentication is the additional difficulty presented to an intruder who wishes to enter a system through the "front door". There are also some disadvantages of two-factor authentication that organizations need to consider, including:

- **Implementation cost**. The costs associated with implementing two-factor authentication are considerably greater than userid-and-password solutions. Additional costs include:
  - Tokens, smart cards, or other hardware
  - Hardware to support the two-factor hardware (e.g., smart card readers)
  - Software license fees
  - Time and effort to provision and train each user
- **Increased support cost**. Until they are used to their operation, users will call with questions when they have difficulty logging in.
- **Lost devices**. Devices may be lost and will need to be replaced. This will be logistically more challenging when users are located in remote places.

These costs all need to be factored in, so that an organization that is considering two-factor authentication will have more realistic expectations and a higher satisfaction rate for management and users.

Biometric Authentication Organizations that are not satisfied with the additional security afforded by two-factor authentication may consider biometric authentication, which is often called *biometrics*. Biometrics, which are also considered a form of two-factor or strong authentication, measure a physical or physiological characteristic of the end user in order to identify whether the person requesting entry to an information system or facility is who they claim to be.

There are several forms of biometrics, including:

- **Fingerprint reader**. Reads a user's fingerprint.
- **Palm scan**. Reads the geometry of a user's entire hand, primarily the angle and length of the fingers.
- **Iris scan**. Reads the image of a user's iris.
- **Facial scan**. Reads key geometric dimensions of a user's face, primarily the position of facial bones.
- **Handwriting (signature) scan**. There are several forms of handwriting biometrics, including a) recognition of the signature image, b) measurement of the pen motions used to write a signature, and c) measurement of the pressure of a stylus pressure on a writing pad when a user writes his or her signature.
- **Voice recognition**. Measurement of a user's voice patterns.

The single greatest advantage of biometrics is that while an intruder can obtain a user's userid and password, and even a two-factor authentication device, it is exceedingly difficult for an intruder to obtain or impersonate a physical or physiological characteristic of any particular user.

Still, there are some disadvantages and challenges associated with the use of biometrics, including:

- **Costs for implementation and maintenance**. Biometric systems are often complex and have capital costs, implementation costs, and ongoing costs associated with them. These need to be taken into account to ensure that the organization is not spending $100,000 to protect a $10,000 asset.
- **Gradual changes in users' characteristics**. No matter what biometric methods are used, it's an accepted fact that the measured characteristics change slowly over time. For instance, a person's signature and voice change over time, as do iris scans.
- **Sudden changes in users' characteristics**. A user with a head cold may register differently in a voice recognition system. A home DIY project may scuff up a user's hands enough to foil a fingerprint reader.
- **False readings**. This is explained below.

Biometric systems are known to sometimes reject valid users and sometimes accept invalid users. The formal terms for these are:

- **False Reject Rate (FRR)**. This is how often a biometric system will reject a valid user.
- **False Accept Rate (FAR)**. This is how often a biometric system will accept an invalid user.

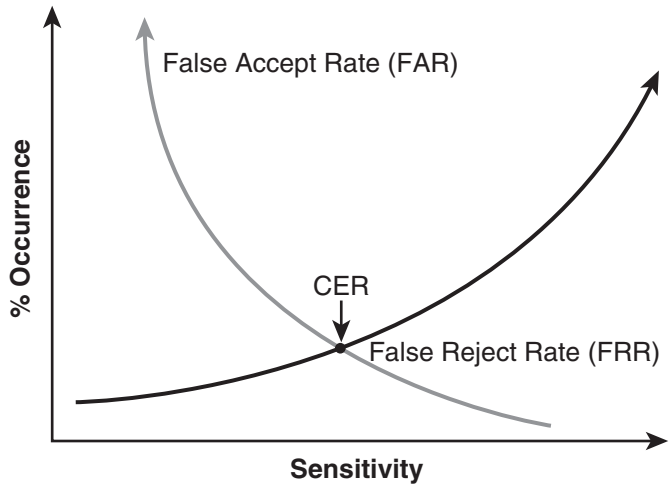


Figure 2-2 Biometric crossover error rate

Source: Course Technology/Cengage Learning

- **Crossover Error Rate (CER)**. This is the point where the False Reject Rate and the False Accept Rate are equal. The smaller the CER, the more accurate and reliable the biometric system will be.

The relationships of FRR, FAR, CER, and sensitivity are illustrated in Figure 2-2.

When tuning a biometric system, the error rate must be as low as possible in order to ensure reliability and usability. If the error rate is too high, users of the system will complain and attempt to bypass or manipulate the system.

Authentication Issues Authentication systems request identifying information from users in order to permit access to legitimate users and deny access to invalid users. Authentication systems don't always work right, and users don't always operate them correctly. In short, things can and do go wrong. Some of the significant issues include:

- **Password quality**. Each organization needs to establish standards for password quality. Passwords need to be complex enough to prevent password attacks, but not so complex that users resort to writing down passwords and leave them where they are easily discovered.
- **Forgotten credentials**. Users sometimes forget their userids and passwords. There needs to be some way for users to recover or reset these items so that they can access the systems they need.
- **Compromised credentials**. Organizations need a way to know when a user's credentials have been compromised (that is, exposed to any third party, which greatly increases the risk of unauthorized entry) and be able to quickly reset credentials or temporarily restrict the compromised user's access to systems.
- **Staff terminations**. Regardless of the circumstances related to a user's termination from an organization, those users' credentials must be quickly rescinded so that the user may no longer access systems and information.

These and other issues present themselves in every environment where authentication is required to access information.

Access Control Technologies and Methods

Several technologies and methods are in more-or-less common use for authenticating users to systems and applications. Authentication is such a common feature in information systems that virtually no one tries to invent a technology any more, but instead supports one or more of the standard technologies and methods that are already available. Those that are discussed in this chapter are:

- LDAP
- Active Directory
- RADIUS
- Diameter
- TACACS
- Kerberos
- Single Sign-On
- Reduced Sign-On

LDAP Lightweight Directory Access Protocol, commonly known as **LDAP** (and pronounced "el-dap"), is an open standard that is defined in **RFC** 4510 (RFC's, or "Request for Comments" are the documents that describe the Internet's technical and procedural standards).

LDAP is a TCP/IP-based communications protocol that is used for various directory purposes, including authentication. LDAP is also a data storage model that provides specific methods for storing directory-type information. Because it is an open standard, LDAP is very popular and is the basis for a number of commercial products, including Microsoft **Active Directory**. Other commercial LDAP server products include:

- Apache Directory Server
- Apple Open Directory
- Fedora Directory Server
- IBM Tivoli Directory Server
- Novell eDirectory
- OpenDS
- OpenLDAP
- Oracle Internet Directory
- Penrose
- SIDVault
- Sun Java Directory Server

Active Directory Microsoft Active Directory is a commercial implementation of LDAP. "AD," as it is commonly called, is built into Microsoft server operating systems and is tightly coupled with Microsoft's workstation and domain authentication and also Exchange e-mail.

RADIUS The Remote Authentication Dial In User Service, or **RADIUS**, is an authentication protocol that traces its origins to dial-up remote access. Another popular use for RADIUS is centralized control of authentication for network devices such as routers.

RADIUS is described in RFCs 2865 and 2866.

Like LDAP, there are many open source and commercial implementations of RADIUS servers available.

Diameter **Diameter** is an authentication protocol similar to RADIUS. The name is a pun on RADIUS (in geometry, a circle's diameter is twice the radius) and provides an upgrade path for RADIUS. Diameter has several advantages over RADIUS, including:

- Diameter uses the more reliable TCP protocol instead of UDP
- A diameter session can be encrypted with SSL (TLS)

Diameter is described in RFC 3588.

TACACS **Terminal Access Controller Access-Control System (TACACS, pronounced "tack-acks")** is a remote access authentication protocol that permits a device to communicate to a central authentication server to determine whether a user should be permitted to log on to the device. TACACS is defined in RFC 1492.

TACACS has been largely replaced by TACACS+ and RADIUS. An RFC draft has been developed for TACACS+.

Kerberos **Kerberos** is a standard protocol that provides for mutual authentication (an end user and a Kerberos server authenticate each other) over a non-secure network. There are several components in a Kerberos environment:

- Client—the workstation (usually) that desires to access systems or services
- AS (authentication server)—a centralized system to which a user initially authenticates
- TGS (ticket granting server)—a centralized system that issues tickets
- SS (service server)—a server that provides some useful service
- TGT (ticket granting ticket)—a token that permits access to a SS
- ST (service ticket)—an encrypted key

When a user wishes to log on to the network and access a service or application, the following steps are performed:

1. The client authenticates to the AS. This creates a user session that will expire, typically in 8 hours.
2. The AS sends a TGT back to the client system.
3. The client sends the TGT to the TGS to get authenticated.

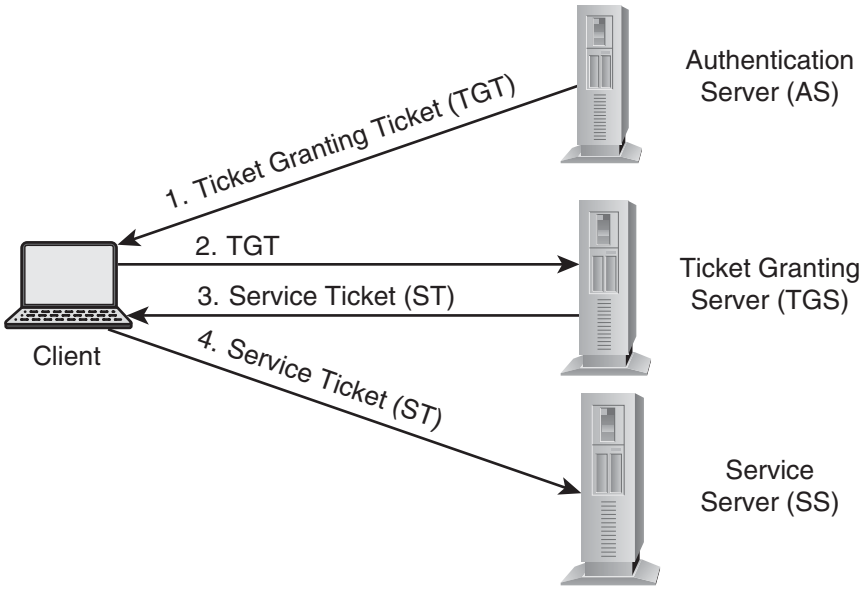


Figure 2-3 Kerberos authentication components

Source: Course Technology/Cengage Learning

4. The TGS creates an encrypted key with an expiration time and sends it to the client.
5. The client sends the ST to a SS that the user wishes to access.
6. The SS confirms that the ST is still valid (by checking the expiration time). If the ST is valid, communication is established between the client and the server (SS).

The components that participate in Kerberos authentication are shown in Figure 2-3.

Single Sign-On **Single sign-on**, or SSO, is an access control method whereby a user can authenticate once and be able to access many different information systems without having to re-authenticate into each one.

In SSO, applications and systems are logically connected to a centralized authentication service that controls user authentication. When a user first logs in to an application, they will be required to provide a userid and password (or two-factor or biometric or whatever happens to be required). The application—and the centralized service—will recognize the user as being logged in. Later, when the user wishes to access a different application or system, the user's logged-in state will be recognized and directly admitted to the application.

The advantage of SSO is the convenience of eliminating many redundant logins for busy end users, and the centralized management of access for many applications and systems. A distinct disadvantage of SSO is that a user's compromised login credentials means that an intruder will have access to all of the applications and systems that the user also has.

Reduced Sign-On SSO is similar to **reduced sign-on**, an authentication method where many applications and systems in an organization will utilize a centralized user management

service such as LDAP or Active Directory. However, applications and the centralized service will not manage the logged-in state, which means that users will have to log in to each application and system using their single userid and password.

Access Control Attacks

Several methods can be used to attack a system's access control mechanism as a means for gaining access to the system. Usually the motivation for such an attack is to steal information, alter information, or gain access to functions. Persons who desire to launch an attack do not possess a working userid and password, so they must resort to an attack in order to access the desired information or function. The types of attacks include:

- Buffer overflow
- Script injection
- Data remanence
- Denial of Service
- Dumpster diving
- Eavesdropping
- Emanations
- Spoofing and masquerading
- Social engineering
- Phishing, spear phishing, and whaling
- Pharming
- Password guessing
- Password cracking
- Malicious code

Buffer Overflow

A **buffer overflow** attack is an attempt to cause a malfunction of an application by sending more data to a program than it was designed to handle properly, causing the program to malfunction or abort. If a program does not properly check input data, a too-long input string can fill the input buffer and overwrite other memory locations in the program.

Sometimes it is possible to insert specially crafted computer instructions into an input string that the program will begin to execute. This can cause the program to begin executing instructions of the attacker's choosing, which can result in a devastating malfunction or security breach.

Buffer overflows are easily prevented by having all programs properly set up input variables and by limiting their bounds when they accept input. But much software was written in an era prior to buffer overflow being a serious threat, and much of this older software is still in circulation today.

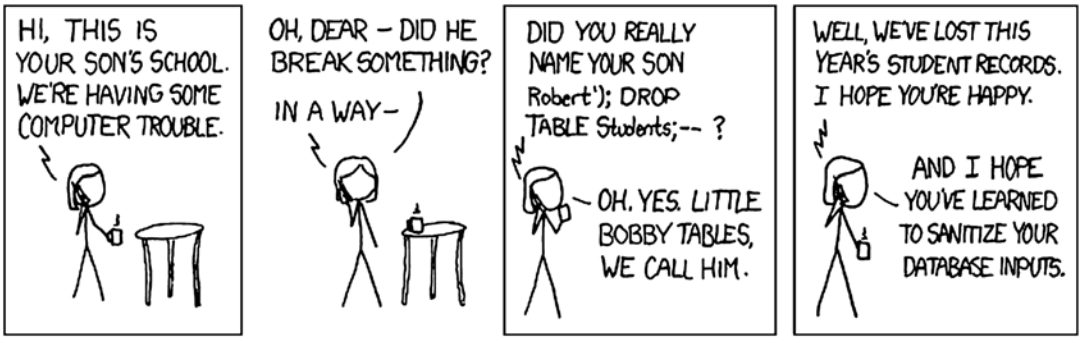


Figure 2-4 A SQL injection illustration

Source: Image courtesy xkcd.com

Script Injection

A **script injection** attack (also known as *code injection*) is similar to a buffer overflow attack. Script injection occurs when software programs do not parse input data for script commands, and they inadvertently execute the script commands in subsequent processing steps.

A common form of script injection is known as **SQL Injection**, whereby specially crafted SQL statements can be inserted into an input field, causing the database server on the back-end to execute the injected SQL statements. This is illustrated in a comic in Figure 2-4.

Like buffer overflow, script injection is an easily prevented attack, and yet there is much online software that does not properly detect and block attempts at script injection.

Data Remanence

Data remanence refers to data that remains on a storage device, often unintentionally. Data can remain on a device even after a user "removes" the data. This data can fall into the hands of others, sometimes to the detriment of the original owner of the data.

A typical scenario is a company or individual who sells their computer to another party, who then discovers the prior owner's data still on the hard drive.

Some examples of data remanence include:

- **Deleted hard drive files.** Deleting files does not actually remove them, but only "dereferences" them. Tools are available to easily recover these files, often in their entirety.
- **Data on slack space.** Slack space is the space on a hard drive between the end of the file and the end of the disk sector used by the file.
- **Erased hard drive files.** Even if tools are used to erase files, it may still be possible to recover them.
- **Formatted hard drive.** Formatting a hard drive does not erase old data files. Tools are available to easily recover many files on a formatted hard drive.
- **Discarded CDs, floppy discs, and backup tapes.** Important data can be present on other types of discarded media such as those shown here.

Denial of Service

An attack that disables a service or makes it unreachable to its users is a **Denial of Service (DoS)** attack. There are two primary ways of carrying out a DoS attack:

- Sending a flood of messages to a service that is so heavy that legitimate use of the service is all but impossible. This is usually achieved by sending a high volume of messages over a prolonged period of time. This type of attack can sometimes result in malfunctions of an application's operating system.
- Sending specially crafted messages that cause the application or service to malfunction or abort, making it unavailable for legitimate users.

A **Distributed Denial of Service (DDoS)** attack is an attack launched from many places at once. The objective of a DDoS attack is to incapacitate a system or service in a way that is difficult to block. A DoS attack that originates from a single system is easy to block by configuring a router to drop packets from the attacking system. However, a DDoS attack can originate from thousands of systems, making it virtually impossible to block by any normal means.

Dumpster Diving

Some organizations are not careful about the printed matter that they discard. They throw documents containing sensitive information into recycling or trash bins. Someone who attempts to find discarded documents in the trash is **dumpster diving**.

In many jurisdictions, it is not illegal to rummage through someone else's garbage. Illegal or not, it is not a good practice to discard sensitive information into recycling or trash bins. Instead, documents with sensitive information should be shredded.

Eavesdropping

Eavesdropping takes many forms, but the effect is the same: people who desire sensitive information will attempt to obtain it by observing communications. Eavesdropping takes many forms, including:

- **Network sniffing**. An intruder (who could be an employee or an outsider who has gained access to an internal system by some nefarious means) can start a network sniffing program on a computer that will enable the capture and storage of all network traffic. Depending upon the architecture and technologies used in the network, an intruder can capture quite a lot of network traffic and possibly harvest some sensitive information that could be contained in e-mails, web browsing sessions, file transfers, and so on. Some older protocols such as TELNET and FTP do not encrypt userids and passwords as they traverse the network, which makes them especially vulnerable to sniffing.
- **Wireless network sniffing**. Many public WiFi hotspots employ no encryption, which means that all WiFi network traffic is being transmitted "in the clear," making it easy for an eavesdropper to capture and record for later analysis and use. A growing segment of the workforce is mobile and workers often "hang out" at cafes and other venues with WiFi connectivity, much of which is unprotected.
- **Shoulder surfing**. Someone who uses a laptop computer in a public location such as a restaurant, café, airport, train, or airplane is potentially exposing sensitive information

on the screen to anyone who can see it. It is also easy to observe someone's typing, especially when they are typing in a password. If the user is using a complex password, they might be typing it more slowly, which can make it even easier for an observer to view.

- **Mobile calls and conversations in public places**. Some people have a naturally loud voice, making it easy for anyone nearby to overhear a conversation that may be sensitive in nature. Someone who wants to learn more about a big company just needs to hang out at a nearby coffee shop or restaurant to overhear conversations by people who are unaware that outsiders may be listening.

Emanations

Computer and network hardware devices employ high–speed electronics that can emanate electromagnetic radiation (EMR). Sometimes these **emanations** contain data that can be sensitive in nature. Two examples of EMR emanations are:

- **Computer monitors**. The older CRT-type monitors can emit EMR containing information about what is being displayed on the monitor.
- **Network cabling**. Faulty or improperly terminated network cabling, particularly the coaxial type of cabling, can sometimes act like an antenna, broadcasting whatever data is being transmitted over the network.

TEMPEST is a code name for a U.S. military project dedicated to the study of **compromising emanations** (**CE**). The U.S. Army, the NSA, and agencies in other NATO countries have laboratories and certifications that are used to test systems to ensure that they do not emit compromising emanations that could result in the compromise of military secrets.

Spoofing and Masquerading

An attack can be successful if the attacker pretends to be someone (or some*thing*) they are not. Weaknesses in the TCP/IP protocol make it fairly easy for a system to create messages that claim to be originating from any IP address. This **spoofing** can fool the target system into thinking that the messages are originating from a trusted system instead of from an untrusted system.

Network routers can be configured to repel some of these attacks by rejecting incoming messages that claim to be originating from inside the trusted network. Firewalls also help to mitigate this threat.

Because TCP/IP permits the creation of messages that claim to be originating from any IP address, systems should not authenticate incoming messages based only on its IP address. Instead, systems should use additional means for authenticating incoming messages to make sure that they are genuine.

Spoofing can take many other forms besides that of falsifying source IP addresses. An intruder can attempt to break in to a web application by stealing cookies from legitimate users. Stealing cookies is not particularly easy, but there have been vulnerabilities in Microsoft Internet Explorer and Firefox that make end user workstations vulnerable to cookie theft.

Social Engineering

Many would-be intruders are skilled at **social engineering**, a deceptive method of communicating with others by pretending to be fellow employees or business partners in need of some help. Because of humans' natural desire to help others (either for the intrinsic value of helping or from the good feeling that comes from helping another person in need), employees can sometimes easily be convinced that the stranger who is attempting to gather intelligence is actually a fellow colleague who needs assistance.

A social engineer may opt to make several contacts into an organization and get small bits of information from each person. One such social engineering scenario can go something like this:

1. The social engineer calls an IT employee, claiming to be another employee on travel, and asks for the URL for the VPN (remote access) server or external employee portal.
2. The social engineer calls another employee and asks for the e-mail address of a targeted employee. The intruder assumes that the part of the e-mail address preceding the '@' is the user's userid.
3. The social engineer calls another employee and asks for the targeted employee's cube number; he claims to have forgotten his cube number, and because he's on travel, he can't just get up and look.
4. The social engineer calls another employee and asks for the phone number for the IT helpdesk.
5. The social engineer calls the helpdesk, claiming to be the targeted employee (from step #2). He correctly identifies himself by providing his cube number. The social engineer claims to have forgotten his password and requests a password reset. He claims to be the targeted employee out on business travel in urgent need of information on a file server, and therefore cannot go through a typical password reset. He needs to have the new password so that he can log in to the VPN or external portal. Wanting to be the hero who helped, the helpdesk person complies and provides the password. If he's particularly brazen, the social engineer might even verify the userid.

The information that the social engineer/intruder obtained from five people in a short space of time was enough for him to log on to the company VPN and then go anywhere inside the network where the real employee was allowed to go. The intruder could read and send e-mail messages on behalf of the targeted person, and access file servers to harvest vast amounts of sensitive information.

Another form of social engineering involves incoming e-mail and is described in the next section.

Phishing

A spammer's frequent ruse is a **phishing** attack, which is the creation of forged e-mails that appear to have originated from a financial institution or other high-value organization. The forged e-mail will contain instructions that direct the recipient to click on a link and provide information on a form. The victim is led to believe that he or she is helping the institution by verifying their sensitive credentials, when in reality they are handing those credentials over to a criminal. Figure 2-5 shows a typical spam e-mail that attempts to lure users to a phishing site.

From: Internal Revenue Service (info@irs.gov)
To: xxxxxxxxxxxxxx
Date: Friday, December 7, 2007 2:30:53 AM
Subject: IRS Notification Tax refund

Internal Revenue Service
United States Department of the Treasury

Tax Notification

Internal Revenue Service (IRS)
United States Department of the Treasury

Date: 11/24/2007

After the last annual calculations of your fiscal activity we have determined that you are eligible to receive a tax refund of **$134.80.**

Please submit the tax refund request and allow us 6–9 days in order to process it.

A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, Click here.

Regards,
Internal Revenue Service

Document Reference: (92054568).

Figure 2-5 Spam message that lures unsuspecting users to a phishing site

Source: Course Technology/Cengage Learning

Spear phishing is a form of phishing where the attacker targets specific users or groups of users in phishing scams. **Whaling** is another form of phishing where attackers target top executives in an organization and attempt to lure them to fake web sites to harvest sensitive information.

Pharming

In a **pharming** attack, an attacker directs traffic destined for a specific web site to an imposter site, usually for the purpose of harvesting logon credentials from unsuspecting users. The attack is directed either at a DNS server, by exploiting one of several known vulnerabilities that permit the attacker to "poison" the DNS server with data that directs users to the imposter site. The attacker can also attack users' systems by planting a fraudulent entry in the system's *hosts* file.

Password Guessing

A common form of attack against an information system is an attempt to guess someone's legitimate logon credentials through a technique called **password guessing**. An intruder knows that easy entry to an information system is often no more difficult than the right combination of userid and password. There are a number of methods that an intruder may use, including:

- **Guessing**. The intruder may use a *dictionary attack*, where the most common passwords are tried, to see if the intruder can get lucky and gain entry into a target system. If the intruder is attempting to gain entry using a specific person's userid, the intruder can try and find out personal information about that person such as birthdate, pet's name, partner's name, and try combinations of these to gain entry to a system.
- **Brute force**. In a brute force attack, an intruder will try many passwords in hopes that one of them will work. A brute force attack typically consists of sequential guesses at a password until the correct value is found. This type of attack can take a long time, since there can be millions of possible passwords for a given user account.

Information systems now typically lock a user account after several unsuccessful attempts have been made to log in. This type of control helps to hinder password guessing attacks by severely limiting the number of guesses that an intruder may use before the user account is locked.

Password Cracking

If an intruder is able to access the hashed passwords on a system, then the intruder may resort to **password cracking** to obtain those passwords. The intruder who is able to obtain encrypted passwords must then programmatically hash every possible combination of characters until the hashed value from his guessed password matches the hashed passwords he obtained.

An advantage (from the intruder's point of view) of this type of attack is that the intruder can perform this password cracking on his own system. And while password cracking is resource intensive, it requires no resources on the target system and hence should not raise any alarms (associated with resource consumption) on the target system. When the intruder has successfully cracked a password, he can then easily use them to log on to the target system without any incorrect guesses that would otherwise result in a locked account.

Tools that are used for password cracking include *crack*, *L0phtcrack*, and *John the Ripper*. These tools are free and reliable.

Malicious Code

Malicious code—also known as *malware*—started with the ©Brain virus in 1985 and has taken on a life of its own in the years since. More often, malicious code is designed to exploit vulnerabilities in information system software, not for its own sake, but to achieve some objective such as stealing information or installing bot software that is used to remotely control the system later on.

There are several different forms of malicious code in circulation, including:

- **Viruses**. The original malware—viruses embed themselves in an .exe file and hide there until the user runs the .exe file, activating the virus code. Once active, the virus can attach itself to other .exe files and perform other interesting and harmful tricks on an end-user's system.
- **Worms**. A worm does not embed itself in an .exe file but instead exists as one or more separate, independent programs. Many worms can replicate automatically without human intervention, which has led to some worms infecting hundreds of thousands of systems within minutes of release.
- **Trojan horses**. *Click here for your income tax refund*. That is a common ploy that is used by virus writers to trick unsuspecting victims into running their malicious programs.

In the 1980s when viruses first became active, they most often circulated via floppy diskettes when users exchanged information with each other. In the 1990s, e-mail became the new preferred mode of travel, and some malicious code known as mass-mailing worms actively exploited e-mail programs to propagate themselves to all recipients in users' address books. Spam is another prevalent means for propagating malicious code.

While malicious code still propagates via .exe files and e-mail, most malicious code is transported via web browsers. Vulnerabilities in web browser programs and end-user operating systems has given rise to a wave of web sites with built-in malicious code that is downloaded to unsuspecting victims who visit those sites.

Malicious code is developed to spread via image files, flash movies, PDF files, Zip archives, macros in Office documents, instant messaging programs, and mobile devices. It seems as though every new type of device or communication technology is soon desecrated by malicious code that either exploits weaknesses in those technologies or simply uses them to move around.

Access Control Concepts

Many terms and models are used to describe and classify access control. This section contains principles, types, and categories of controls.

Principles of Access Control

We need to step back and take a look at the big picture with regards to access control and authentication. The issue at stake is, *who is permitted access to which systems, data, and functions?* This is not so much a question about technology, but policy. Deciding which

persons have access to what systems, data, and functions should be a business policy. Then the technology should be designed, configured, and operated to support that policy.

Two important principles of access control are *separation of duties* and *least privilege*.

Separation of Duties The principle of **separation of duties** (which is sometimes known as segregation of duties) states that no single individual should have so many privileges that he or she is able to complete important technical or business functions on their own.

When a single individual is able to perform some important business functions, there is a potential for fraud or abuse. These functions should be divided into individual tasks that should be performed by separate individuals or groups.

Some examples of functions that should be divided are:

- **Financial payments**. In an accounting department, the functions of creating a new payee, requesting a payment, and making a payment should be done by separate individuals. The separation of duties in this case will reduce the likelihood of fraudulent payments perpetrated by an accounting department employee.
- **Software changes**. Any change to software code should be formally requested by one individual, performed by another person, verified through a code review by another person, and tested by yet another person. The separation of duties here will reduce the chances of unauthorized code being released.
- **Creation of a computer user accounts**. The functions of requesting a computer account, approval, and creation of a computer account should be performed by separate persons. The separation of duties in this example will reduce the chances of the creation of inappropriate user accounts. There should be additional approvals required for privileged or administrative accounts such as those used by system administrators or database administrators.

Least Privilege The principle of **least privilege** states that any individual should have access to *only* the systems, data, and functions that they *require* to perform their stated duties.

Least Privilege and Server Applications Least privilege does not apply just to people. Applications and service processes on a system should never be configured to run at root or administrative level, but instead at the lowest privilege possible. The primary reason for this is that an application malfunction or misconfiguration could harm the entire system if the application runs as root or administrator. But if an application is configured to run as a non-privileged user, then the application cannot harm the operating system or other users on the system.

User Permissions on File Servers and Applications Probably the most useful context to view least privilege is a workplace file server. Typically a file server is used to share files and directories among groups of users. It may be tempting to give all users access to all directories—this approach would incur almost zero overhead on system administrators, but this would be a blatant violation of least privilege.

Another approach to use is to give users access to nothing on the file server, and then add whatever specific accesses they may require. This would support the concept of least privilege,

although this approach would incur a lot of support overhead, since every time a user needed access to some other file or directory, they would have to ask someone to permit this access.

Least Privilege on Workstations Another situation where least privilege is vitally important is end-user workstations. Many versions of Microsoft Windows are configured for ordinary users to run with administrative privileges. This can result in great harm to the operating system if the user makes an error or downloads and activates malware. The impact of user errors and malware is much more limited if the user is not running in administrative mode.

Non-repudiation is a concept that is related to access control. Non-repudiation is discussed fully in Chapter 5, "Cryptography."

Types of Controls

From a "big picture" perspective, controls that govern access and operation of information systems are classified into three types: technical, physical, and administrative. A **control** is an activity, process, or apparatus that ensures the confidentiality, integrity, or availability of an asset. Each is explained here.

Technical Controls **Technical controls**, which are sometimes called **logical controls**, are the programs and mechanisms on information systems that control system behavior, and user access. Some examples of technical controls are:

- **Authentication**. Information systems utilize authentication to control which users are permitted to access data or functions.
- **Access control list** (**ACL**). These control user or system access to files, networks, applications, or systems.
- **Firewall**. This is a network-level device placed at a network boundary that blocks unwanted network traffic.
- **Remote access**. Used to facilitate access to a system or application from a remote location.
- **Anti-virus and anti-spyware**. This software is used to detect and block malicious and unwanted software from being installed on a system.
- **Encryption**. The practice of scrambling information so that it can only be read by authorized parties.
- **Configuration management**. A software application that is used to monitor and manage the configuration of systems and/or applications in an environment.

Physical Controls **Physical controls** are used to manage physical access to information systems such as application servers and network devices. Some examples of physical controls include:

- **Video surveillance**. A detective control used to observe the movements of people and equipment in various places.
- **Key card access control**. A preventive control that limits which personnel are permitted to access a building and/or various areas or zones within the building. It is also a detective control, as most key card systems also record all attempted (whether successful or unsuccessful) entries.

- **"No Trespassing" signs**. A deterrent control that notifies persons that unauthorized persons should not enter a facility.
- **Fencing**. A preventive control that restricts peoples' movements.

Administrative Controls **Administrative controls** represent a broad set of actions, policies, procedures, and standards put in place in an organization to govern the actions of people and information systems. Some examples of administrative controls include:

- **Policies**. These are the high-level statements made and communicated by the organization's management that say, in effect, *this is how we are going to run this organization*. Some of the policies that would be in place include:
  - Security policies
  - Acceptable use policies
- **Processes and procedures**. Critical business activities that are documented and managed include user access administration, change control, configuration management, new employee hiring, vulnerability management, and service continuity management.
- **Standards**. These are the formal statements that specify what suppliers, makes and models of products, system configurations, etc. will be used in an organization. Standards state, *this is* how *we will do things in this organization*.

Categories of Controls

When you design or work with an information system, you will need to know how access to the information system is controlled. The six categories of controls that are used to protect information are:

- Detective
- Deterrent
- Preventive
- Corrective
- Recovery
- Compensating

Associating activities with one of these six categories of controls is not always an exact science. Some controls can be both preventive and deterrent, for instance.

Detective Controls **Detective controls** are these mechanisms that record events that occur. Detective controls are entirely *passive*—they *detect,* but do nothing else. They do not prevent unwanted events from occurring, although they may be aware of them.

Examples of detective controls include:

- **Video surveillance**. Cameras can be placed in key locations such as building entrances and locations where high-value activities take place such as bank vaults, gold refineries, and data processing centers. When connected to recording equipment, whatever happens within the view of surveillance cameras is recorded and archived for a period of time ranging from a few days to several years.

- **Access logs**. Information systems usually record events such as users logging in. Systems also usually record unsuccessful logins, which can be a sign of attempted intrusions by unauthorized parties who are trying to guess a user's password.
- **Transaction logs**. In addition to recording logins, information systems often record actions performed by users. These can range from making adjustments in a financial ledger to creating new user accounts. An action that is captured in a transaction log can also include when a user merely accesses information, such as a customer profile that includes sensitive information such as health or financial details.
- **Intrusion detection systems (IDS)**. An IDS monitors activities and is designed to recognize unwanted activities that may be signs of an intrusion. There are two types of IDS: network-based IDS (NIDS) and host-based IDS (HIDS). NIDS systems monitor network traffic and generate alerts when unwanted or unusual network traffic is seen. HIDS are usually software programs that run on servers and monitor network traffic going to and from the server, as well as other activities on the server.

Detective controls are only effective if the controls are monitored. This is because detective controls only record accesses; they do not block unwanted accesses.

There are situations where implementing a preventive control is not feasible. In such a situation, a detective control should be implemented, so that it will be possible to at least record unwanted accesses.

Deterrent Controls

Deterrent controls are designed to be highly visible and give persons the impression that any unauthorized activities will be stopped and/or persons apprehended. Deterrent controls are designed to prevent an individual from attempting to trespass, steal, destroy, or cause any other unwanted event.

Deterrent controls may consist of signs that alert persons of controls (which may or may not actually exist), or of detective or preventive controls that are deliberately made visible to onlookers.

Some examples of deterrent controls include:

- **Signs**. From "No Trespassing" to "These premises are under video surveillance" to "Beware of guard dogs," signs send a clear message to would-be troublemaker that he or she is likely to be caught or their activities blocked in some manner.
- **Guards**. The presence of security personnel can be an effective deterrent, particularly if they are armed.
- **Guard dogs**. Often used to protect facilities from intruders.
- **Visible surveillance cameras and monitors**. Cameras and monitors that are placed out in the open say, "We are watching you and we may also be recording you."
- **Barbed wire and razor wire**. Those sharp edges often dissuade even a physically fit person from wanting to scale a fence, because of the fear of injury.

Controls that are labeled as deterrent are usually also preventive or detective, as deterrent controls often perform real actions. But an example of a *purely* deterrent control would be a sign that warns of guard dogs when no guard dogs actually exist.

Preventive Controls **Preventive controls** are designed to prevent unwanted activities. These controls are usually preferred over detective controls, since they are designed to prevent unwanted events from occurring in the first place. A prevented event is far easier to deal with than a detected event.

Preventive controls may prevent all persons from performing an activity, or they may prevent only unauthorized persons from performing unwanted actions. In a pure sense, a preventive control may absolutely prevent unwanted activity, or it may make the activity much more difficult to perform. A few types of preventive controls include:

- **Firewalls**. These devices block unwanted network traffic by examining each incoming packet and making a block-or-pass decision, based upon a set of rules that are configured by a network administrator.
- **Anti-Virus software**. Programs on a PC or server that are designed to watch for specific known viruses and other malware, and block the entry of these unwanted programs. Anti-virus programs recognize viruses through the use of "signatures", where the virus is recognized and blocked. Anti-virus programs also utilize a mechanism known as *heuristics* where the anti-virus program detects a virus through its behavior.
- **Anti-Spyware software**. Similar to anti-virus software, anti-spyware blocks spyware and other unwanted programs through signatures and heuristics.
- **Encryption**. Files, directories, entire volumes, and backup tapes can be encrypted to protect sensitive information from disclosure to unauthorized parties.
- **Intrusion Prevention System (IPS)**. These devices listen to network traffic, watching for specific patterns and anomalies, and then block traffic directly or by instructing a network device such as a switch or firewall to block specific traffic. Like anti-virus software, IPS's watch for traffic that matches specific signatures, and also make blocking decisions by observing behavior using a mechanism known as *heuristics*.
- **Fencing**. Physical fences prevent unwanted persons from trespassing on a protected facility.
- **Bollards**. These are the heavy rigid posts that prevent motor vehicles from entering a protected area. Figure 2-6 shows bollards protecting the entrance of an office building.

Corrective Controls **Corrective controls** are events that occur after a security event has occurred. Generally, corrective controls are those activities that are undertaken in order to prevent the recurrence of an unwanted event.

Here is an example. A recently-terminated employee who was unhappy about his unemployment decided to sabotage his former employer's information systems. He was able to log on to these systems remotely because his logon credentials had not yet been removed. The organization discovered this and made some improvements in the termination process in order to ensure that terminated employees' logon credentials are immediately removed. These process improvements are the corrective actions in this case.

Recovery Controls Like corrective controls, **recovery controls** take place after an incident has occurred. Recovery controls are activities that enable the restoration to normal operations after some event.

Figure 2-6 Bollards control motor vehicle traffic and block entry to protected areas

Photo by Rebecca Steele

An example of a recovery control is the restoration of system files after a virus infection that corrupted critical system data.

Compensating Controls Sometimes a system may lack certain capabilities that make it difficult or impossible to enact specific controls. In order to compensate for the missing or deficient control, another control can be introduced to manage the risk. Such a substitute control is called a **compensating control**, because it compensates for the lack, or failure, of another control.

Using a Defense in Depth Control Strategy

To reduce the risk of unauthorized access, it is recommended that several controls be put into place to protect an asset. The existence of several layers of controls increases the likelihood that an asset will not be compromised, than if there was only one control protecting the asset. The practice of using several controls to protect an asset is known as defense in depth.

The advantage of a defense in depth strategy is that a malfunction, defect, or compromise of a single control does not completely compromise the protection of the asset. The other controls that are still in place contribute to the protection of the asset.

In order to be most effective, a defense in depth strategy should employ various types of controls, perhaps from two or more vendors. This will result in the greatest protection from compromise. For example, if a database is protected by several layers of firewalls of the same type, a failure or compromise in one layer may render all layers vulnerable to compromise.

Example 1: Protected Application A financial institution wishes to protect its online customer financial data from unauthorized access, while still providing access to authorized customers. The financial data is protected through an architecture that provides for several layers of controls in order to provide the greatest possible protection. The security features of this architecture could include the following:

- Authentication that requires a user name, strong password, and account number.
- Entire user session protected with 128-bit SSL (TLS) encryption.
- Access permitted only from previously-registered workstations.
- Session timeout that requires re-authentication by the user.
- Removal of all unnecessary services on all servers in the environment.
- Up-to-date security patches on all servers.
- Up-to-date anti-virus software on all servers.
- Intrusion detection systems in one or more places in the application environment.
- Three-layer application architecture with web servers on the front end, application servers in the middle tier, and database servers in the third tier.
- Different brands of firewalls at the first, second, and third tiers of the environment.
- Two-factor authentication required for all administrative access to devices, servers, operating systems, and databases.
- Application servers permit connections only from front-end web servers. Database servers permit connections only from application servers.
- Encryption of sensitive data on databases.

While this may sound like a long list of controls, most environments will employ many more than are listed here.

It may be evident to the reader that the controls in this example protect the sensitive data from more than one type of threat. It is necessary to understand all types of threats and vulnerabilities and to implement controls to address each one.

Example 2: Protected Facility The research and development division of a large manufacturing company wishes to protect its research and development facilities from unwanted access. The company operates in a highly competitive market that has experienced espionage incidents by competitors and foreign government agents. The organization employs several methods to prevent and detect access by unauthorized persons, including:

- Security cameras connected to a manned surveillance center
- Fences with barbed wire
- Guard dogs and security guards patrolling the grounds
- Checkpoint that challenges all incoming vehicles

- Bollards that prevent vehicles from entering restricted areas
- Entry doors require key card and biometric hand scan
- Zones of security within the facility that restrict different classes of employees to different areas in the facility
- Security guards within the facility

Like the preceding example, this organization probably employs additional means for protecting the facility.

Testing Access Controls

Because access controls are so vital to the confidentiality and integrity of information, they should be tested in order to be sure that they are working properly and free of defects. The two types of testing that can be performed on a system are penetration testing and application vulnerability testing. The purpose of these two types of testing is to discover vulnerabilities that could be exploited by an attacker to gain unauthorized access to a system.

In addition to testing, access controls on live systems typically create audit log entries to record significant events.

Penetration Testing

Penetration testing, often coined "pen testing", is a procedure that is used to discover defects at the operating system or server level. Tools that are specifically designed for pen testing are used to scan one or more target systems in order to discover open ports that may indicate the presence of vulnerabilities. The scanning consists of transmitting TCP/IP packets to the target system in attempts to communicate with various common (and not-so-common) services, in order to discover which services are operating on the target system.

Tools make pen testing a lot easier by automating the scanning and analysis of scan results. Some of the tools in common use include:

- Nessus
- Nikto
- GFI LANguard
- Superscan
- Retina
- ISS Scanner
- Qualysguard
- Microsoft Baseline Security Analyzer

These and other tools can find vulnerabilities of many varieties, including:

- Missing patches
- Old versions of services
- Misconfigured services

Many of these and other vulnerabilities are easily exploited by intruders who wish to gain access to vulnerable systems, particularly for systems that are accessible over the Internet.

Application Vulnerability Testing

The proliferation of web-based applications has naturally led to a vast number of these applications containing vulnerabilities that intruders can exploit for various nefarious purposes, including stealing or damaging information. High value applications such as online banking are naturally those that are targeted intensely by intruders. Some tools that are available to identify vulnerabilities include:

- IBM Watchfire AppScan
- HP SPI Dynamics WebInspect
- Nessus

The vulnerabilities that can be found by these **application vulnerability scanning** tools include:

- Cross-site scripting
- Injection flaws
- Malicious file execution
- Insecure Direct object Reference
- Cross Site Request Forgery
- Information Leakage and Improper Error Handling
- Broken Authentication and Session Management
- Insecure Cryptographic Storage
- Insecure Communications
- Failure to Restrict URL Access

(Source: Open Web Access Security Project: owasp.org)

These vulnerabilities usually exist as a result of improper web application design or coding. Increasingly, organizations use application vulnerability scanning tools to discover vulnerabilities in their own web applications so that they can fix those vulnerabilities before they can be discovered by intruders.

Audit Log Analysis

Access controls on information systems create audit logs that should be regularly examined; this activity is called **audit log analysis**. Several types of problems can occur on a system that might otherwise go unnoticed, including:

- **Attempted break-ins**. Often, systems will log all successful and unsuccessful login attempts. A significant number of unsuccessful login attempts may be an indication that an intruder is attempting to break in to a user account.
- **System malfunctions**. System error logs may include entries that could be a sign of tampering or attempted break-ins.

- **Account abuse.** Close examinations of user logs can sometimes identify account abuse, including credential sharing, where a user shares their credentials with others, resulting in concurrent logins.

Because they contain important data about system accesses and events, audit logs themselves can be the target of an attack, primarily as a means for an intruder or insider to erase his or her tracks. For this reason it is recommended that one or more of the following measures be taken to protect audit logs:

- Write audit logs onto a write-once medium such as optical storage
- Write audit logs onto a central, highly-protected server that administrators cannot access
- Extend intrusion detection capability to systems that store audit logs
- Employ measures to prevent a Denial of Service attack that attempts to exceed the storage capacity of audit log media

Chapter Summary

- Identification is used to identify a subject without confirmation.
- Authentication is used to identify a subject with confirmation, such as a password, token, or biometric.
- Authentication can be based upon something the user *knows*, something the user *has*, or something the user *is*. Strong authentication, also known as *two-factor authentication*, employs something the user *has* or *is*.
- Biometric authentication involves measuring some physiological characteristic of the subject such as fingerprint, hand shape, iris pattern, speech, or handwriting.
- Commonly used standards used for authentication include LDAP, RADIUS, Diameter, TACACS, and Kerberos.
- Single Sign-On (SSO) is a means of authenticating a user once to an environment and utilizing that authentication to permit the user access to all applications in the environment without having to authenticate to each one separately.
- Information systems are often attacked as a means of bypassing access controls and gaining control of a system. Methods of attack include buffer overflow, script injection, malicious code, Denial of Service, eavesdropping, spoofing, social engineering, phishing, and password attacks.
- Malicious code is used to attempt to interfere with or gain control of a system. The types of malicious code are viruses, worms, and Trojan horses.
- The concept of *separation of duties* is used to ensure that no single individual has too many privileges.
- The concept of *least privilege* means that any user should have only the access privileges required to carry out his or her responsibilities.
- The types of controls used to protect a system or process are *technical*, *physical*, and *administrative*.

- The categories of controls are *detective*, *deterrent*, *preventive*, *corrective*, *recovery*, and *compensating*.
- The concept of *defense in depth* states that several layers of controls should be used to protect an asset. Then if any single control fails, other controls will still be in place to provide protection.
- Access controls should be tested to ensure that they function properly. The types of tests available include *penetration testing* and *application vulnerability testing*.
- Audit logs should be in place to record events, including attempted break-ins, system malfunctions, and abuse. Audit logs themselves should be protected to prevent tampering.

Key Terms

Active Directory A Microsoft implementation of LDAP.

Administrative controls The policies, procedures, and standards put in place in an organization to govern the actions of people and information systems.

Application vulnerability scanning A means of testing an application to identify any vulnerabilities.

Audit log analysis An activity used to detect unwanted events that are recorded in an audit log.

Authentication The act of proving one's identity to an information system by providing two or more pieces of information, such as a userid and a password, in order to gain access to information and functions.

Biometrics A means for measuring a physiological characteristic of a person as a means for positively identifying him or her.

Buffer overflow An attack on a system by means of providing excessive amounts of data in an input field.

Compensating control A control that compensates for the absence or ineffectiveness of another control.

Compromising Emanations (CE) Emanations of electromagnetic radiation (EMR) that disclose senstive information.

Control An activity, process, or apparatus that ensures the confidentiality, integrity, or availability of an asset.

Corrective control An activity that occurs after a security event has occurred in order to prevent its reoccurrence.

Crossover Error Rate (CER) The point where False Reject Rate and False Accept Rate are equal.

Data remanence The unintentional data that remains on a storage device or medium.

Denial of Service (DoS) An attack where data is sent to a target system in an attempt to cause the target system to malfunction.

Detective control A control that is used to detect specific types of activity.

Deterrent control A control used to deter unwanted activity.

Diameter An authentication, authorization, and accounting protocol that is a replacement for RADIUS.

Digital certificate An electronic document that utilizes a digital signature and an identity, used to reliably identify a person or system.

Distributed Denial of Service (DDoS) A Denial of Service attack that originates from many systems. See also *Denial of Service*.

Dumpster diving An attack where an attacker rummages through refuse bins ("dumpsters") in an attempt to discover sensitive discarded information.

Eavesdropping An attack where an attacker attempts to intercept communications.

Emanations Typically RF emissions from a computer or conductor that permits eavesdroppers to eavesdrop on computer activity.

Encryption A means of scrambling information to make it unreadable except by parties who possess a key.

False Accept Rate (FAR) How often a biometric system accepts an invalid user.

False Reject Rate (FRR) How often a biometric system rejects valid users.

Hash A computational transformation that receives a variable sized data input and returns a unique fixed-length string. Hashing is considered irreversible it is not possible to obtain an original plaintext from a known hash.

Identification The act of claiming identity to an information system.

Kerberos An authentication service that utilizes a centralized authentication server.

LDAP Lightweight Directory Access Protocol, a centralized directory service often used for access management and authentication.

Least privilege The access control principle that states that an individual should have only the accesses required to perform their official duties.

Logical controls See *technical controls*.

Malicious code Computer instructions that are intended to disrupt or control a target system.

Malware See *malicious code*.

Password A secret word or phrase entered by a user to authenticate to a system.

Password cracking An attack where the attacker uses tools to methodically guess passwords in order to gain access to a system.

Password guessing An attack where the attacker guesses likely passwords in an attempt to gain access to a system.

Penetration testing An activity that consists of transmitting network packets to a target system in order to discover unprotected, misconfigured, or unsecure services on a target system.

Personal Identification Number (PIN) A numeric password. See also *password*.

Pharming An attack where the attacker poisons *DNS* or *hosts* information to redirect communications intended for a legitimate system instead to an imposter system, as a means for harvesting sensitive information.

Phishing Fraudulent e-mail messages that attempt to lure an unsuspecting user to provide private information via a fraudulent web site (usually) or in an e-mail reply (less often).

Physical controls Mechanisms that control or monitor physical access and environmental systems.

Preventive control A control that blocks unauthorized or undesired activity.

RADIUS Remote Authentication Dial In User Service, a remote access authentication protocol.

Recovery control A control that is used to restore conditions to normal.

Reduced sign-on A type of authentication where users have a limited set of userids and passwords that are used to access systems and applications.

RFC Request for Comments; the formalized documents that describe the Internet's technical and procedural standards.

Script Injection An attack on a system where script language accompanies input data in an attempt to execute the script on the target system.

Separation of duties The work practice where high risk tasks are structured to be carried out by two or more persons.

Single Sign-On An access control method where users can authenticate once and be able to access other systems and applications without being required to re-authenticate to each one.

Smart card A credit-card sized memory device used for authentication.

Sniffing The act of eavesdropping on a network by capturing traffic.

Social engineering An attack on an organization where the attacker is attempting to gain secrets from staff members, usually for gaining unauthorized access to the organization's systems.

Spear phishing A specially targeted phishing attack. See also *phishing*.

Spoofing An attack where the attacker forges the origin of a message as an attempt to disrupt or control a system.

SQL injection An attack where SQL statements are injected into an input stream in the hopes that the SQL commands will be executed by the application's database server.

Strong authentication A means of authenticating to a system using a means strong than userid and password, such as a hardware token, smart card, or biometric. Also known as *two-factor authentication*.

Technical controls Programs and mechanisms that control user access system behavior.

TEMPEST The code name for a U.S. military project dedicated to the study of compromising emanations (CE).

Terminal Access Controller Access-Control System (TACACS) A remote authentication protocol used to authenticate user access to a computer or network–based resource. Superseded by TACACS+ and RADIUS.

Token A hardware device used for authentication.

Two-factor authentication See *strong authentication*.

Whaling A specially targeted phishing attack that targets executives in an organization.

Review Questions

1. The process of obtaining a subject's proven identity is known as:
   a. Enrollment
   b. Identification
   c. Authentication
   d. Authorization
2. Which of the following is the best example of strong authentication?
   a. Biometric
   b. What the user has
   c. What the user knows
   d. Token
3. The only time that a user may share their password with another user is:
   a. When the other user requires higher access privileges
   b. During a disaster
   c. Only temporarily until the other user is issued a userid and password
   d. It is never appropriate for a user to share their password.
4. The term *False Reject Rate* refers to:
   a. How often a biometric system will reject an invalid user
   b. How often a biometric system will accept an invalid user
   c. How often a biometric system will reject a valid user
   d. How often a biometric system will accept a valid user
5. *Password quality* refers to:
   a. Password encryption
   b. Password expiration
   c. Password complexity
   d. All of the above
6. Every month, the human resources department issues a list of employees terminated in the previous month. The security manager should:
   a. Use the list to conduct an audit of computer accounts to make sure the terminated employees' accounts have been terminated
   b. Make sure that computer accounts are terminated as soon as possible after the issuance of the list of terminated employees
   c. Request that the human resource department notify account managers of terminations daily instead of monthly
   d. Request that the list of terminated employees be encrypted for security reasons

7. The principal security weakness with RADIUS is:
   a. Traffic is not encrypted
   b. Passwords do not expire
   c. It uses the UDP protocol
   d. RADIUS sessions are connectionless
8. The use of LDAP as a single source for authentication data helps an organization to achieve:
   a. Fewer password resets
   b. Effective password management
   c. Single Sign-On
   d. Reduced Sign-On
9. An auditor has produced a findings report that cites the lack of separation of duties as a significant problem. Management should consider:
   a. Separating development and production environments
   b. Outsourcing the indicated process
   c. Stop outsourcing the indicated process
   d. Examining the indicated process and reassign duties among a greater number of individuals
10. All of the following controls are preventive controls EXCEPT:
    a. Fencing
    b. Surveillance cameras
    c. Firewalls
    d. Bollards
11. An attack on a server that originates from many sources is known as a:
    a. DDoS
    b. DoS
    c. Botnet
    d. Teardrop
12. The most effective way to protect audit log data is to:
    a. Write audit log data to tape
    b. Write-protect audit log data
    c. Write audit log data to write-once media
    d. Write audit log data to optical storage
13. The purpose of a defense in depth strategy is:
    a. To make protected assets difficult to find
    b. To ensure that protected assets are reachable

c. To protect assets from unauthorized access
d. To protect assets using a variety of controls

14. Anti-malware is a form of:
    a. Preventive control
    b. Detective control
    c. Corrective control
    d. Recovery control
15. The most effective way to prevent password cracking is:
    a. Make the password hash files inaccessible
    b. Remove password cracking tools from the target system
    c. Protect passwords using strong encryption
    d. Remove the target system from the network

Hands-On Projects

Project 2-1: Levels of Authentication

In this project you will explore the levels of identification and authentication used by the online merchant web site Amazon.com. Many web sites use several levels of identification and authentication that correspond to various activities and functions that a user might perform on the web site.

1. If you do not have an online account with Amazon.com, set one up now.
2. Remove any cookies associated with Amazon.com. In Firefox, go to Tools > Options > Privacy > Cookies, then search for and remove amazon.com cookies. In IE, go to Tools > Internet Options > Privacy > Sites. In Safari, go to Edit > Preferences > Security > Show Cookies.
3. Go to the Amazon.com web site and note how it identifies you. Since you have removed your cookies, you should appear as an anonymous user or first-time visitor to Amazon.com, similar to Figure 2-7.
4. Log in to the Amazon.com web site, and then log out. This will re-establish your userid cookie with the web site.
5. Visit Amazon.com again. This time, Amazon should recognize you and display a "Welcome back" message, similar to what is shown in Figure 2-8.
6. Some time in the future (maybe in a few hours or days), visit Amazon.com again. The site should recognize you. This time, visit your account settings page or order merchandise. Even though the web site recognizes you, it may ask you to re-enter your password, proving your identity through authentication, before showing you potentially sensitive information.

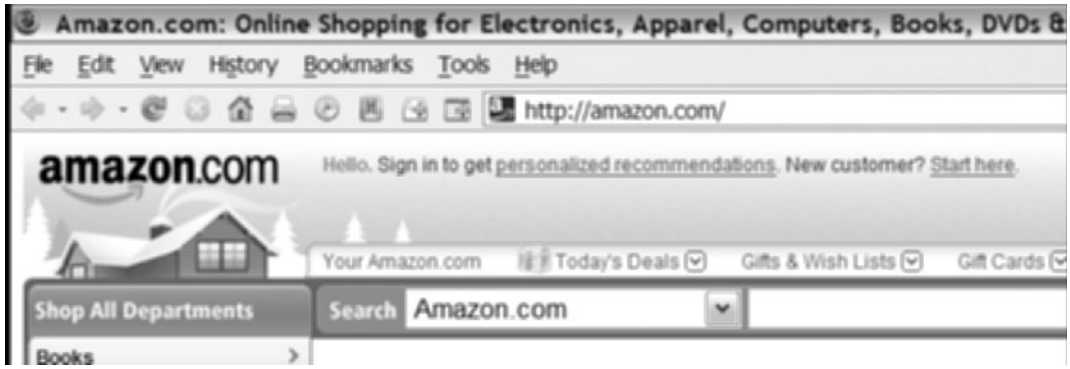


Figure 2-7 Application session, user is logged out

Source: Course Technology/Cengage Learning

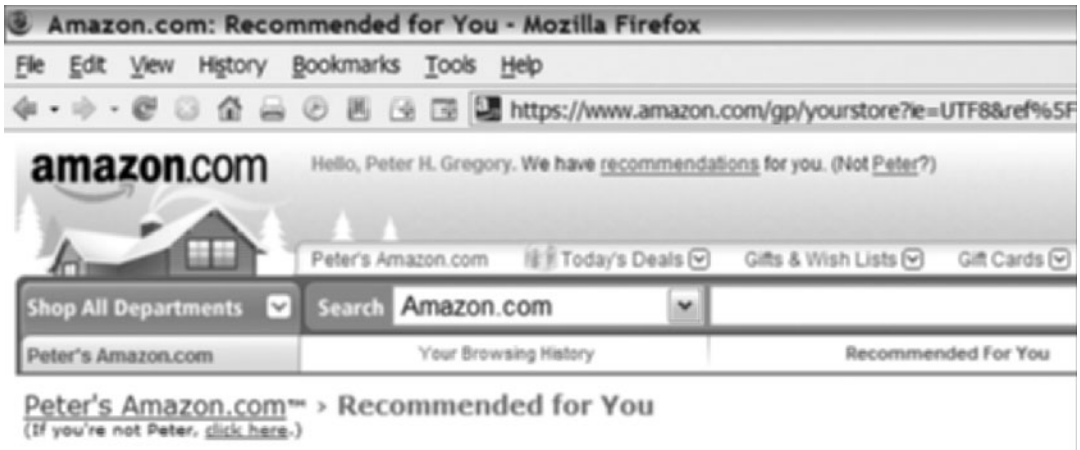


Figure 2-8 Application session, user is logged in

Source: Course Technology/Cengage Learning

7. You will have viewed three different levels of authentication: an anonymous/unknown user, a weakly-identified user (through your userid cookie), and a more strongly identified user (through userid and password authentication).

Project 2-2: Personal Firewalls

In this project you will install and experiment with firewall software. Firewalls are used to block unwanted network traffic by controlling the type of traffic that is permitted to pass between networks, or between a network and a system. This project will give you some hands-on experience with personal firewall software and insight into how network firewalls function.

1. If you are using Windows, download and install ZoneAlarm (www.zonelabs.com and look for the free version) or Comodo (www.personalfirewall.comodo.com). If you are using a Mac, the

OSX operating systems have firewalls built-in; you can find information on using the firewall on the Apple web site.

2. Observe the firewall in action. Zone Alarm detects when a program is trying to communicate over the network and will ask you if the program should be permitted to. Figure 2-9 shows Zone Alarm asking whether Internet Explorer should be able to communicate.
3. Look at the firewall's program configuration, where the firewall knows which programs should be able to communicate. Figure 2-10 shows Zone Alarm's Program Control configuration.
4. Look at the firewall log to see what network traffic the firewall is permitting and blocking. Figure 2-11 shows Zone Alarm's firewall log.
5. Test the firewall by attempting to communicate with your computer from an external source. You can try and ping the computer from an external system. Or, use one of the readily available Internet firewall test sites to see if your computer is reachable from the site. Some sites to try: security.symantec.com, www.auditmypc.com, or www.hackerwatch.org/probe/. If your computer is not protected by a hardware firewall (many newer DSL and Cable modems have firewalls built-in), your firewall should log activity that is generated by the site you used to scan your system.

Figure 2-9 Zone Alarm asks whether Internet Explorer may communicate

Source: Course Technology/Cengage Learning

Figure 2-10 Zone Alarm program control configuration

Source: Course Technology/Cengage Learning

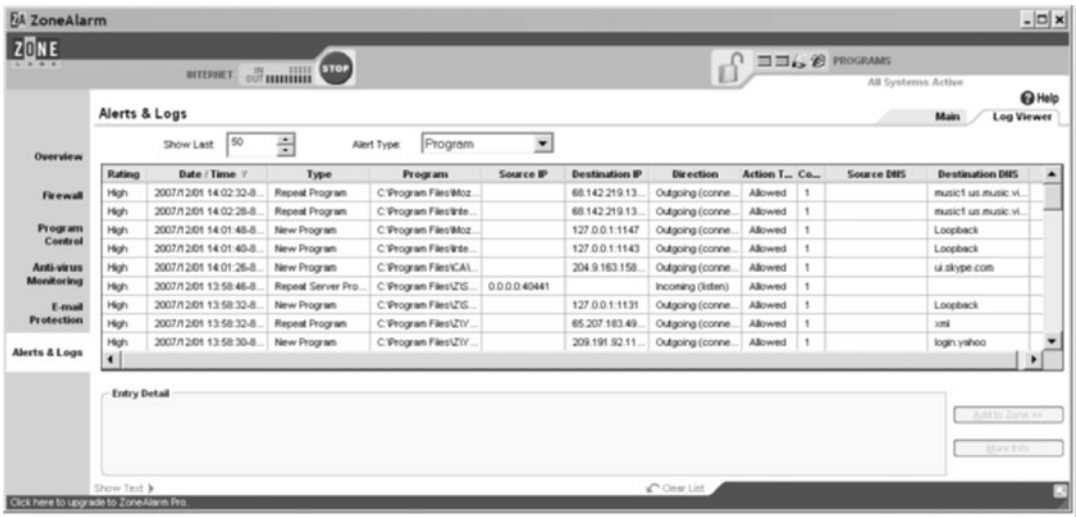


Figure 2-11 Zone Alarm firewall log

Source: Course Technology/Cengage Learning

6. You have viewed a firewall in action: you've responded to alerts, made configuration changes, and observed the effects of a security scan.

Project 2-3: Testing Anti-Virus Software

In this project you will test your anti-virus software to see if it really works, without exposing you to the risks associated with real malware. Unless you partake in high-risk activities that regularly expose you to active malware, you may never have seen your anti-virus software actually catch a virus. So, then, how can you tell whether it actually works?

1. Check your anti-virus program's status and make sure that its real-time detection is functioning. Usually you can do this by double-clicking on the anti-virus program in your Windows system tray.
2. Go to the virus test web site, www.eicar.org. EICAR is the European Institute for Computer Antivirus Research. Click on the Anti-Malware Test File link (alternately, go to http://eicar.org/anti_virus_test_file.htm).
3. Carefully read the instructions on the next page, "The Anti-Virus or Anti-Malware test file." On this page you can download any of several forms of the EICAR test file.
4. Try downloading each form of the EICAR test file and note how your anti-virus software responds. Your anti-virus software should immediately pop-up a window similar to the following when you try to download and save the *eicar.com* or *eicar.com.txt* file. An example virus detection pop-up window is shown in Figure 2-12.
5. Try downloading the *eicar_com.zip* file. In this download, the eicar.txt file is in a compressed Zip archive. Did your anti-virus program recognize the EICAR test file?
6. Try downloading the *eicarcom2.zip* file. This download file consists of the eicar test file in a compressed Zip archive that is within another compressed Zip archive. If your anti-virus software is *really* good, it will have detected the EICAR test file here too.

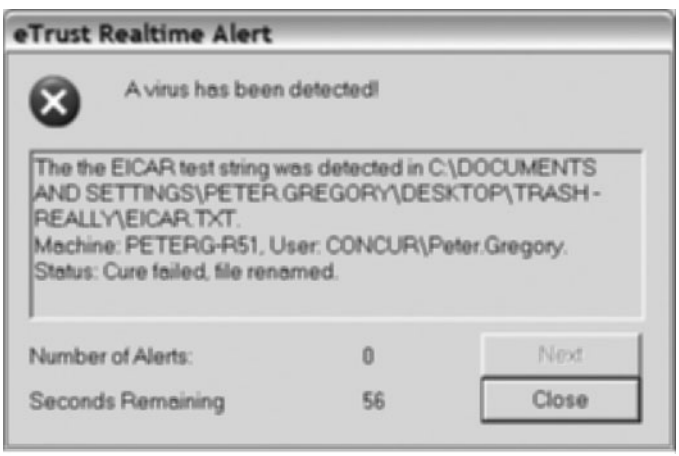


Figure 2-12 Anti-virus software popup window

Source: Course Technology/Cengage Learning

7. If your anti-virus software did not detect the EICAR test file in any of these cases, then you should suspect that your anti-virus software real-time virus detection is not working. Take another look at your anti-virus software configuration. Contact the anti-virus software vendor if you have still having problems.
8. If your anti-virus software did not detect the EICAR test file, another thing to try is to scan your hard drive with your anti-virus program. If the scan does detect the EICAR test file, then you may conclude that your real-time detection is not working but scanning is still functioning.

Project 2-4: Protect Data with Encryption

In this project you will encrypt text files and see how encryption can protect files from unauthorized disclosure. Encryption is one common way that data can be protected from unauthorized access from unauthorized persons.

1. Obtain a copy of WinZip version 9 or newer. WinZip introduced AES encryption starting in version 9. You can download WinZip from download.com or winzip.com.
2. Select or create a small text file to encrypt.
3. Create a new WinZip archive. Add the file from step 2 to the archive. Be sure to select the Encrypt Added Files option, and select None for the Compression option. See Figure 2-13.
4. Close the WinZip archive. Now view the WinZip archive with notepad or other text editor. It will appear to be scrambled, similar to Figure 2-14.

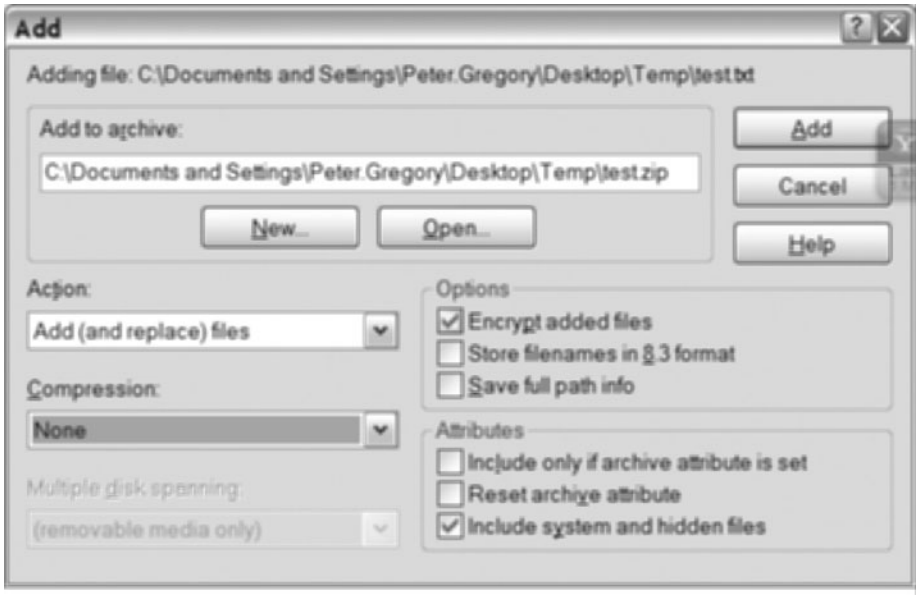


Figure 2-13 Using WinZip to encrypt a file

Source: Course Technology/Cengage Learning

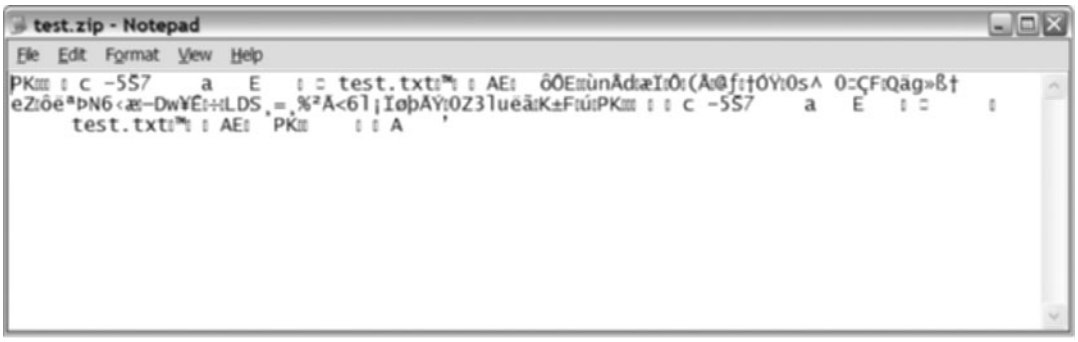


Figure 2-14 WinZip and AES encryption protect a file from unauthorized persons

Source: Course Technology/Cengage Learning

5. Re-open the WinZip archive. Note that you can see the name of the file in the archive without being asked for the decryption key.
6. Extract the file from the WinZip archive. Note that you are required to furnish the decryption key to extract the file; the contents of the file are safe.

Case Projects

Case Project 2-1: Develop an Authentication Plan

As a consultant with the Security Consulting Company, you have been hired to determine how users should be identified and authenticated to a financial services application. You also need to determine how users should first register to use the application.

The application is used to manage an investment portfolio. Functions that can be performed include:

- Initial account registration
- Managing an account profile, including contact information
- Depositing money into a fund
- Withdrawing money from a fund
- Transfering funds from one investment method to another

Develop use cases for each of the above functions, and specify how users should identify themselves to the application for each use case.

Case Project 2-2: Observe a Defense in Depth Environment

Identify a facility or an IT environment that you can visit. Study the environment; what assets are being protected? What controls can you find that are

used to protect assets? Write down all of the controls that you can find and describe how they protect assets.

If possible, have an employee give you a tour of the environment. What additional controls can be found?

When you list the controls that you find, identify their type: detective, preventive, deterrent, compensating, recovery, corrective, or mitigating.

Identify any additional controls that could be implemented to further protect assets.

Case Project 2-3: Learn About Script Injection Vulnerabilities

Search for a script injection demo on the Internet. Search on one of the following terms:

- SQL injection demo
- script injection demo

Find a site that shows an actual SQL or script injection exploit on a demo web site. Observe the exploitation in action. How did the script injection work? If an actual attack was launched against a vulnerable site, what are the possible consequences? What safeguards can be taken to protect an application from such attacks?

chapter 3

Application Security

Topics in this Chapter:

- Types of Applications
- Application Models and Technologies
- Application Threats and Countermeasures
- Security in the Software Development Life Cycle
- Application Security Controls
- Databases and Data Warehouses

The (ISC)^2 *Common Body of Knowledge* (CBK) defines the key areas of knowledge for Application Security in this way:

Application security refers to the controls that are included within systems and application software and the steps used in their development. Applications refer to agents, applets, software, databases, data warehouses, and knowledge-based systems. These applications may be used in distributed or centralized environments.

The candidate should fully understand the security and controls of the systems development process, system life cycle, application controls, data warehousing, data mining, knowledge-based systems, program interfaces, and concepts used to ensure data and application integrity, security, and availability.

Key areas of knowledge:

- *Understand the role of security in the system life cycle*
- *Understand the application environment and security controls*
- *Understand databases and data warehousing and protect against vulnerabilities and threats*
- *Understand application and system development knowledge security-based systems (e.g., expert systems)*
- *Understand application and system vulnerabilities and threats*

Types of Applications

Applications are computer programs that perform useful work for people. They may be as complicated as a corporate financial management system or a manufacturing resource planning system, or as simple as a retirement calculator. Applications perform a set of instructions: they may accept input data, perform calculations, and create output data. *How* they do these things varies widely, depending upon the purpose of the application and the technologies used to build and operate it.

In this section the following types of applications will be discussed:

- Agents
- Applets
- Client-server
- Distributed
- Web applications

Agents

Agents are small standalone programs that are part of a larger application. Agents carry out specific functions, such as remote status collection or remote system management.

Agents generally run autonomously and without any human interaction. On a Windows system an agent often runs as a service, and on Unix an agent is usually started by the system startup scripts.

Some examples of agents include:

- **Anti-virus**. You could consider the anti-virus program on a workstation or server as an agent in an enterprise environment that includes a central management console.
- **Patch management**. An agent on each server periodically queries the OS on the existence of software patches, and will install patches when commanded to do so from the central patch management server.
- **Configuration management**. A central server tracks and manages the OS configuration of each server and workstation by communicating to agents on those managed systems. Agents will collect configuration information and pass it back to central servers; agents will also perform configuration changes upon command.

Applets

An **applet** is a software program that runs within the context of another program. Unable to run on its own, an applet performs a narrow function.

Unlike a subroutine, which is a part of a running program, an applet is a separate object. Probably the most common use of applets is within Web browsers.

Examples of Web browser applets include media players such as Flash and Shockwave players, and content viewers such as Adobe Reader. Figure 3-1 shows a Java applet running in a Web browser window.

Client-server Applications

The software components in **client-server applications** are not centralized, but instead are present in two places: clients and servers. Clients and servers usually communicate with each other via networks. Specific characteristics of clients and servers are explained here.

- **Client characteristics**. Client software is the part of the application used by humans, and primarily contains user interface logic that displays instructions and data, accepts input data from a keyboard or other device, and accepts instructions or directives from users. Client software is dominantly built upon personal workstations running Windows, UNIX, MacOS, and other operating systems.
- **Server characteristics**. In typical client-server applications, the server component performs database updates and communicates with clients. Server components typically do not have user interface logic but instead run as daemons or services.

Client-server architectures were developed to meet the higher-processing demands of increasingly sophisticated graphical user interfaces by moving the display and input logic from a central system to the end user workstation. Database and other back-end functions remained on central servers. Clients and servers often communicated with each other over TCP/IP using protocols such as **ODBC (Open Database Connectivity)** and **SQL*Net**.

The primary advantage of client-server architecture (depicted in Figure 3-2) was the ability to provide a more complex user interface to end users without the need to invest in significantly

Figure 3-1 Java applet in a browser window

Source: Course Technology/Cengage Learning

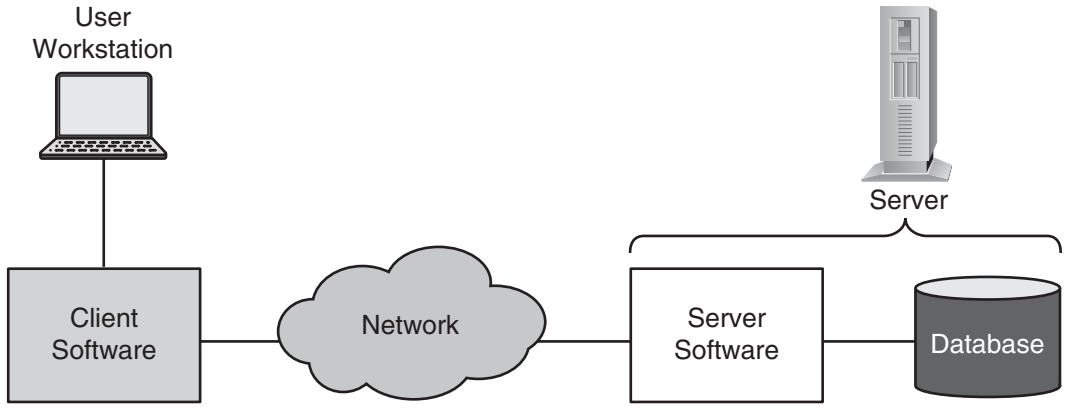


Figure 3-2 Typical client-server architecture

Source: Course Technology/Cengage Learning

larger servers. The chief disadvantage of client-server architecture was the network communication between clients and servers that usually created a significant performance bottleneck that prevented a client-server from scaling well.

The peak of popularity of client-server architecture has passed, although it is still in wide use, mostly in applications that were developed before software development organizations chose to make Web browsers their primary client platform.

Distributed Applications

Distributed applications have software components running on several separate systems in a wide variety of architecture including two-tier, three-tier, and multi-tier. Usually, distributed systems are designed in a way to physically or logically separate different functions in the application. There are many possible reasons for this separation, including scalability, performance, geographical, and security.

Often, distributed applications consist of separate components that come from different origins. For instance, an application may be written in Java and designed to run on a specific run-time environment, and use a database management system from another company that, for performance and other reasons, will reside on separate systems. More complex systems may have additional components that, for different reasons, may reside on separate platforms. Figure 3-3 shows a typical distributed application environment.

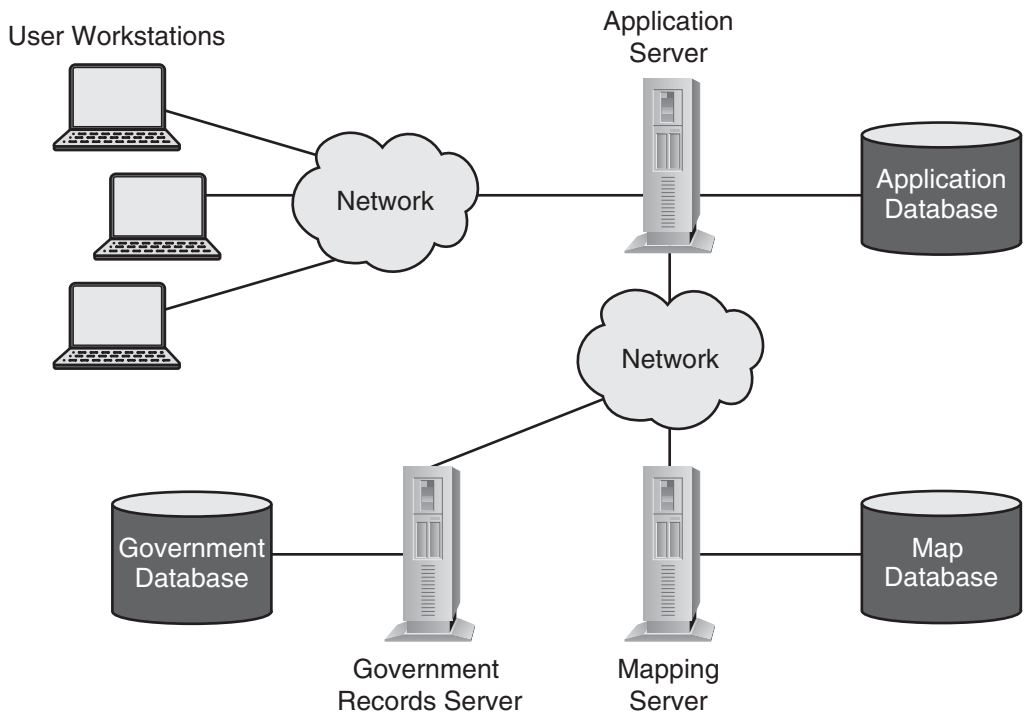


Figure 3-3 Typical distributed application architecture

Source: Course Technology/Cengage Learning

The software components in a distributed application may be separated for performance reasons. There may be a large user base and it may make better economic sense to build the application on several smaller servers instead of one large server.

Distributed applications are often designed to reduce security risk. For example, an application that is used to manage sensitive information, or one that is accessed over the Internet, may be designed with multiple tiers in order to reduce the risk of unauthorized disclosure of information. For instance, **two-tier application** may have a business logic front-end and a database back end, and a **three-tier application** typically consists of a user interface front end, a middle tier containing business logic, and a database back end.

A significant issue with distributed applications is version control and standardization. Managing and tracking the versions of software throughout the distributed application, and making sure that components continue interoperating properly, is a challenge, particularly when various components are updated periodically. The near-constant state of change requires coordination and regression testing, to keep the distributed application working properly.

Web Applications

In the late 1990s, the near-ubiquity of web browsers and advances in browser related technologies created the next opportunity for client-server and distributed applications: **web applications**. Web applications provide several significant advances over client-server applications including:

- **Thinner clients**. End user workstations need only a lightweight OS and a web browser. The browser becomes the client software, which works with all of the enterprise's web applications.
- **Better network performance**. More business logic resides on the server, and only display logic resides on the workstation, significantly reducing demands on the network. This enables more users to use the application without incurring meltdowns on the network.
- **Lower cost of ownership**. The organization only needs to make sure that workstations have a reasonably current version of a web browser. The administrative overhead related to maintaining versions client software components for all of the organization's client-server applications is eliminated.
- **More terminal types supported**. Because the client side of the application standardizes on HTML, several browser and terminal types are supported. Users are no longer locked into a hardware or OS platform, but can access applications using a variety of terminal types including Windows, UNIX, and Apple workstations, and also mobile devices such as smartphones and PDAs.
- **Any user can access the application**. Because a web application requires only a browser as a client, any user anywhere in the world can potentially access the application.

Web applications significantly reduce the number of software programs that must be installed and maintained in end user workstations. This in turn has curbed the increase in hardware resources required for workstations.

Application Models and Technologies

Computer systems and application programming languages are generally built upon models that give the language some form and structure. Four models that have been the most popular are control flow, structured, object-oriented, and knowledge-based.

Control Flow Languages

The earliest computer languages, known as **control flow**, were sequential in nature—that is, they executed statements one after the other. Most languages used some variation of an "if-then" construct as well as a "goto" construct to alter the sequence of instructions.

The disadvantage of control flow is the difficulty in verifying a program's integrity. Excessive use of "goto" statements turned linear logic into "spaghetti" code that was difficult to analyze and understand. The "goto" statement was demonized, and structured languages won favor.

Structured Languages

Programming languages with procedural structure were developed to overcome the deficiencies of control flow applications with their "goto" statements. **Structured languages** used *subroutines* or *functions* and relied less on *goto* (some structured languages do not have goto at all).

Structured languages tend to be structured in "blocks" of code that are bracketed by keywords such as `if...fi`, `BEGIN...END`, `{...}`, `if...then...else...endif`, and so on. The flow of logic in structured languages tends to be hierarchical rather than linear, which tends to make analysis and verification somewhat easier. Programming languages continued to evolve, and the next level of maturity was object oriented programming.

Object Oriented Systems

Object oriented (**OO**) systems were developed to face the growing problem of programmer inefficiency by providing an environment in which objects (pieces of software) could be easily reused. Object oriented is more than just hierarchical programming—it provides a framework for easily building large, complex systems that have reusable code written in different languages and which reside in a distributed environment.

Object Oriented Programming

Object oriented programming (**OOP**) originated in the 1960s with the computer languages Simula and Smalltalk. Then, as now, object oriented (commonly known as OO, and pronounced *oh-oh*) programming is a completely different approach to computer languages than the structured languages in use such as BASIC, C, and Java. Object oriented programming has a particular vocabulary that is used to describe how components are named and assembled into programs. These terms are:

- Class
- Object
- Method
- Encapsulation

- Inheritance
- Polymorphism

Class A **class** defines the characteristics of an *object*, including its characteristics such as attributes, properties and fields, plus the *methods* it can perform.

Object An **object** is a particular *instance* of a *class*. The class *superhero* defines all superheroes and lists their characteristics. The object *Superman* is one particular superhero. The object *Superman* is an instance of the class *superhero*.

Method A **method** defines the abilities that an object can perform. It may contain instructions, as well as input variables and output variables. A method is similar to a *function* or *subroutine* in structured programming. It consists of some instructions or calculations, and communicates using *message passing*. The method *fly()* is one of Superman's *methods*.

Encapsulation **Encapsulation** refers to the implementation details in a method that are concealed. For example, the code for Superman's *fly()* method contains several other methods like *propulsion()* and *steering()* that other objects do not need to be concerned about.

Inheritance The term **inheritance** refers to the characteristics of a subclass that inherit attributes from their parent classes. And in turn, subclasses can introduce their own attributes that are passed to *their* subclasses.

Polymorphism The characteristic of **polymorphism** allows *objects* of different types to respond to *method* calls differently, depending upon their *type*. For instance, a call to a *compute-tax()* method will result in different behavior depending upon the country (*type*) where the transaction takes place (there are not only different tax rates, but different taxable goods, and some people are taxed at different rates).

Distributed Object Oriented Systems Distributed systems may be built upon object oriented (OO) frameworks. These systems may be programmed with OO languages such as Java or C++. Modules on different systems that need to communicate with each other will typically use an Object Request Broker (ORB), a service that is used to locate an object on another system across networks. Common ORBs in use include CORBA (Common Object Request Broker Architecture), EJB (Enterprise Java Bean), DCOM (Distributed Common Object Model), or JRMI (Java Remote Method Invocation).

Knowledge-based Applications

Knowledge-based systems are applications that are used to make predictions or decisions based upon input data. They include feedback mechanisms that enable them to learn and refine their guidance, improving their accuracy over time. The objective of knowledge-based systems is the ability for a system to possess some of the qualities of human reasoning. It is for this reason that knowledge-based systems are often termed Artificial Intelligence.

Examples of knowledge-based applications include weather forecasting, statistical data modeling, and decision-makers for mortgage and credit applications.

Neural Networks

Neural networks are so-named because they are modeled after biological reasoning processes that humans possess. A neural network (NN) consists of interconnected artificial neurons that store pieces of information about a particular problem. Neural networks are given many cases of situations and outcomes; the more events the neural network is given, the more accurately it will be able to predict future outcomes. This is done primarily through the NN being able to assign weights to different inputs. For instance, a hurricane-forecasting neural network that is used to make landfall predictions will heavily weigh the storm's location, wind speed and ocean temperature, but place less weight on the phase of the moon and little or no weight on the day of the week.

Expert Systems

Expert systems accumulate knowledge on a particular subject, including conditions and outcomes. The more samples that the expert system is able to obtain, the greater is its ability to predict future outcomes.

An expert system contains a *knowledge base* that is the total accumulated knowledge and outcomes of past events that have been entered into the expert system. The expert system also includes an *inference engine* that analyzes information in the knowledge base in order to arrive at a decision or solution to a new problem.

Threats in the Software Environment

Because software applications are so often used to manage things of value, they may be subject to attack by those who wish to steal those assets and take them for their own. But value is not the only reason that applications are attacked; other reasons that applications are attacked include:

- **Industrial espionage**. Organizations with valuable secrets are often targeted by those who wish to steal those secrets for their own gain.
- **Vandalism and disruption**. Individuals and groups who, for a wide variety of reasons, wish to vandalize and harm the operations of specifically or randomly targeted organizations.
- **Denial of Service**. A more targeted attack where the attackers' objective is to completely disable the target system.
- **Political/religious**. Attacks perpetrated through political or religious motives at a national or international scale.

The threats to software applications discussed in this section include:

- Buffer overflow
- Malicious software
- Input attacks
- Logic bombs
- Object reuse

- Mobile code
- Social engineering
- Back door

Buffer Overflow

Software applications usually function by soliciting and accepting input from a user (or another application) through an interface. An attacker can attempt to disrupt the function of a software application by providing more data to the application than it was designed to handle. A buffer overflow attack occurs when someone attempts to disrupt a program's operation in this manner.

In a buffer overflow attack, the excess input data overflows the program's input buffer and overwrites another part of the program's memory space. Depending upon the hardware and software architecture of the attacked program, this can lead to corruption of other variables in the program (which could lead to an unexpected change in the program's behavior), or the overflow could overwrite instructions in the software. A well-formed attack can plant specific instructions in the input buffer (that will be known to overflow the instruction space in the attacked program) that will result in a distinct change in the program's behavior.

Types of Buffer Overflow Attacks

There are several specific types of buffer overflow attacks, discussed here.

Stack Buffer Overflow

In this type of attack, the program writes more data to a buffer located on the stack than was allocated for it. This causes the corruption of other data in the stack, which results in the program's malfunction.

If the attacker is familiar with the program that he is attacking, he can attempt to place specific data in the overflowed portion of the stack in order to cause a specific type of malfunction to occur. The particular malfunction that is desired will depend upon the motives of the attacker.

NOP Sled Attack

The **NOP sled** attack is a specific stack overflow attack where the attacker overflows the stack with harmless NOP (no-op) instructions. The point of the NOP sled attack is to improve the chances that the attacker will be able to find an attack point. By flooding the stack with lots of NOPs, the program will encounter and "slide down" the NOPS until it reaches the pointer that the attacker placed in the buffer. The program will then jump to the memory location referenced by the pointer, resulting in whatever behavior the attacker intended.

When an attacker is attempting a buffer overflow attack, he cannot see the attacked program's memory space; instead, he must guess its structure. The NOP sled attack helps to improve the attacker's guesswork at how to exploit the target program.

Heap Overflow

The **heap** is the dynamically allocated memory space created by a program for storage of variables. Usually a **heap overflow** attack will result in the corruption of other variables that are already on the heap. A heap overflow attack will result in corrupted

data that may change the actual behavior of the program, or simply alter data used by the program, which could affect other users or stored data.

Jump-to-Register Attack The **jump-to-register** attack is another approach to buffer overflows. In this attack, the return pointer is overwritten with a value that will cause the program to jump to a known pointer stored in a register that points to the input buffer.

Historic Buffer Overflow Attacks Several wide-scale buffer overflow attacks have been perpetrated through the Internet, and some have caused significant damage totaling hundreds of millions to billions of U.S. dollars. Notable buffer overflow attacks are described here.

- **Morris worm.** Created by Robert Tappan Morris in 1988, the Morris Worm exploited a buffer overflow vulnerability in the "finger" program on UNIX systems. It also exploited several other vulnerabilities including default passwords and the excessive use of trusted relationship between computers. The Morris worm did no real damage other than make thousands of computer systems unavailable for use until the worm could be eradicated.
- **Ping of death.** The Ping of Death (POD) is a buffer overflow attack wherein the attacker sends a "ping" (literally, an ICMP echo request) packet with a very large payload to a target system. A ping is usually 64 bytes in length, whereas a Ping of Death packet is as large or larger than the maximum IP packet size, which is 65,535 bytes. The target is often unable to properly process the incoming packet, resulting in a buffer overflow that causes the system's TCP/IP stack to malfunction. The Ping of Death attack is also a Denial of Service attack because it renders the target system unusable by its users.
- **Code Red.** Released in July, 2001, this computer worm attacked a buffer overflow vulnerability in Microsoft IIS web server, for which a patch had been available for about a month.
- **Slammer.** This worm exploited a buffer overflow in Microsoft SQL Server and Desktop Engine (MSDE) database products in January, 2003. Slammer had an efficient network scanning propagation mechanism that allowed it to infect most of its 75,000 servers within minutes of release. A patch to mitigate the buffer overflow vulnerability had been available for six months, but was installed on few systems.
- **Blaster.** This worm exploited a buffer overflow in the DCOM RPC service on Windows systems. A patch for the vulnerability was issued in July 2003 but few organizations installed it by the time it appeared on August 11, 2003.
- **Sasser.** Released on or about April 30, 2004, the Sasser worm exploited a buffer overflow in the LSASS (Local Security Authority Subsystem Service) in Windows 2000 and Windows XP. A patch had been available for only seventeen days.

Buffer Overflow Countermeasures Several tactical and strategic countermeasures are available to reduce or eliminate the risk of buffer overflow attacks. Buffer overflow countermeasures are used to either remove buffer overflow capabilities or detect and block buffer overflow activity.

- **Choose a safe language.** Programming languages like C and C++ do not automatically check input buffer lengths or perform other boundary checking. For instance, the strcpy() function that is used to copy strings performs no boundary checking and will merrily copy data right over other variables. Java, .NET, and many other languages have built-in boundary checking that—in most cases—prevents buffer overflows.
- **Use of safe libraries.** Whether C or C++, or a "safer" programming language is used, libraries with functions for inputting and processing data will significantly reduce the risk of events like buffer overflows.
- **Executable space protection.** Attackers use buffer overflows to insert code into the memory of a program. Executable space protection, a feature of some operating systems, forces programs to abort if they attempt to execute code in the stack or the heap. Some CPUs support executable space protection in hardware.
- **Stack smashing protection.** This refers to techniques used to detect changes in the stack. Typically a "canary value" is placed between a buffer and the stack. The canary value is so-called after the use of canaries in underground mines as an indicator of air quality. In stack smashing protection, the canary value is set to a known, random value, and after a function call is returned, the canary value is checked again. If the stack has been smashed by a buffer overflow, the canary value will have changed, and the program can take evasive action. If the canary value is unchanged, then the program has not been tampered with.
- **Application firewalls.** Firewalls that perform deep packet inspection (DPI) examine the payload of each packet entering a system. An **application firewall** recognizes the patterns used in buffer overflow and other attacks and will block those packets, effectively preventing attacks.

Malicious Software

Malicious software, also known as malicious code, is a class of software that comes in many forms and performs a variety of damaging actions. The purposes of malware include:

- **Propagation.** Sometimes the ability for malware to propagate—that is, to spread from system to system—is the only purpose for particular malware programs.
- **Damage and destruction of information.** Malware can alter or delete files on target systems.
- **Steal information.** Malware can locate and steal valuable information such as e-mail addresses, userids and passwords, bank account numbers, and credit card numbers. Malware can harvest and transmit this information back to the malware's owner or operator.
- **Usage monitoring.** Malware can implant the means to record subsequent communications, keystrokes and mouse clicks, and send this data back to the malware's owner-operator.
- **Denial of Service.** Malware can consume all available resources on a target system, rendering it essentially useless for its intended use.
- **Remote control.** Malware can implant a **bot** onto a target system that allows an attacker to remotely control the system. Large collections of bots are called *bot armies*,

and the people who build and control bot armies are known as *bot herders* or *botnet operators*.

Types of Malicious Software Malware has been developed into many forms that are described in this section. It can be said that malware has undergone the same types of innovation that software has undergone. New methods of development and propagation have been developed that give malware new ways of spreading from system to system, and also new ways of evading system and network defenses.

- Viruses
- Worms
- Trojan horses
- Rootkits
- Bots
- Spam
- Pharming
- Spyware and Ad-ware

Viruses **Viruses** are the original malware on Intel x86 processor systems popularized by Microsoft DOS and Windows since the 1980s. Viruses are computer code fragments that attach themselves to a legitimate program file on a computer. The virus can only run when the legitimate program is run.

By definition, viruses generally require human intervention to propagate. A user must run a program in order to make the virus spread.

Viruses used to propagate through file sharing (when users would trade information or programs via floppy disks), but more often they travel through e-mail and web traffic.

Several types of viruses are discussed here.

- **Master Boot Record (MBR) viruses**. The earliest method of virus propagation, these viruses attach themselves to the master boot record of a floppy disk. If the system is booted when the floppy disk is present in the system, the virus will be activated on the system. When other floppy disks are inserted after activation, the virus may be copied on to those floppy disks also. When floppy disks were the primary means for transferring data from computer to computer, this was a common way for viruses to propagate from computer to computer.
- **File infector viruses**. These are the viruses that attach themselves to executable programs (.EXE and .COM files) and are activated each time the executable program is run.
- **Macro viruses**. In the early 1990s, Microsoft and other companies developed the concept of macros that could be embedded into document and spreadsheet files. Writers of viruses and other malicious code quickly realized that these new capabilities could be used to propagate malware.

When a user opens a document that contains a macro, the macro is executed. The embedded macro may be written in a script language such as Visual Basic or Visual C++. The macro may contain any legitimate instructions that may vastly exceed anything that the user would want.

Melissa and *I Love You* were macro viruses that propagated through documents that contained macro instructions to mail copies of themselves to everyone in a user's local e-mail address book. These macro viruses spread quickly through the Internet and caused considerable damage primarily through clogging e-mail servers with thousands of virus-caused messages.

Viruses employ several methods to avoid detection by anti-virus programs. The methods in use include:

- **Multipartite viruses**. These use more than one means for propagating from one system to another. For example, Ghostball infected both executable .COM program files as well as floppy disk boot sectors.
- **Stealth viruses**. A stealth virus uses some means to hide itself from detection from the operating system.
- **Polymorphic viruses**. Viruses are easily stopped when anti-virus programs recognize the virus through its signature. Virus creators have introduced polymorphic viruses that change themselves as they move from system to system in order to avoid detection. However, engineers in the anti-virus companies are able to solve the puzzle of polymorphic viruses and create a signature for them.
- **Encrypted viruses**. In another method to avoid detection, viruses will encrypt most of their code, using a different key on each system they infect, which makes most of the body of the virus different on each detected system. However, a part of the virus—the decryption code—must remain the same; it is this portion of the virus that the anti-virus software must be able to identify in order to stop the virus.

Worms Generally speaking, **worms** are like viruses, but they usually require little human intervention to spread. Instead, they have their own means of propagation built-in.

Two common types of worms that are found today include:

- **Mass mailing worms**. Mass mailing worms propagate via e-mail. Generally, when a mass-mailing worm arrives in a user's inbox, the worm is activated when the recipient opens the message. The worm's malicious code could reside within the HTML code in the message, or in an attached file.
- **Port scanning worms**. A port scanning worm is able to propagate with no human intervention at all. A port scanning worm scans the network for other systems that may be vulnerable and attempt to spread to those neighboring systems. If it's able to infect a new system, it will install itself and begin the scanning to look for new victims.

Several infamous worms utilized port scanning to identify new targets that they would attack with specific buffer overflow attacks. The Morris Worm, Blaster, SASSER, Code Red, and Slammer are described in the "Buffer Overflow" section earlier in this chapter. Figure 3-4 shows the rapidity with which the Code Red and Nimda worms spread through the Internet in 2001.

Trojan Horses Like the ancient Greek legend, a computer-based **Trojan horse** is a lie. A Trojan horse claims to be one thing, but is instead something else—something with more malicious intent.

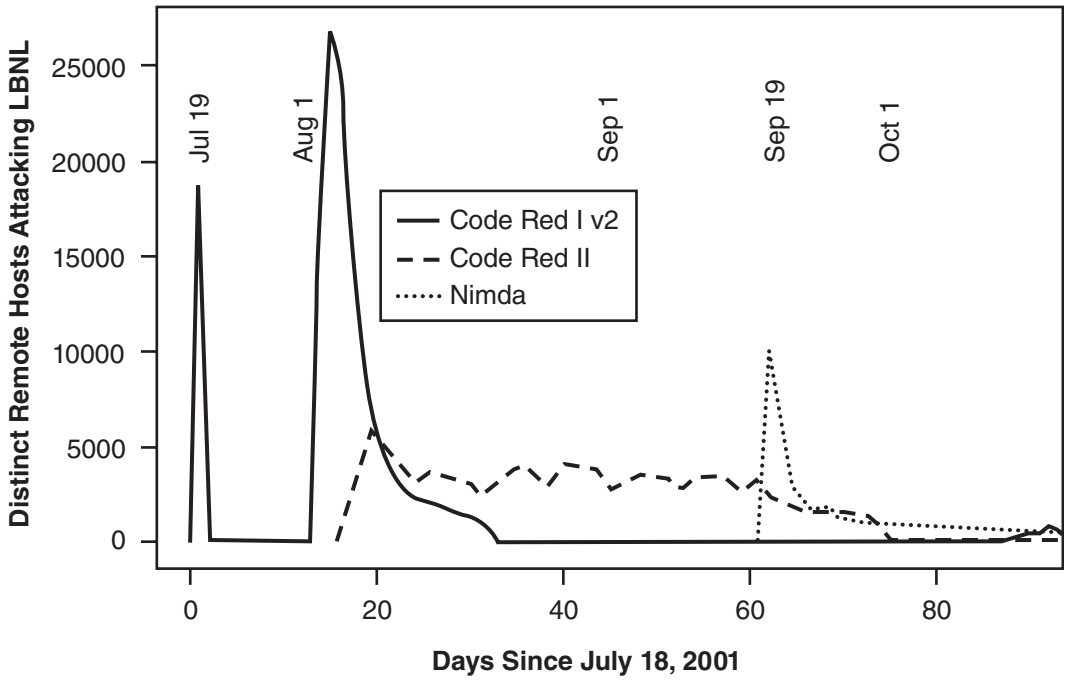


Figure 3-4 Code Red and Nimda spread quickly through the Internet

Source: Diagram with permission from "How to 0wn the Internet In Your Spare Time", S. Staniford, V. Paxson and N. Weaver, Proc. USENIX Security Symposium 2002

For example, a user may receive an e-mail message that says, "Take a look at this great new computer game," or, "Have a look at these pictures of <some popular model or celebrity>." Unsuspecting users willingly execute these programs without a second thought.

The user who runs a Trojan horse program may or may not see some visual resemblance of what the program claims to be. However, the Trojan horse is also performing some additional (and probably malicious) action. It might be corrupting or destroying files, stealing data, or sending e-mails to your friends.

Rootkits One of the newest forms of malware, **rootkits** are malware programs that are designed to avoid detection by being absolutely invisible to the operating system. Rootkits achieve this by altering the OS itself so that its presence is nearly impossible to detect.

Methods used by rootkits to avoid detection include:

- **Process hiding**. Rootkits can hide their own process(es) from users by altering the tools that are used to list processes on a system. By manipulating process-listing tools into "looking the other way," rootkits can hide themselves from most users.
- **File hiding**. Rootkits can hide files as a way of avoiding detection. However, legitimate programs also sometimes hide files, so this alone is not a dependable way of identifying a rootkit.
- **Registry hiding**. Rootkits can hide registry entries in an attempt to function without being detected. However, some legitimate programs also hide registry entries, so this alone is not a sure-fire way to identify a rootkit.

- **Running underneath the OS.** Rootkits can hide from the OS by running underneath or beside it. A rootkit can insert itself into the system by already "being there" when the OS boots.

Virtual OS technology will, for a time, make it easier for rootkits to avoid detection, until companies that make virtual OS products (as well as those that make anti-malware products) are able to figure out which features in their products are vulnerable and permit the introduction of rootkits.

Like anti-virus technology, anti-rootkit technology will become engaged in a cat-and-mouse struggle with rootkit developers in what could be a long-term conflict.

Bots Short for "robots," **bots** are sometimes a part of the malicious payload found in malware. Bots enable a "bot herder" (the owner of the bot program) to remotely control the infected computer for a variety of purposes including:

- **Relaying spam.** Spammers and bot herders can cooperate to use bots as systems to relay spam in order to evade blacklisting (a technique that spam blockers use to block spam by blocking all e-mail from specific IP addresses).
- **Hosting phishing sites.** Phishing scams can use systems owned by bots to host the sites where victims are solicited for sensitive information. By moving the sites quickly from bot-system to bot-system, phishers can evade detection and shutdown.
- **Denial of Service attacks.** Bot herders can launch Denial of Service (DoS) attacks from bot-controlled systems by instructing those systems to launch thousands of network messages per second to a target system. A bot herder can launch a distributed Denial of Service (DDoS) attack by directing hundreds, thousands, or tens of thousands of bot-systems to attack the same target simultaneously.

Spam In a nutshell, **spam** is unwanted e-mail. It accounts for well over ninety percent of all e-mail on the Internet. But more than that, spam is unsolicited "junk mail" that takes many forms including:

- **Unsolicited commercial e-mail (UCE).** There are e-mails that are trying to sell every sort of goods and services ranging from porn to prescription drugs to get-rich-quick schemes. Although UCE is also used to market even legitimate goods and services, users often frown on this type of advertising and frown at companies that advertise in this way.
- **Phishing.** These two-part attacks consist of legitimate-looking e-mail messages from large and well-known organizations (often financial institutions) that use some means to trick a user into visiting a web site. This web site will resemble a legitimate site and ask for login or other credentials or information such as credit card numbers, social insurance, numbers, or other information that will be used to defraud the user. The most common phishing scams purpose to come from banks that ask users to log in and confirm account numbers or credit card numbers.
- **Malware.** Spam is often used to directly deliver malware to users' computers, but it is also often used to lure people to web sites that contain malicious code in the form of viruses, worms, or bots.

Pharming In a pharming attack, an attacker directs all traffic destined for a particular web site towards an imposter web site. The attack diverts traffic by "poisoning" the organization's DNS servers or by changing the **hosts file** on individual users' systems.

For instance, an attacker may wish to defraud users by stealing their online banking credentials for the well known (and fictitious) Spendthrift Savings and Loan (ssloan.com). The attacker will set up a phony site that looks just like the real ssloan.com site. Then, the attacker will attack organizations' DNS servers in an attempt to poison their cache files. The attacker might also craft some malware that will insert a phony record into users' hosts file on their workstations.

Both attack methods will result in users' browsers going to the *phony* ssloan.com web site instead of the legitimate one. Users who do not notice this will enter their ssloan.com credentials, which the attacker can later use to log in to the *real* ssloan.com to steal users' funds.

Figure 3-5 shows how a typical pharming attack works.

Spyware and Adware **Spyware** and **adware** encompass a wide variety of means that have been developed to track the behavior of users' Internet usage patterns. While not strictly malicious, many find the techniques and motives used by spyware and ad-ware to be suspicious and an invasion of their privacy. Spyware and adware take on many forms including:

- **Tracking cookies.** Many web site operators will track users' individual visits to web sites through the use of tracking cookies that may accompany banner ads. There are a few, very large banner ad placement companies, and their use of cookies can range from legitimate to downright abusive.

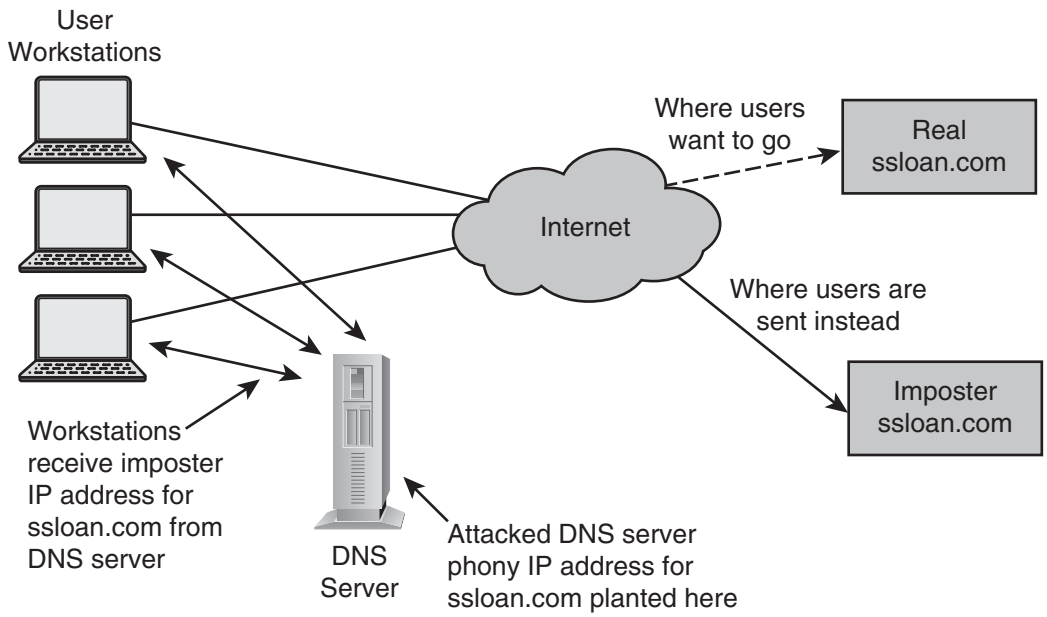


Figure 3-5 Pharming attack redirects users to a phony application server

Source: Redrawn with permission from S. Staniford, V. Paxon, and N. Weaver, "How to 0wn the Internet In Your Spare Time," Proc. USENIX Security Symposium 2002

- **Web beacons**. Sometimes known as "web bugs," web beacons are tiny 1×1 pixel images that are embedded in web pages as a means for tracking users' Internet usage. An alternative to cookies, web beacons are far more difficult to detect and block.
- **Browser helper objects (BHOs)**. Sometimes they take the form of helpful toolbars, but at other times they are completely invisible and "stealthy." BHOs can be used to track use of users' Web browsers. I should be quick to point out that not all BHOs are malicious—many serve a useful and legitimate purpose.
- **Key loggers**. Arguably the most invasive form of spyware, a **key logger** actually records a user's keystrokes (and, often, mouse movements and clicks) and transmit that data back to a central location.

Malicious Software Countermeasures Several measures are needed to block the ability for malware to enter and run on a system. These countermeasures include:

- Anti-virus
- Anti-rootkits
- Anti-spyware
- Anti-spam
- Firewalls
- Decreased privilege levels
- Penetration testing
- Hardening

Anti-virus **Anti-virus** programs run on a system and employ various means to detect the possible entry of malware and have the ability to block its entry. Anti-virus software can also remove malware if it is already present on the system.

Anti-virus software uses two primary means for detecting malware: signature-based and heuristics-based. In signature-based detection, the anti-virus program periodically downloads an updated list of virus "signatures"—usually fragments of actual malware—that anti-virus software can use to match and confirm the presence of malware. In heuristics-based detection, the anti-virus software detects malware's presence through its anomalous behavior on the system.

Anti-virus programs are found in many places in an organization as part of a defense in depth to prevent the unwanted consequences of malware. The places where anti-virus software can be found include:

- **End user workstations**. In the beginning this is the only place where anti-virus software was used. Today this is considered the last defense.
- **E-mail servers**. Because so much malware spreads through e-mail, e-mail servers are a natural choice.
- **File servers**. Because malware can hide in documents and program files, anti-virus software is often utilized on file servers.
- **Web proxy servers**. Many organizations funnel all web traffic (that is, the inbound and outbound traffic that results from employees' visiting web sites) through proxy servers.

This can help the organization control web usage by blocking access to unwanted (porn, gambling, hate-related, illegal, and so on) web sites and also block malware.

- **Security appliances**. The drive to simplicity and lower TCO has given rise to a generation of all-in-one security appliances that perform several functions including firewall, web content filter, spam filter, and anti-virus.

Anti-rootkit Software

Anti-rootkit software uses techniques to find hidden processes, hidden registry entries, unexpected kernel hooks, and hidden files in order to find rootkits that may be present on a system. Anti-rootkit software programs use various means to find these hidden objects in a system, generally through the use of directly examining the running operating system instead of using tools that the rootkit may have been able to manipulate.

Anti-spyware Software

Software to block spyware and adware is similar to anti-virus software: it monitors incoming files and examines them against a collection of signatures, and blocks those files that match known signatures.

Like anti-virus software, **anti-spyware** can scan a hard drive to identify spyware, adware, and other unwanted programs, and remove them as directed by the user.

It used to be necessary to use separate, unbundled anti-spyware programs, but increasingly anti-spyware accompanies many of the popular anti-virus programs. In the long run, separate anti-spyware may disappear from the market altogether, the feature reduced to an option in anti-virus programs, whether or not to detect and block spyware.

Anti-spam Software

Spam blockers effectively eliminate most of the spam coming in to an organization, blocking the majority of the unwanted e-mail that carries malware, phishing scams, fraudulent advertising, and porn.

Spam filters examine all incoming e-mail messages and perform a content analysis in order to arrive at a "score" for each message. Messages whose score exceeds a threshold are diverted to a spam quarantine or deleted. Messages whose score does not exceed the threshold are delivered to the end user's inbox.

Blocking spam is an inexact science because spammers are always finding new ways to get through, and the spam filters seem to be in a game of endless catch up. Still, the better spam blockers eliminate 95–98% of incoming spam, while inadvertently flagging legitimate e-mails as spam less than one percent of the time.

There are four common spam blocking architectures in use, including:

- **Client-based**. In this architecture the spam blocking software resides on the end user workstation. This method has fallen out of favor because of the administrative overhead required to keep yet another defensive software program operating on client workstations. Another disadvantage of this model is the failure to eliminate spam from the network, since it has to be delivered to the end user before it is detected and removed.
- **E-mail server-based**. Here, the spam blocking software is installed on the e-mail server. The advantage to this method is that the spam blocking software is centralized, and spam is not delivered to end users.

- **Appliance-based**. A spam blocking appliance sits in front of corporate e-mail servers, blocking all incoming spam and delivering only the legitimate e-mail to the mail server. The advantage of this architecture is that the e-mail server is relieved of the burden of receiving all of the legitimate e-mail plus the spam.
- **Spam blocking service**. In this model, incoming e-mail is delivered to an off-site spam blocking service provider that filters out the spam and delivers only legitimate e-mail to corporate e-mail servers. The advantage of this model is that spam no longer consumes network bandwidth on corporate Internet connections.

Most organizations opt to allow users to be able to access their own quarantines. This gives end users the ability to recover any incoming e-mails that were incorrectly marked as spam.

Firewalls

Firewalls are the time-tested and still-preferred means for blocking unwanted network traffic from crossing a network boundary. Firewalls are typically used as perimeter devices, protecting organizations from unwanted traffic that originates from the Internet.

Firewalls examine each inbound packet and compare the source and destination addresses and port numbers against a list of permitted and blocked addresses. The list of permitted and blocked addresses on a firewall is called the list of *firewall rules*.

Firewalls are also used to segregate various networks within organizations. Examples of such uses include:

- **Isolation of labs**. In organizations where employees are developing and experimenting with software and systems in a lab, often a firewall will be used to isolate the lab from the rest of the enterprise. A firewall in this case will protect the enterprise from the lab—as well as protect the lab from the enterprise.
- **Isolation of production service networks**. Organizations that are network-based service providers often segregate their production networks from their corporate networks. This prevents ordinary corporate users from being able to directly access production systems.
- **Demilitarized Zones (DMZ)**. Online applications that store or process sensitive information often require firewalls to separate front-end systems from back-end systems, so that back-end systems like database management servers cannot be directly accessed from the Internet. Firewall rules separating tier-one and tier-two systems provide an additional layer of defense by permitting only front-end applications servers to directly contact back-end database servers. Figure 3-6 shows a typical DMZ architecture with firewalls isolating each layer.
- **End user workstations**. Most end user workstations are laptop computers that are often taken outside the confines of the enterprise network and connected directly to the Internet. This necessitates the use of so-called *personal firewalls* that are used to block unwanted traffic. Personal firewalls are software programs that operate on workstations, and like physical network firewalls, examine each incoming network packet and make a pass-or-drop decision based upon a preconfigured set of rules.

Decreased Privilege Levels

When malware successfully breaks into a system and is executed by the user, the malware usually is executing with the same privilege level as the user. This is a serious problem for most organizations, since the default privilege level for most end

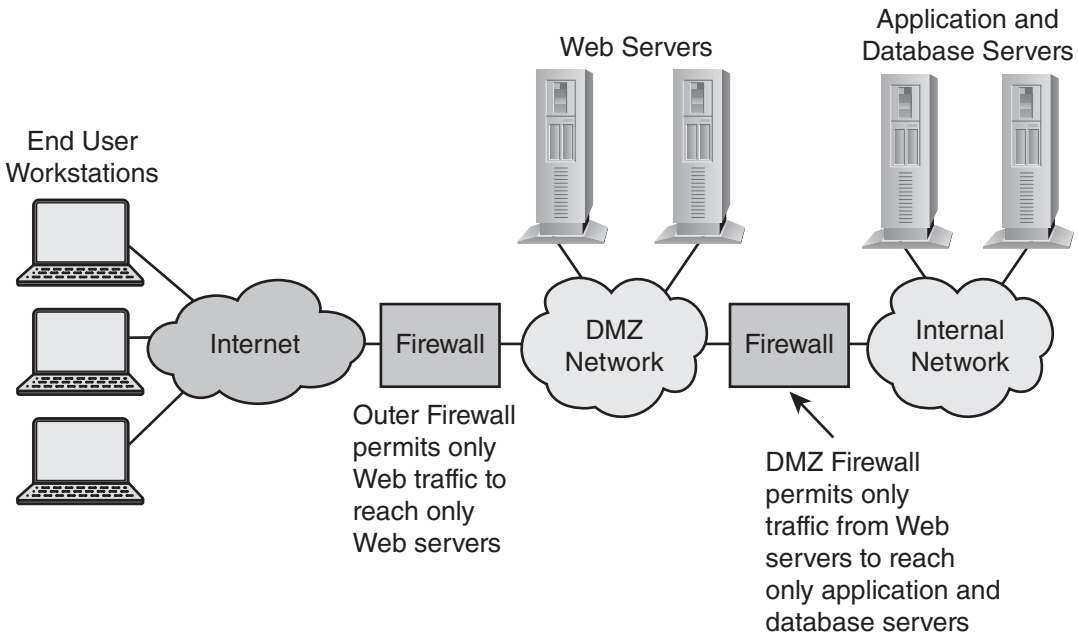


Figure 3-6 Typical DMZ network architecture protected by firewalls

Source: Course Technology/Cengage Learning

user workstations is set to "administrative." In other words, when the end user has administrative-level privileges on a system and the user has activated malicious code, then the malicious code is able to execute with administrative privileges and do whatever it wants on the system, including any of the following:

- Change system configurations
- Alter or remove system programs
- Disable anti-virus, anti-spyware, and firewall software
- Access, change, or remove any file on the system

For this reason, many organizations are moving towards a model where end users do not have administrative privileges on their workstations, but instead operate at an "end user" privilege level. Because users at end-user privilege level are not able to make most changes to the operating system, any malicious code that the user unintentionally brings in will likewise be unable to make changes to the operating system. The risk of harm to the end user and to the enterprise at a whole is reduced considerably.

A side benefit of reducing user privileges to end user level is a decreased number of tech support calls to repair *uh-oh*'s, when often-inexperienced end users muddle up operating system configurations.

Penetration Testing Rather than simply relying upon security configuration settings, an organization should also test the settings by using tools to simulate a hacker's attempt to find weaknesses in a system. Such tests are known as *penetration tests*, often known as "pen tests."

Pen tests send network packets to a target system in an attempt to discover the network-based services that are present and active on a system, and whether any of those services have any exploitable vulnerabilities. If any vulnerabilities are present, they'll be noted along with their severity in a report or other output created by the pen testing tool.

The object of penetration testing is to discover and fix vulnerabilities before a hacker is able to discover and exploit them. It's typically a race against time to fix serious vulnerabilities before hackers discover them, particularly on high-value sites.

Hardening Server operating systems are very complex and often are pre-configured for a wide variety of tasks. This often means that many of the programs and features that are available are activated by default. The result is a server with its necessary feature(s) activated, plus many additional unnecessary features also activated and ready to accept input from any friendly or unfriendly party.

If any vulnerability is discovered in any of these unnecessary features, an attacker may be able to exploit one or more of these vulnerabilities and break in to the server. Certainly this type of situation is one that should be avoided. The practice of **hardening** is used to identify and remove these vulnerabilities.

Situations like this have led to the publication of "server hardening" guidelines that, when followed, result in a server that is "lean and mean," with far fewer potential vulnerabilities. The common principles behind server hardening include these concepts:

- **Deactivate or remove unnecessary services**. Every software component that is not required for a server to fulfill its purpose should be either deactivated (good) or removed altogether (better).
- **Robust network configuration**. Servers' TCP/IP configuration should be set to recommended values to make the server more able to repel network-stack attacks.
- **Robust software configuration**. Any required software programs on the server should be configured to be as secure as possible. Server programs should be configured to run with the lowest possible privilege levels.
- **Administrator account hardening**. Administrator account names should be changed, and passwords set to highly complex and not easily broken values. All unused administrator accounts should be locked or removed.
- **Security patches**. Servers, particularly those that are exposed to the Internet, should have up-to-date security patches installed regularly.

Server hardening guides are available from operating system vendors (Microsoft, Sun Microsystems, Red Hat, etc.) as well as from security organizations like the U.S. National Institute for Standards and Technology (NIST), the U.S. Computer Emergency Response Team (US-CERT), and the SANS Institute. Organizations often use one or more of the server hardening guides or build one of their own, borrowing guidance from one or more of these guides or others.

Input Attacks

Applications and tools often request input from users. A common method of attacking an application is to provide data that causes unexpected behavior in the application.

Input attacks—sometimes called malformed input attacks or **injection attacks**—are designed to exploit weaknesses in the application by causing unexpected behavior including:

- **Elevation of privileges**. The attacker will input specially coded data in an attempt to cause a malfunction that will result in the attacker having a higher level of access or privilege in the application.
- **Execution of arbitrary code**. The attacker may wish to run specific commands on the target system.
- **Malfunction**. The attacker may wish to cause the application to malfunction and be in a disabled state for legitimate users.
- **Abort**. The attacker may wish to cause the application to completely abort and thus be unavailable for any legitimate use.

Types of Input Attacks Several types of input attacks can be launched against an application, including:

- **Buffer overflow**. This is discussed in detail earlier in this chapter.
- **Integer overflow**. An attack where the attacker attempts to cause an application to perform an integer operation that will create a numeric value larger than can be represented in the available storage.
- **SQL injection**. In this type of attack, the attacker inserts specially coded and delimited SQL statements into an input field in the hopes that the injected SQL will be executed on the back end. This type of attack is possible in applications that dynamically build SQL statements.
- **Script injection**. Similar to SQL injection, an attacker inserts script language into an input field in the hopes that the scripting language will be executed.
- **Cross-site scripting (XSS)**. An attack where an attacker can inject a malicious script into HTML content in order to steal session cookies and other sensitive information.
- **Cross-site request forgery (XSRF)**. This is an attack where malicious HTML is inserted into a Web page or e-mail that, when clicked, causes an action to occur on an unrelated site where the user may have an active session.

Input Attack Countermeasures Measures that can be used to prevent input attacks include:

- **Effective input field filtering**. Input fields should be filtered to remove all characters that might be a part of an input injection. Which characters are removed will depend upon the types of software used by the application. For numeric fields, reasonableness checks should be performed to prevent overflow attacks.
- **Application firewall**. Network firewalls inspect only the source and destination addresses and the port numbers, but not the contents of network packets. Application firewalls examine the contents of packets and block packets containing input attack code and other unwanted data.
- **Application vulnerability scanning**. Organizations that develop their own applications for online use should scan those applications for input attack vulnerabilities, in order to identify vulnerabilities prior to their being discovered and exploited by

outsiders. Application vulnerability scanning is discussed in more detail later in this chapter in the section, "Security in the software development life cycle."

- **Developer training**. Software developers should be trained in secure application development techniques. This is discussed in more detail later in this chapter in the section, "Security in the software development life cycle."

Object Reuse

Many system resources are shared in multiprocessing systems. This includes memory, databases, file systems, and paging space. When one process utilizes a resource, the process may write some information to the resource temporarily.

Operating systems generally zero out or overwrite memory used by a previous process before allocating it to another process. But a flaw in the design of an OS may make it possible for a process to discover the residual data left by a process that previously occupied a particular part of memory. This flaw is known as **object reuse**.

Similarly, processes may create temporary files in a file system or records in a database that are not intended for use by other processes. However, design flaws or malfunctions may make it possible for a process (or malicious code) to discover and use this residual information.

Object Reuse Countermeasures

Several measures should be taken to prevent object reuse vulnerabilities. Among these measures:

- **Application isolation**. Applications should be isolated to individual systems. In this way, applications are less likely to encounter residual information left by other applications.
- **Server virtualization**. Often it is not feasible to isolate applications to one-per-machine. However, virtualization technology may make it more cost-effective to isolate applications by running them on virtual machines.
- **Developer training**. Software developers can be shown how to write secure software that does not leave residual code that can be used by other processes.

Mobile Code

Also known as executable code, active content, and downloadable content, **mobile code** can be downloaded or transferred from one system for execution on another system. Examples of mobile code include:

- **Active website content**. This includes ActiveX, Java, JavaScript, Flash, Shockwave, and so on. This content originates on a Web server and executes on a user's workstation. Depending upon the technology associated with the downloaded content, this mobile code may have restricted access to the end user's system or may have full control over it.
- **Downloaded software**. This includes software of every kind from legitimate (and not-so-legitimate) sites. Some of this software may be purely benign, but others can be Trojan horse programs and worse. Some is outright malware, with or without a disguise.

Mobile Code Countermeasures Measures to protect systems from unwanted mobile code include the following:

- **Anti-malware**. This includes anti-virus, anti-spyware, and so on. These protective programs should be in place, properly configured, and up-to-date.
- **Reduced user privileges**. End users should not be permitted to install or execute mobile code on their workstations, except in explicitly permitted situations such as company-produced mobile code.
- **Mobile code access controls**. Access controls should be in place to prevent unauthorized persons from downloading any mobile code that they are not permitted to access or use.
- **Secure workstation configuration**. Workstations should be configured to restrict mobile code except in cases where specific mobile code is permitted. This may involve centralized workstation configuration that cannot be defeated or circumvented by end users.

Social Engineering

A social engineering attack is an attack on the *personnel* in an organization. Usually the purpose of a social engineering attack is to gain secrets from individuals that can later be used to gain unauthorized access to the organization's systems. The social engineer uses a technique known as **pretexting** in an effort to pretend that they are someone else.

Social engineering owes its success to basic human nature: people are willing to help others in need and "be the hero." Social engineers prey on this weakness in feigned calls for assistance.

Social Engineering Countermeasures The best countermeasure against social engineering is education: people in the organization, particularly those with administrative privileges (system administrators, network administrators, database administrators, and so on), need to be educated on the proper procedures for providing company sensitive information to others. For instance, all calls to staff members about IT access should be referred to the IT helpdesk, calls about legal contracts should be referred to the legal department, and so on.

IT helpdesk personnel (and those in other parts of the organization that take calls from employees) should have precise instructions on identifying other staff members and on what information is permissible to provide (and what is not).

Back Door

A **back door** is a mechanism that is deliberately planted in a system by an application developer that allows the developer or other person to circumvent security. Back doors may be present in an application for several reasons including:

- **To facilitate testing during application development**. For instance, back doors can be activated by entering specific values that will cause the program to enter an interactive debug mode.
- **To facilitate production access**. For example, a back door is created so that a developer can access an application while it is in production. This would be considered an

inappropriate use of a back door, since developers should never have access to a production application or production data.

- **To facilitate a break-in.** Sometimes back doors are inserted into an application to permit an unauthorized party to access application functions or data that the party should not have access to. This is clearly inappropriate. This use resembles a **logic bomb**, which is discussed in the next section.

Back Door Countermeasures Back doors can be difficult to find, particularly if they are inserted for disreputable purposes. Routine functional testing and QA testing may not reveal back doors, whatever their purpose. Instead, other means are required to find them, including:

- **Code reviews.** When one developer makes changes to a software application, one or more other developers should examine the software to identify and approve of all changes. This should prevent both the "legitimate" back doors as well as illegitimate ones.
- **Source code control.** A formal source code management system should be used that will identify and record all changes made to the code. Such capabilities should make it easier for someone to more easily see all changes in the code, making it more difficult for someone to plant an illegitimate back door.
- **Source code scanning.** Tools that are used to scan static source code for security vulnerabilities should be able to find back doors (or at least flag the unusual logic associated with a back door).
- **Third-party code reviews and assessments.** Occasionally, outside personnel should be contracted to examine static and running code in order to identify any vulnerabilities and undesired features such as back doors. A third-party organization will be more motivated to find anomalies in software than its own developers.

Logic Bomb

Logic bombs, sometimes known as **time bombs**, are instructions deliberately placed in application code that perform some hostile action when a predetermined condition is met. Typically a logic bomb consists of code that performs some damaging action on a date in the distant future. Most often, a developer will plant a logic bomb in an application if he believes he will be terminated from employment. The logic bomb will "go off" at some later date, and the terminated programmer will feel that he got his just revenge.

Logic Bomb Countermeasures Logic bombs and back doors are very similar: both involve unwanted code in an application. The countermeasures for logic bombs are the same as for back doors: code reviews, source code control, source code scanning, and third party assessments. See the previous section on back door countermeasures for additional details.

Security in the Software Development Life Cycle

The **software development life cycle** (SDLC) is the collection of processes and procedures used to develop and maintain software applications. Applications can be far more secure if the SDLC includes the right security-related activities in the right places. The details discussed in this section are:

- Security in the conceptual stage
- Security application requirements and specifications
- Security in application design
- Threat risk modeling
- Security in application coding
- Security in testing

NIST 800-64, *Security Considerations in the Information System Development Life Cycle*, is a high quality standard that was developed by the U.S. National Institute of Standards and Technology. Security and development professionals are urged to incorporate recommendations found in this work.

Security in the Conceptual Stage

Changes to applications (as well as the creation of new applications) begin with conceptual ideas. Even at the idea stage, some notions of security need to be taken into account. Example mentions of security might include:

- **Sensitive information**. What sensitive information will be present in the application? Should the information be protected?
- **Information flows**. How will sensitive data be transmitted into the application? How will sensitive data be transmitted out of the application? Are any of these information flows with outside organizations?
- **User access**. Who are the application's users, and how will they access the application?
- **Administrative access**. What personnel will be required to access the application and its supporting infrastructure? How will these accesses take place?
- **Third-party access**. Will any third-party personnel be required to access the application? How will this access be controlled?
- **Regulatory requirements**. Are there any regulatory requirements which must be met in this application? Examples include PCI DSS, HIPAA, GLBA, FERC, NERC, and Sarbanes Oxley in the U.S., and the European privacy law 95/46/EC.
- **Use of services infrastructure**. Will the application utilize any enterprise wide services such as authentication, single sign-on, configuration management, or access to centrally managed storage on a SAN or NAS?
- **Application dependencies**. What other applications will depend upon this application? Which other applications does this application depend upon?

An organization with a mature development life cycle may wish to develop worksheets for conceptual-stage activities that will help facilitate the identification of security-related issues that need to be addressed early in the development of the application.

Security Application Requirements and Specifications

After the application has been conceptualized, one or more persons will be charged with the development of functional requirements and specifications. Requirements and specifications are detailed statements that describe the behavioral characteristics of the application.

Requirements and specifications can become quite voluminous. Even for a modest project, an application can have hundreds of requirements and specifications that easily exceed one hundred pages in length!

To give you an idea of how detailed the requirements and specifications should be: a developer should be able to develop the entire application, all the way down to individual input forms and fields, and produce absolutely correct operating code without ever having to speak to another person about it. Not that a developer *should* develop this way, but only to say that a developer *could*, because the requirements and specs should be *that detailed*.

Requirements and specifications should provide detailed descriptions of every form, every field, every calculation, and every page, column, heading, and subtotal in every report. Every inbound and outbound flow should be described in exhaustive detail, and every behavioral characteristic in the application should be described in enough detail so that the developer can develop everything.

Further, the requirements should be able to form the kernel of a completely detailed test plan, so that every function of the application can be tested and verified, without the need for any additional functional information about the application.

Characteristics that should be included in requirements and specifications include:

- User and administrative roles
- Access control mechanisms and settings
- Audit logging
- Configuration management
- Workflow
- Use cases
- Reports
- Interfaces to other internal and external systems

Security in Application Design

When the application's detailed functions and specifications have been completed, the application itself can be designed. The design elements that can be completed in the application design include all database schema, input and output records and fields, workflows, use cases, user roles, administrative roles, audit logs, connections to management systems and services, and other points of integration with other applications, systems, and services. These elements and concepts are described in detail in this section.

When the application's functional specifications and requirements have been developed, creation of the application's design should be straightforward. Still, the designers may discover ambiguities and may need to consult with the persons who developed the functional specs and requirements to eliminate the ambiguities, allowing the designer to complete the design.

The design should be reviewed by those who developed the functional specifications and requirements, to ensure that the design properly reflects the application's specs and requirements. The application's developers should also be present in the review, since they are the personnel who will soon be building the application.

The resulting application design should accurately depict the application's specification and requirements and be smoothly and harmoniously integrated into the overall technology environment.

Threat Risk Modeling

Building an application according to sound requirements, specifications, and design, and testing against those same bodies is not enough to know whether the application will be vulnerable to known threats. **Threat risk modeling** should be performed, to identify those threats that may require controls or other countermeasures as a part of the application's design.

The proper time to perform threat risk modeling is after the application has been designed, but before the application coding begins. Threat risk modeling can be thought of as a security test of the design, like a stress test, that is conducted before the application is built. This is similar to the kinds of computer model stress testing that is performed on large engineering structures such as dams and bridges. Assuredly those kinds of structures are thoroughly tested for physical strength before a shovelful of cement is poured or a pound of steel is erected. Similarly, applications should be stress tested with threat risk analysis before anything is built.

Suggested tool for threat modeling:

- Microsoft Threat Analysis and Modeling

Security in Application Coding

When all requirements, specifications, design, risk threat modeling, and review of all of these works have been completed, application coding may begin. To many, this may seem an arduous and burdensome process, but nowhere in the software development life cycle is it more cost effective to ensure that an application is secure than in the specifications and design phase.

Remember the "1-10-100 Rule". It costs ten times as much to secure an application after it has been developed, and one hundred times as much to secure an application after it has been implemented. Clearly the best way to secure an application is in its design.

Common Vulnerabilities to Avoid Applications should be coded defensively to ensure that they are free of vulnerabilities. The most common vulnerabilities in Web-based applications, according to OWASP (Open Web Application Security Project—a non-profit organization dedicated to the secure development of Web applications)—are:

- **Unvalidated input**. All input must be properly validated, so that unsafe or unexpected input values are not passed into the application.

- **Broken access control**. Application users should not be able to manipulate the application to circumvent security settings or role-based access controls.
- **Broken authentication and session management**. Application users should not be able to manipulate authentication and session management in order to bypass security controls.
- **Cross-site scripting attacks**. Applications should parse all input data and strip out delimiters and other data that could be a part of a scripting attack.
- **Buffer overflows**. Applications should do proper boundary checking on all inputs to prevent unexpectedly long input strings to cause unexpected behavior.
- **Injection flaws**. The application should reject all script injections, for example SQL statements or JavaScript.
- **Improper error handling**. All application errors should be handled gracefully and properly, so that the application does not produce error statements that betray internal information about the application.
- **Insecure storage**. All data should be stored using proper access controls, and encryption when appropriate.
- **Denial of Service**. The application should not malfunction or abort because a user (or process) provided malformed data in an input field.
- **Insecure configuration management**. All components of the application environment and supporting infrastructure should be configured securely so that all components are free from vulnerabilities.

Use Safe Libraries One great way to avoid many common vulnerabilities (such as script injection and **buffer overflow**) is to use source code libraries that have been thoroughly tested against these vulnerabilities. Objects and functions in these libraries should be used to parse all input strings, for example.

Security in Testing

After the application has been developed, it must be tested to ensure that it was coded properly and is free from errors. A proper software development project has a comprehensive set of functional specifications and requirements, which become a part of the application's test plan.

All functional aspects of the application need to be tested. This includes all fields, workflows, use cases, reports—everything. Detailed testing should be organized and planned, and all test results archived.

The entire application environment needs to be tested with security testing tools to ensure that the application is free from security defects. Applications that are web-based should be tested with scanning tools that are designed to identify common and not-so-common web application vulnerabilities. The two leading tools made for this purpose are WebInspect from HP/SPI Dynamics and AppScan from IBM/Watchfire. Figure 3-7 shows a screen shot of AppScan.

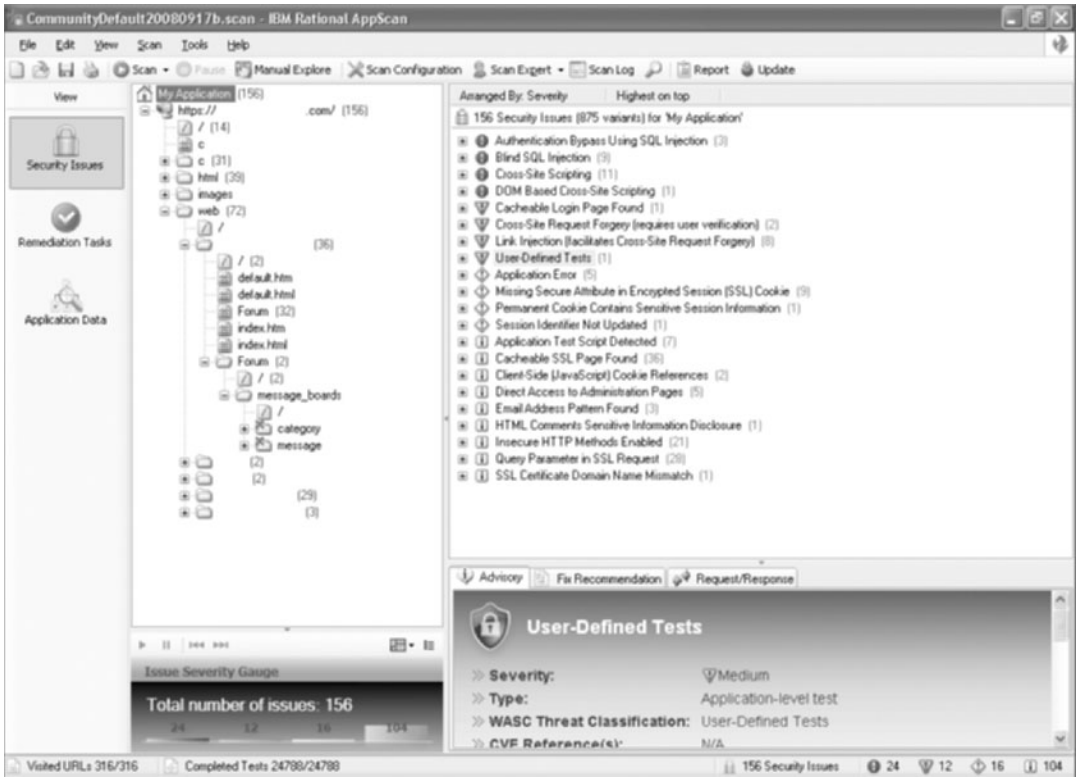


Figure 3-7 IBM/Watchfire's AppScan is used to identify web application vulnerabilities

Source: Course Technology/Cengage Learning

Protecting the SDLC Itself

In addition to the measures described above that result in more secure software, other steps should be taken to protect the SDLC process itself. These measures include:

- **Source code access control**. Only authorized developers should have access to all application source code. Fewer still should have permission to make changes to application source code.
- **Protection of software development tools**. All tools and libraries used to develop software should be protected from unauthorized access and modification. This will help reduce the possibility of vulnerabilities being introduced into an application through tampering with its development tools.
- **Protection of software development systems**. Systems used in the development of applications, ranging from developer workstations to source code repositories should be protected with the same rigor as application servers. As application servers become more hardened, software development systems will otherwise become the next "soft target."

Application Environment and Security Controls

Applications typically require their own security controls, in order to manage and measure activities and events performed by the application. These security controls are required in order to control and verify the integrity of the application, often a necessary task in environments where applications control critical business processes that must be audited from time to time. Without these controls it would be impossible to be able to verify that the applications are operating properly.

The controls that are required by applications are:

- Authentication
- Authorization
- Audit logging

Authentication

An application must unambiguously know the identity of all users who access it. This is accomplished with authentication, where a user proves their identity to a system or application, usually by providing a userid and password. The application's designers will decide whether the application should perform authentication on its own (which includes storing userids and passwords in the application's database) or whether the application should instead leverage an enterprise-wide authentication service that my be implemented with LDAP (Lightweight Directory Access Protocol) or Microsoft Active Directory. Centralized authentication lowers the cost of user access administration, and end users will have fewer userids and passwords to remember.

Authorization

One of the two purposes of access control is to determine whether the individual who wishes to access the application is allowed to. The second purpose is to determine what data and functions the person is permitted to do. This is known as **authorization**.

Authorization is the concept of giving users access to data and functions. An application controls access typically by reading some sort of a *profile* that states which functions a user is permitted to perform. This may seem simple enough, were it not for the fact that some enterprise applications (like a financial management application, customer relationship management application, or a manufacturing control application) could have hundreds of functions and thousands of users. Managing those users and functions could require considerable administrative overhead. That is why role-based access control was invented. This is described in the next section.

Role-based Access Control In larger applications with hundreds or even thousands of assignable functions and thousands of applications, managing, tracking and auditing these function assignments could become a logistical nightmare. It's for this reason that **role-based access control** is used by many applications. Role-based access control, often known as RBAC, simplifies access control in large applications.

In an RBAC-enabled system, analysts and administrators develop a set of *roles*, which are typically tied to organization job descriptions. Permissions for each of the functions are assigned to each role, which represents the typical worker with the job description that corresponds to the role. Then, each user of the system is assigned to the *role*, which automatically gives the user the permissions that are set up for the role.

Audit Log

An **audit log** is a listing of all of the significant events that occur in an application environment. The purpose of an audit log is to provide a running record or diary of all events that take place in an application: when the events occurred, who performed the events, and details about events such as the details about changed data.

Applications must separately record all significant events and transactions in an audit log. A separate audit log provides a linear (time-based) sequence of events that take place throughout the application's use.

A precise list of the events and transactions that should be recorded is determined in the requirements and functional specifications stage in the software development life cycle (SDLC). The SDLC is examined in greater detail earlier in this chapter.

Audit Log Contents At a minimum, the following information must be present in each audit log entry:

- **Date and time**. The exact time of the event. The time zone should be unambiguous.
- **User**. The userid or name of the user associated with the event.
- **User's location**. This may be a terminal id, IP address, or other identifying information to show where the user was likely located when the event occurred.
- **Event name**. The name of the event (such as "Update salary").
- **Relevant data**. If a user changed a value in a database, the audit log should show the old and new values. If a new record is entered, its original data should be included.

Audit Log Protection Audit logs must be protected against alteration, destruction, and tampering. Characteristics of audit logs should include:

- **Free from alteration**. No individual should be able to alter any information in an audit log. Ideally an audit log should be written to write-once media.
- **Free from erasure**. The audit log should not be able to be erased.
- **Free from unauthorized initialization**. Only authorized individuals or mechanisms should be able to initialize an audit log. Audit log initialization should itself be an audit event.

Databases and Data Warehouses

Databases are often used to store business data on information systems. While end users may store small pieces of data in documents, spreadsheest, and presentation file, most applications

store their information in database management systems (DBMSs) like Microsoft SQL Server, Oracle, IBM DB2 and Sybase.

Database Concepts and Design

This section describes various architectures used by database management systems. A **database** is an ordered collection of data that exists for a common purpose. For instance, an organization may build a database of its employees in order to store information about employees including contact information, compensation, benefits, continuing education, and disciplinary action.

A **data warehouse** is a type of database that is used for decision support and research purposes. For example, an online retailer may build a data warehouse that consists of all of its customer transactions. Analysts can use various tools to access and analyze historic transactions in order to identify trends that may help the organization to improve its business in the future. Business intelligence tools can help an analyst to easily identify trends and conditions that may otherwise be unapparent.

Transactions are used to update data within a database. For instance, an online banking application utilizes transactions to record deposits, withdrawals, and other activities in customer bank accounts.

Database Architectures

Database management systems (DBMSs) have a design that governs how data will be organized. Generally, a given make and model of database will be built around one particular model. If you prefer that your data be stored using a different model, then you will need to find yourself a different database product.

The common architectures used by DBMSs are:

- Hierarchical
- Network
- Relational
- Object oriented
- Distributed

Hierarchical Databases

In a **hierarchical database**, data is organized in a tree structure. Each field or record has only a single parent field or record, but can have zero, one, or many child fields or records. An example of a hierarchical data model is the Internet's Domain Name Service (DNS) model. The hierarchical database model is considered legacy, because this model has not been used by database producers in many years.

Network Databases

Network databases are an extension of hierarchical databases, in which records can be "networked" to other records elsewhere in the database than through the hierarchy itself. Like hierarchical databases, network databases are considered legacy.

Relational Databases

Fields and records in **relational databases** are designed to be related to other fields and records. A relational database is two-dimensional, having *rows* and *columns*

(sometimes known as fields). The structure of a relational database is defined by its *schema*, which is essentially a lengthy keywords-delimited text file called Data Definition Language (DDL) that define tables, rows, columns, keys, and indices. Tools called *data modelers* are used to create a relational database schema.

The power of relational databases comes from relationships, which are used to identify related records. For instance, a field in a *sales* table can be used to store a *salesman* number, a *foreign key* that points to the *primary key* on a salesman table elsewhere in the database. Other tables can also have a salesman field that will also point back to the salesman table.

Large applications can have databases that contain hundreds of tables, all linked together through these relationships.

Object Oriented Databases In an **object oriented database (OODB)**, data is organized and stored as objects. Like OO programming languages, these objects can be organized with classes, inheritance, and encapsulation. The operations that can be performed with OODB database objects are stored in the objects themselves.

Distributed Databases **Distributed databases** are so-called because of their physical nature more than by whether they are relational, hierarchical, or object oriented. Distributed databases may on one system, on two or more systems in a single location, or in several geographic locations.

Database Transactions The real power in databases comes from the ability for software applications to perform transactions. By this I mean that the database management system (DBMS) becomes the engine for storing, changing, and retrieving data, relieving the software developer from the details of file manipulation. In the vernacular, the programmer can write simple language to instruct the database, "get record number 1234 from the *salesman* table and change the *salary* value to 3000," or, "create a new record in the products table with the following data in the fields …"

SQL is the common language used in software applications to communicate these transactions to relational databases. SQL is a standard data manipulation language supported by nearly all modern programming languages, which usually provide some easy means for constructing SQL statements to manipulate data in the RDBMS.

Relational databases also have a notion of "transactional integrity" in which a complex transaction will never be partially completed under any circumstance. This is achieved by delimiting a series of transaction statements with the terms, "Begin work" and "Commit." For example:

```
BEGIN WORK
INSERT INTO salestable (number, name, phone) VALUES
('551', 'Scott Brewer', '206-555-1212');
UPDATE commission SET rate= '440' WHERE
salesman='551';
COMMIT;
```

In this example, the developer can be confident that the two commands (insert and *update*) will both be performed, or neither will be performed. Regardless of any error or malfunction that can occur, a situation where only one of these two commands has completed will not happen.

Database Security Controls

Databases have security controls that determine who can access a database, as well as which data a user or role is permitted to view or change. Two primary ways of controlling access in a database are **access controls** and **views**.

Access Controls Databases embody the concept of a userid and password that must be provided before any person can access the database. But since most users don't access a database directly, often user authentication is done at the application layer, and then the application accesses the database directly, on behalf of the user.

RDBMSs use Data Control Language (DCL) to define which users are able to view and manipulate which tables, records, and fields in a database. The DCL serves as a way to configure a database's **access controls**—the mechanisms used to control how objects (in this case, data) may be accessed by users. A sample DCL statement reads:

```
GRANT SELECT ON salestable TO user1, user2, user3.
```

Views A **view** is a virtual table that can be created in a relational database. A view does not take up additional data storage. Views can be used to control access to data in two ways:

- **Access controls on views.** Users who need to be able to view certain information can be given permission to access the view only, but not the underlying tables.
- **Include only the viewable fields.** If users should be able to see some fields but not others, a view can be created that includes only the fields that they are permitted to see.

Chapter Summary

- Applications are computer programs that perform useful work for people. The common types of application programs are agents, applets, client-server, distributed, and Web applications.
- Application languages are based upon design models. Four such models in common use are control flow, structured, object-oriented, and knowledge-based.
- Application software faces a large number of threats, including: buffer overflow, malicious software, input attacks, logic bombs, object reuse, mobile code, social engineering, and back doors. The types of malicious code include viruses, worms, Trojan horses, spyware and adware, pharming, and rootkits.
- Countermeasures against the threats to application software include: using safe programming languages and libraries, firewalls, anti-malware tools (anti-virus,

anti-spyware, anti-rootkit, etc.), decreasing application privilege levels, application scanning, penetration testing, source code reviews, developer training, and system hardening.

- Social engineering is an attack on personnel in an attempt to trick them into giving up secret information.
- The software development life cycle (SDLC) is the collection of processes and procedures used to design, build, and maintain software. Security needs to be a part of every of the SDLC to ensure that the application that is being built and maintained has security incorporated into the design instead of added on at the end of the project. Also, all project information including requirements, design, test plans and results, and source code need to be protected against unauthorized access and use.
- Security controls are required to control and verify the integrity of the application. The controls that are needed include authentication, authorization, and audit logging.
- The types of databases are hierarchical, network, relational, object oriented, and distributed. Database transactions are the actions performed on databases when data is added or changed. Databases have access controls that control the actions that users may perform and who may perform them.

Key Terms

Access Control Any means used to control which subjects are permitted to access objects.

Adware Cookies, web beacons, and other means used to track individual Internet users and build behavior profiles for them.

Agent Small, standalone programs that perform some task for a larger application environment.

Anti-rootkit Software that uses techniques to find hidden processes, hidden registry entries, unexpected kernel hooks, and hidden files in order to find rootkits that may be present on a system.

Anti-spyware Software that is designed to detect and remove spyware.

Anti-virus software Software that is used to detect and remove viruses and other malicious code from a system.

Applet A small program that runs within the context of another program.

Application firewall A firewall that examines the contents of incoming messages in order to detect and block attempted attacks on an application.

Audit log The record of events that occur in an application environment.

Authorization The process of permitting a user to perform some specific function or access some specific data.

Back door A feature in a program that allows access that bypasses security.

Bot Malicious software that allows someone to remotely control someone else's computer for illicit purposes.

Class The defining characteristics of an object.

Client-server application An application in which user interface logic resides on a client system and data storage and retrieval logic resides on a server.

Configuration management The process of recording configuration changes that are made in an environment.

Control flow A computer language methodology where instructions are followed sequentially until a "goto" type statement is encountered, in which case the control is transferred to the location specified by the goto statement.

Cross-site request forgery (XSRF) This is an attack where malicious HTML is inserted into a Web page or e-mail that, when clicked, causes an action to occur on an unrelated site where the user may have an active session.

Cross-site scripting (XSS) An attack where an attacker can inject a malicious script into HTML content in order to steal session cookies and other sensitive information.

Data warehouse A database management system that is designed and built to store archival data for decision support and research purposes.

Database An ordered collection of data that exists for a common purpose.

Database management system (DBMS) A set of software programs used to manage large organized collections of data called databases.

Demilitarized zone (DMZ) A means of protecting application servers and the remainder of an enterprise network by placing them on a separate firewalled network.

Distributed application An application in which its components reside on many systems.

Distributed database A database that is logically or physically distributed among several systems.

Elevation of privileges An attack where an attacker is able to perform some manipulation in order to raise his privileges, enabling him to perform unauthorized functions.

Encapsulation A design attribute that permits the hiding of internal details about an object in an OO system.

Expert system A software system that accumulates knowledge on a particular subject and is able to predict outcomes based upon historical knowledge.

Firewall A hardware device or software program that controls the passage of traffic at a network boundary according to a predefined set of rules.

Hardening The process of configuring a system to make it more robust and resistant to attack.

Heap overflow An attack that attempts to corrupt a program's heap (the dynamically allocated memory space created by a program for storage of variables).

Hierarchical database A database model that is built on a tree structure.

Hosts file A file on a workstation or server that associates host names and IP addresses.

Inheritance The characteristics of a subclass that inherits attributes from its parent class.

Injection attack An attack on a system where some scripting or procedural language is inserted into a data stream with the intention that the scripting will be performed.

Input attack Any attack on a system where specially coded data is provided in an input field with the intention of causing a malfunction or failure of the system.

Jump-to-register A type of buffer overflow attack where a function's return pointer is overwritten, in order to alter the behavior of a program.

Key logger A hardware or software component that records keystrokes on a computer.

Knowledge-based system A system that is used to make predictions or decisions based upon input data.

Logic bomb Computer code placed in a system that is intended to perform some harmful event when certain conditions are met—usually a specific day or time in the future.

Method A function or calculation that an object is capable of performing.

Mobile code Computer code that is downloaded or transferred from one system for execution on another system.

Network database A database model based upon the hierarchical model, but with the ability for records to be related to other records in the database.

Neural network A software system that simulates the human reasoning process and is able to make predictions and decisions based on prior results.

NOP sled A type of stack overflow attack where the attacker floods the stack with NOP (no-operation) instructions in an attempt to take control of the program.

Object An instance of an OO *class*.

Object orientation (OO) A methodology for organizing information and software programs that supports objects, methods, and object reuse.

Object oriented database (OODB) A database that is organized and stored as objects.

Object oriented programming (OOP) A programming language methodology that consists of code contained in reusable objects.

Object reuse An attack on a system where one user or program is able to read residual information belonging to some other process, as a means for exploiting the other process through a weakness that can be discovered in the residual data.

Open Database Connectivity (ODBC) A TCP/IP-based client-server communications protocol used to facilitate database transactions over a network.

Patch management The process of managing the installation of patches on target systems.

Polymorphism The ability for an object to respond to a call differently, depending upon the object's type.

Pretexting An act of deception intended to persuade a targeted individual into providing information under false pretenses.

Relational database A database model based upon tables of data and the relationships between them.

Role-based access control (RBAC) An access control method where access permissions are granted to roles, and users are assigned to those roles.

Rootkit Malicious code that is designed to avoid detection by hiding itself by some means.

Side channel attack An attack on a system where a subject can observe the physical characteristics of a system in order to make inferences on its internal operation.

Software development life cycle (SDLC) The overall process used to design, create, and maintain software over its lifetime.

Spam Unwanted e-mail that usually contains unsolicited commercial advertisements, pornography, or attempts to lure recipients into opening malicious attachments or visiting malicious web sites.

Spyware Usually unwanted and sometimes malicious software that is used to harvest Internet usage information from a user's workstation.

SQLNet A TCP/IP-based client-server communications protocol used to facilitate database transactions over a network.

Structured language A hierarchical computer language methodology that consists of main programs and called subroutines or functions.

Threat risk modeling A process where threats in an environment are identified and ranked, and mitigating controls introduced to counter the identified threats. Also known as *threat modeling*.

Three-tier application An application that consists of three logically separate layers, usually a user interface front end, business logic middle tier, and database management third tier.

Time bomb See *logic bomb*.

Transaction An event where data is updated within a database.

Trojan horse Malicious computer code that claims to perform some benign function while actually performing some additional, malicious function.

Two-tier application An application that consists of two logically separate layers, usually a user interface and business logic front end and a data management back end.

View A virtual table in a relational database.

Virus Malicious code that attaches to a file, document, or master boot record (MBR).

Web application An application that utilizes a Web browser as the client software.

Worm Malicious code that has the ability to self-propagate and spread rapidly from system to system.

Review Questions

1. A media player that is running within a web browser is known as a(n):
   a. Agent
   b. Mashup

c. Applet

d. Script

2. The chief advantage of web-based applications is:

a. Client-side software updates are unnecessary

b. Built-in SSL encryption

c. Ease of use

d. Better security

3. Enterprise Java Bean, Distributed Common Object Model, and Java Remote Method Invocation are examples of:

a. Object request brokers

b. Object oriented frameworks

c. Object oriented languages

d. Distributed systems

4. An attacker is experimenting with an application by inserting long strings of machine language code in the application's input fields. The attacker is attempting:

a. A Denial of Service attack

b. A buffer overflow attack

c. A stack smashing attack

d. Any of the above

5. A risk manager requires that his organization implement a control to prevent application attacks. The best solution is to use:

a. Multitier architecture

b. Code reviews

c. An application vulnerability scanner

d. An application firewall

6. An astute security engineer has discovered that two accomplices are communicating with each other via hidden messages within images on a blogsite. The security engineer has discovered:

a. Emanations

b. A side channel attack

c. A covert channel

d. Steganography

7. Rootkits can be difficult to discover because:
   a. They subvert the operating system
   b. They install themselves in master boot records (MBRs)
   c. They install themselves in flash memory
   d. They use hidden processes
8. The purpose of a bot army is:
   a. To launch Denial of Service attacks
   b. To relay spam, host phishing sites, or launch Denial of Service attacks
   c. To remotely control zombie computers
   d. To build a massively parallel system
9. An IT manager is considering an anti-spam solution. Because one of the primary concerns is e-mail server performance, which solution can be eliminated from consideration?
   a. Appliance
   b. Outsourced
   c. Server-based
   d. Client-based
10. Web beacons are an effective site usage tracker because:
    a. They use hidden form variables
    b. Browsers cannot detect them
    c. Browsers do not block them
    d. They are encrypted
11. The most effective countermeasure for malware is:
    a. Rootkit detection
    b. Decreasing user privilege levels
    c. Anti-virus
    d. Firewalls
12. The primary purpose for decreasing user privilege levels is:
    a. To reduce support costs
    b. To limit the effects of malware
    c. To improve system performance
    d. All of the above

13. Which of the following is NOT normally used in system hardening:
    a. Changing TCP/IP parameters
    b. Removing unnecessary services
    c. Removing unnecessary NICs
    d. Renaming administrator userids
14. The purpose of input field filtering is:
    a. To prevent input injection attacks
    b. To detect application scanning
    c. To prevent SQL injection attacks
    d. To detect unsafe code
15. The best time to develop application test plans is:
    a. During requirements and specifications development
    b. During application design
    c. During application testing
    d. During application coding

Hands-On Projects

Project 3-1: Vulnerability Scanning

In this project, you will perform vulnerability scanning. Various tools are available to scan a Windows computer to determine which patches are missing. Microsoft has published the interface that is used to determine which patches are installed on a system, and also which patches are available. The Secunia Personal Software Inspector (PSI) tool is used to scan a system and identify which patches are missing.

1. Download PSI from Secunia at https://psi.secunia.com/.
2. Install PSI on your system and start the tool. It may appear only as a Systray icon, in which case you need to double-click the Systray icon to pull up the user interface.
3. Click the **Scan** tab.
4. On the Scan window, click **Start Scan**. PSI will begin scanning the system for patches. See figure 3-8.
5. Which Microsoft patches have been identified that need to be installed?
6. What other vulnerabilities has the tool identified?

Figure 3-8 Secunia Personal Software Inspector tool scanning for vulnerabilities

Source: Course Technology/Cengage Learning

Project 3-2: Threat Risk Modeling

In this project you will download and work with Microsoft's Threat Analysis & Modeling tool. Threat risk modeling is used to identify threats to an application's design before it is built. You may wish to use your knowledge about an existing application to enter information.

1. Download the Microsoft Threat Analysis & Modeling tool from this site: http://msdn.microsoft.com. Search on *Microsoft Threat Analysis & Modeling* to find the download link.
2. Install and start the tool.
3. Select New Threat Model From Wizard. The wizard will appear as shown in Figure 3-9.
4. Click **Next**. You'll be asked to enter role names. Enter only one or two roles (or else you will be spending a great deal of time in this tool). Click Next.
5. In Step 2, enter data set names. Again, limit your entry to one or two entries. Click **Next**.

Figure 3-9 Microsoft's Threat Analysis & Modeling tool

Source: Course Technology/Cengage Learning

6. In Step 3 you will be asked to fill in an Access Control Matrix. For each item in Data, you will need to specify which Role has access and which conditions are permitted by each role. After you have completed the access matrix, click **Next**.
7. In step 4, the tool will show which use cases exist in the application. If this appears correct, click **Next**, else click **Back** to make any necessary changes.
8. In step 5, list which application components exist in the application. For example, you might have a simple Front End and a Database. Enter your components and click **Next**.
9. In step 6, you select the technologies used by each component you listed in Step 5. Select the component, then click the **+**button and select which items are present in the component. When you have selected the appropriate items for each component, click **Next**.
10. In step 7, you will instruct the calls that are used in each use case (in this step you are probably wishing you had limited the number of users and data stores). For each Use Case, select which Caller performs which

actions on components, and what data is sent and received. When you have completed listing the calls for each Use Case, click **Next**.

11. In Step 8, the tool will list the threats that exist that could affect the application. Click **Next**, then **Finish**, and then name your threat model.
12. Leave the tool running for the next project.

Project 3-3: Threat Modeling with External Dependencies

In this project you will continue threat modeling by including external dependencies. Threat modeling needs to take into account external dependencies that may mitigate or aggravate threats. Applications do not existing in a vacuum, and their models should accurately depict the real world in which they operate.

This project utilizes the threat model developed in Project 3-3.

1. Start the Microsoft Threat Analysis & Modeling Tool. Open the model created in Project 3-3.
2. Click **Threat Model > New > External Dependency**. In the **Name** field, type *Authentication*. In the **Dependency Type**, select *Web Service*.
3. View various reports with the tool. You will notice that there are no new threats added as a result of your having added the external dependency. How can you accommodate this into the model?

Case Projects

Case Project 3-1: Web Application Vulnerability Scanning

1. Download a demo copy of Watchfire AppScan from this web site:

https://www.watchfire.com/securearea/appscan.aspx

2. Identify a web site that you have permission to scan. Scan the site with AppScan. What vulnerabilities were identified? Were there any false positive findings?

Case Project 3-2: Develop an Application Security Test Plan

As a consultant with the Security Consulting Company, you have been hired to develop a plan for ABC Plastics to protect their online applications.

You have been asked to examine and make recommendations in ABC Plastics' software development process. What changes will you make?

You have also been asked to make recommendations for tools that can be used to measure application security. Which tool(s) will you recommend and why?

Case Project 3-3: Observe Script Injection in Action

How many web sites adequately filter out script injection? Take the sample code below and insert it into form fields on various web sites and see what happens.

```
<script>alert("hello")</script>
```

When a web application does not filter scripting language, is there a security risk? Why or why not?

Case Project 3-4: Pharming Attack Countermeasures

As a consultant with the Security Consulting Company, you have been hired to perform an assessment on the risk of a pharming attack.

Congo River Adventures purchases its supplies through several online merchants. Congo River Adventures' web site advertises which merchants they use, as a way of showing that their services are superior to their competitors. However, Congo River Adventures is now concerned that a hacker could launch a pharming attack against them and divert its employees to imposter supplier web sites. What approach will you take in order to understand and mitigate any risk?

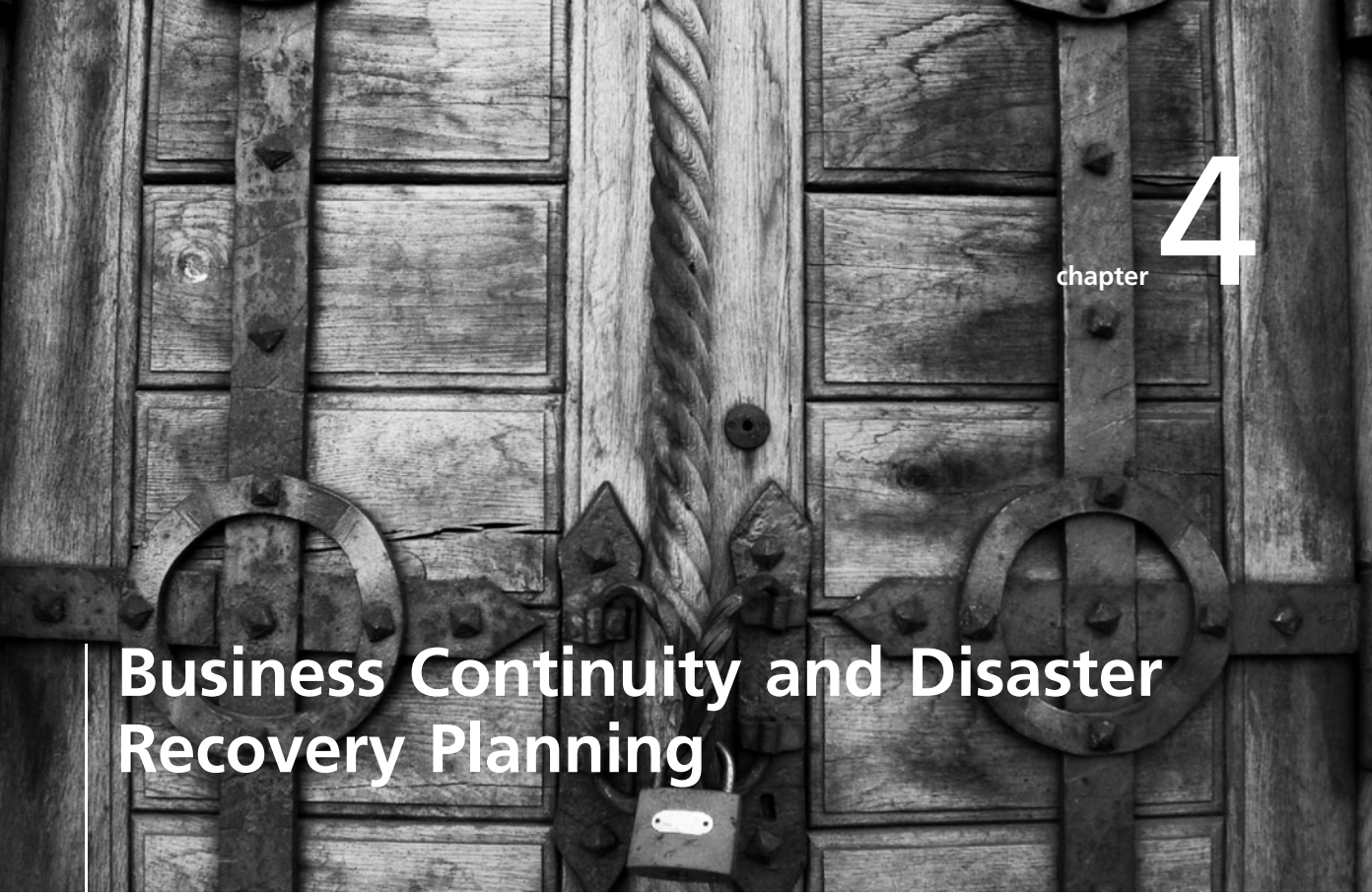
Case Project 3-5: Web Application Security Architecture

As a consultant with the Security Consulting Company, you have been hired to develop a secure application architecture for ABC Plastics' online Web application.

Some of the questions that officials at ABC Plastics are asking include:

- Should the database server and the web server be on the same system?
- How many firewalls should protect the application?
- What forms of access controls should be used to protect the application and its database?

This page intentionally left blank



chapter 4

Business Continuity and Disaster Recovery Planning

Topics in this Chapter:

- Running a Business Continuity and Disaster Recovery Planning Project
- Developing Business Continuity and Disaster Recovery Plans
- Testing Business Continuity and Disaster Recovery Plans
- Training Users
- Maintaining Business Continuity and Disaster Recovery Plans

The (ISC)^2 *Common Body of Knowledge* (CBK) defines the key areas of knowledge for Business Continuity and Disaster Recovery Planning in this way:

The Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) domain addresses the preservation of the business in the face of major disruptions to normal business operations. BCP and DRP involve the preparation, testing and updating of specific actions to protect critical business processes from the effect of major system and network failures.

Key areas of knowledge include:

- *Develop and document project scope and plan*
- *Conduct Business Impact Analysis*
- *Develop recovery strategy*
- *Incorporate the following elements into the plan:*
  1. *Emergency response*
  2. *Notification (e.g., calling tree)*
  3. *Personnel safety*
  4. *Communications*
  5. *Public utilities*
  6. *Logistics and supplies*
  7. *Fire and water protection*
  8. *Business resumption planning*
  9. *Damage assessment*
  10. *Restoration (e.g. cleaning, data recovery, relocation to primary site)*
- *Training*
- *Plan maintenance*

Business Continuity and Disaster Recovery Planning Basics

A **disaster** is a natural or man-caused event that damages property and assets, injures or kills people, and impairs the ability for organizations to continue operating. **Business continuity planning** is the set of activities required to ensure the continuation of critical business processes when a disaster occurs. **Disaster recovery planning** is the set of activities concerned with the assessment, salvage, repair, and restoration of damaged facilities and assets that support critical business processes.

What Is a Disaster?

A **disaster** is any natural or man-made event that disrupts the operations of a business in such a significant way that a considerable and coordinated effort is required to achieve a recovery.

Two main categories of disasters can strike an organization: natural disasters and man-made disasters.

Natural Disasters **Natural disasters** comprise a wide range of natural events that cause damage over often wide areas. These natural events can be more-severe versions of ordinary events, or less common events. The types of natural disasters are:

- **Geological**. These events include earthquakes, volcanoes, lahars, tsunamis, landslides, and sinkholes.
- **Meteorological**. Events in this category include hurricanes, tornados, wind storms, hail, ice storms, snow storms, rainstorms, and lightning.
- **Other**. These include avalanches, fires, floods, meteors and meteorites, and solar storms.
- **Health**. This category includes widespread illnesses, quarantines, and pandemics.

The events described above vary widely in predictability. Many types of storms can be predicted hours or days in advance, giving people a few hours warning for evacuation or last-minute preparation. On the other hand, earthquakes are only statistically predictable, meaning that geographic areas are generally classified as being low, medium, or high risk for earthquakes.

Some natural events cause damage over a wide geographic area, while others are very limited. Hurricanes and earthquakes can damage buildings and roads over hundreds of square miles, while tornadoes and hail can affect just a few square miles—or less.

Man-Made Disasters **Man-made disasters** are caused—or exacerbated—by the action (or inaction) of people or organizations. The types of man caused disasters are:

- **Labor**. The types of events here include strikes, walkouts, and slowdowns that disrupt services and supplies.
- **Social-political**. These include war, terrorism, sabotage, vandalism, civil unrest, protests, demonstrations, cyber attacks, and blockades.
- **Materials**. These include fires and hazardous materials spills.
- **Utilities**. These events include power failures, communications outages, water supply shortages, fuel shortages, and radioactive fallout from power plant accidents.

How Disasters Affect Businesses Disasters can affect businesses in a number of different ways, and this depends both on the nature of the disaster as well as the nature of the business. There are several ways in which a disaster impacts a business.

Direct Damage Some disasters will directly affect business facilities and equipment, making them temporarily unusable or unreachable. For example, a severe wind storm or tornado can damage a part of a building that can be repaired, and/or render business equipment unusable until building repairs have been completed.

Disasters can also permanently damage buildings and equipment, to the extent that they cannot be repaired but instead must be replaced.

Transportation Disasters are well known for disrupting transportation systems. Earthquakes, floods, landslides, and other events can damage freeways, bridges, and roads. This sort of damage can have several effects on businesses including:

- **Supply disruption**. When transportation infrastructure is damaged, shipments of supplies are delayed, which could have a dampening effect on a business' ability to

produce goods and services. If a business produces goods that are shipped to customers, then this too will affect businesses.

- **Customer disruption**. Damaged transportation will prevent customers from being able to reach businesses. Even if businesses themselves are not damaged, a disaster can have devastating consequences on businesses that depend upon visits by retail or wholesale customers.
- **Employee disruption**. Damaged transportation systems can prevent employees from being able to report for work. Again, even if the business is not directly affected by the disaster, if employees are unable to reach the business then the business' ability to deliver goods or services will be affected.

Figure 4-1 shows a roadway made impassable by an earthquake.

Communications Disasters also commonly affect communications infrastructure. Earthquakes, floods, landslides and other events can damage communications cables, towers, switching centers, and other facilities. Disasters can directly damage communications cables, antennas, switch centers, and other communications facilities, and damage to transportation facilities (described in the preceding section) can keep communications workers away from their jobs, which will have a dampening effect on communications as well.

Figure 4-1 Roadway and buildings damaged in an earthquake

Courtesy US Geological Survey. Department of the Interior/USGS

Utilities Disasters frequently affect utilities. Storms and other natural events are especially hard on electric utilities, since most electric systems are built above-ground and are exposed to the weather. Water and natural gas systems are also negatively affected by disasters, although by a smaller margin since most of those facilities are underground.

How BCP and DRP Support Data Security

Recall that the pillars of security are confidentiality, integrity, and availability. Business continuity and disaster recovery planning are concerned with the *availability* of information, particularly when threatened with events that threaten to make data unavailable for long periods of time.

Business continuity and disaster recovery plans do need to take *integrity* and *confidentiality* into account. Even in a disaster situation, disaster procedures need to ensure that data confidentiality and integrity are preserved.

BCP and DRP Differences and Similarities

BCP and DRP have traditionally been treated as separate, although similar, activities that are both concerned with the survival of an organization in a disaster scenario.

BCP has been concerned with the activities required to ensure the continuation of critical business processes in an organization. This may involve the use of alternate personnel, equipment, and facilities—whatever it takes to keep critical processes operating.

DRP has been concerned with the assessment, salvage, repair, and eventual restoration of damaged facilities and systems.

A good analogy to illustrate the differences and similarities is the breakdown of a delivery truck. BCP can be thought of as the rental truck that is used to continue deliveries, while DRP is the repair of the original delivery truck.

Another common distinction used to compare BCP and DRP efforts is this: DRP is often considered an effort to recover IT system and applications, whereas BCP is regarded as the effort to recover business processes that may or may not be directly dependent on IT systems.

Other terms are used in these contexts, including:

- **IT Service continuity**—the ITIL term that ensures the continuity of IT-provided services and systems.
- **Business Continuity and Disaster Recovery Planning (BCDR)**—the combined thought of the once-separate BCP and DRP.

Industry Standards

Several standards and regulations on disaster recovery and business continuity planning have been established, including those listed here.

- **ISO 27001—Requirements for Information Security Management Systems**. This new international standard on information security management systems addresses business continuity management is presented in section A.14.
- **ISO 27002—Code of Practice for Business Continuity Management**. This emerging international standard establishes the principles, terminology, and processes supporting business continuity management.

- **ISO27002—Code of Practice for Information Security Management**. This well known international standard on information technology security practices, presented in section 14, addresses business continuity management.
- **NIST 800-34—Contingency Planning Guide for Information Technology Systems**. The U.S. National Institute for Standards and Technology published this seven-step process for BCP and DRP projects.
- **NFPA 1600**. This is the Standard on Disaster/Emergency Management and Business Continuity Programs that was developed by the U.S. National Fire Protection Association.
- **NFPA 1620**. The Recommended Practice for Pre-Incident Planning, a standard that guides organizations in their development of disaster recovery plans.
- **HIPAA**. The U.S. Health Insurance Portability and Accountability Act includes the "Security Rule" that requires several measures be taken to protect patient health information in electronic form. HIPAA requires that organizations that manage electronic health information have a documented and regularly tested disaster recovery plan.

Benefits of BCP and DRP Planning

Besides the increased likelihood of surviving a disaster, there are several other benefits that an organization will enjoy through having undertaken a business continuity and disaster recovery planning project.

- **Reduced risk**. After having undergone risk and threat analysis and mitigation, risks that may jeopardize the organization's ongoing operations will be reduced.
- **Process improvements**. Business processes are going to receive very close scrutiny throughout the project. Project staffers will recognize opportunities for process improvements in both the BIA phase as well as when contingency plans are developed.
- **Improved organizational maturity**. There is nothing like a BCP/DRP project, with its intense scrutiny on processes, to get an organization to improve its process maturity.
- **Improved availability and reliability**. One of the objectives of business continuity and disaster recovery is the improved resilience of processes and systems. This will result in improved availability and reliability of business processes and the IT systems that support them.
- **Marketplace advantage**. An organization that has been able to reduce risks, improve processes, and enhance availability and reliability is going to have a stronger market position.

The Role of Prevention

The surprising and unexpected consequences of a disaster can have a devastating effect on an organization.

The point of BCP and DRP is not prevention of the disaster itself, but prevention of what is otherwise unpreparedness on the part of the organization. The purpose of BCP and DRP is the development of the processes, procedures, and standby assets to be placed into action when a disaster strikes.

The steps in a BCP/DRP project will identify the criticality of specific business processes and systems, which leads to investments in standby or backup capabilities that are used

when a disaster strikes. The steps in running a BCP/DRP project are discussed in the next section.

Running a BCP/DRP Project

The development of business continuity and disaster recovery plans is a significant undertaking that can consume dozens of manhours in the smallest businesses to thousands of manhours in large organizations. Any activity of this magnitude requires formal planning, budget, and support.

A business continuity and disaster recovery planning project has several distinct activities and phases. A common methodology has emerged that most organizations follow; this methodology is described in this chapter.

Pre-project Activities

Prior to the actual start of the project, several key actions should be completed including:

- Obtaining executive support
- Formally defining the scope of the project
- Choosing project team members
- Developing a project plan
- Developing a project charter

These steps are described in more detail in the remainder of this section.

Obtaining Executive Support The completion of a business continuity and disaster recovery planning project takes a significant amount of resources, particularly man-hours and expenses. Diverting resources from everyday processes and responsibilities will have a negative impact on key business activities, enough that managers will be tempted to pull staff off of the project, delaying its completion.

For this reason it is imperative that executive support be obtained before the BCP/DRP project is started. The executive support should be exceedingly clear and unambiguous regarding:

- The scope of the project
- The priority of the project
- The budget for the project
- The appropriate staffing levels for the project
- The expected completion date for the project
- Any rewards that will be given upon the completion of the project
- The year-to-year support for the maintenance of the plan

Defining the Scope of the Project The scope of the BCP/DRP project is one of the most important decisions that will be made. It defines what part(s) of the organization are included in the project, and what parts are excluded from the project.

The decision about the scope of the project needs to be an informed decision. The scope of the project needs to be wide enough to include all of the known-critical parts of the organization (without which the organization would struggle mightily to survive, should a disaster occur).

The scope of the project should not include parts of the organization that are outside the control of the executive sponsors. The reason for this is two-fold: first, those outside parts of the organization may feel suspicious about the BCP/DRP project, in that it might be an attempt to gain control over that part of the organization; second, the executive(s) who sponsor and support the project cannot commit resources to the project that are outside of their span of control. In other words, one part of an organization cannot impose a BC/DR plan upon another part of the organization without their consent, participation, and executive support.

Another factor that needs to be considered is the size of the BCP/DRP project. In a very large organization with multiple locations and/or business units, managing such a large project may be too cumbersome. Perhaps it would be better to scale down a project to include just certain locations and/or business units. Separate BCP/DRP projects in other locations or business units can be carried out by separate project teams at the same time, or at a later time. As the saying goes, "You don't want to bite off more than you can chew."

Choosing Project Team Members At first blush, it may seem an easy task to choose the staff members who will contribute to the BCP/DRP project. However, every choice has a consequence, and yet consequences will be unavoidable in almost every case.

One motivator for choosing project team members is the quality and success of the project. This will create a tendency to select the most senior staff members from various groups—those who know the most about how different departments are operated. In many cases these will be the best choice for staffing the BCP/DRP project team, but not in all cases. Remember that the project will require five, or ten, or twenty, or forty, hours per week from each team member. Choosing the best and the brightest from each group will put existing operational teams at a decided disadvantage by taking away their best members.

Swinging the pendulum to the opposite side is also an option: selecting junior people from each team or department will not have the same negative impact on those teams. However, the BCP/DRP project may suffer if its team members have little familiarity with how their respective departments really function.

Clearly, some middle ground is called for. The nature of that middle ground will vary from company to company. It may be who is selected for the team, or how many hours per week each team member will be able to contribute to the project. A balance is needed between getting good talent for the project team versus maintaining enough support for day-to-day operations. The urgency for getting BCP and DRP plans in place plays a part as well.

Developing a Project Plan Every journey begins with a plan. An organization's BCP/DRP project should have a detailed plan that identifies the milestones and the work: when will the milestones take place, and who will do the work to accomplish them.

Except in the smallest organizations, the project should have an experienced project manager who knows how to develop project plans, conduct project meetings, communicate clearly, manage the people who are performing the tasks on the plan, make schedule changes, and make necessary changes to the plan that will arise throughout the project.

Ideally, the project manager will have been involved in a BCP or DRP project in the past so that she is familiar with these types of projects and the common issues that arise in these projects.

In a large BCP/DRP project, it is best to develop the plan in stages. Until the **Business Impact Analysis** is completed, for example, it will be difficult to estimate the amount of work required to develop contingency plans. This is because no one on the project team will know for certain which contingency plans will need to be developed, or what resources will be required to develop them. It is suggested that a large BCP/DRP project be split into three phases:

- Phase I: Business Impact Analysis
- Phase II: Develop Contingency Plans
- Phase III. Test Contingency Plans

One of the last milestones for Phase I should be the development of a detailed project plan for Phase II. Similarly, one of the last milestones for Phase II should be the development of a detailed project plan for Phase III.

Developing a Project Charter All of the main items of preparation that take place prior to the actual start of the project should be documented in a project charter document. The charter document should contain all of the items being discussed in this section, and a few more:

- Purpose of the BCP/DRP project
- Executive sponsorship
- Scope
- Budget
- Principle team members
- Milestones

The charter document should be drafted, reviewed, and signed by the executive sponsors and principle team members. Doing so will accomplish two things: the project will be well defined, and all of the key participants in the project will be committing to its success.

Performing a Business Impact Analysis

A **Business Impact Analysis** (**BIA**) is essentially a catalog of all of an organization's important business processes that includes information about the criticality of each. The steps required to perform the BIA are:

- Survey business processes
- Perform risk analysis and threat assessment
- Determine maximum tolerable downtime (MTD)
- Establish key recovery targets

These steps are described in the remainder of this section.

Survey In-Scope Business Processes The first and very necessary step in a BIA is a survey of all of the important business processes that are within the scope of the overall project. The survey itself need not be complicated, but it may be very labor intensive and time consuming in a larger organization with many important business processes.

The objective of the survey is the capture of several characteristics of each important business process. These characteristics will enable team members to complete subsequent steps of the BIA.

The project team will need to decide what constitutes "important" in determining which processes are important enough to be considered in the BIA, and which are not sufficiently important.

Information Collection It is important for the collection of business process information to be as uniform as possible. I suggest that the project team develop an "intake form" that can be used to capture process information. When multiple staff members are performing process surveys, an intake form helps the survey process to be more consistent than if each staff member used their own "style" to get the same information. A sample intake form is shown in Table 4-1.

Process Name	(name of the process)
Date	(date of the interview)
Interviewer	(name of the person conducting the interview)
Interviewee	(name of the person being interviewed)
Interviewee Contact	(e-mail, phone, location, etc.)
Department	(Interviewee's department)
Process Owner Name	(department manager or other responsible party who is accountable for the performance of the process)
Process Purpose	(why the process is performed)
Process Inputs	(data, people, supplies, or other things that the process uses)
Process Outputs	(data, products, or other outcomes from running the process)
Supplier Dependencies	(names of suppliers that are essential to the ongoing operation of the process)
Personnel Dependencies	(names of staff members who are essential to the ongoing operation of the process)
Asset Dependencies	(list of assets that are essential to the ongoing operation of the process)
Information System Dependencies	(list of IT applications that are essential to the ongoing operation of the process)
Communications Dependencies	(list of communications facilities (phone, FAX, Internet, etc.) that are essential to the ongoing operation of the process)
Facilities Dependencies	(list of facilities that are essential to the ongoing operation of the process)
Other Internal Dependencies	(other internal dependencies not listed above that are essential to the ongoing operation of the process)
Other External Dependencies	(other external dependencies not listed above that are essential to the ongoing operation of the process)

Table 4-1 **Sample BIA process intake form**

Staff members who are conducting interviews can bring along a notebook computer and type in the information given to them, or they can hand-write information on pads of paper and type it in later.

Each process needs to have its own form. In a department with many processes, a single interview can result in many completed forms.

Information Consolidation As information is collected on each process, the information should be electronically transferred from individual intake forms onto a spreadsheet.

It is suggested that the spreadsheet be set up as follows:

- Columns in the spreadsheet will correspond to fields in the intake form.
- Rows in the spreadsheet will correspond to individual intake forms.

The purpose of putting all of the information into a spreadsheet is that it gives analysts an opportunity to view all of the processes in a single view.

As the BIA work advances, the project manager (or other individual) should keep the process spreadsheet up-to-date. It will be used in later stages of the BIA.

Threat and Risk Analysis

Once all processes have been identified, and basic information about each process captured on the input forms described in the previous section, a threat risk analysis needs to be performed on each process.

Depending upon the skills of the project team members and the needs of the project, the threat-risk analysis can be performed as a single task or broken up into a **risk analysis** and a **threat analysis**. The remainder of this section will assume that the two will be done separately.

The purpose for threat and risk analyses is to identify threats and risks that can jeopardize critical business processes—not just from a disaster recovery perspective, but from *any* perspective. The ultimate objective of business continuity planning and disaster recovery planning is not just recovering from disasters, but also preventing and avoiding disaster-related and other events from threatening the continuity of critical business processes.

Threat Analysis A **threat analysis**, sometimes known as threat modeling, is the process of identifying factors that may jeopardize the ongoing performance of a business process or system.

A single threat analysis can be performed for the entire business (or, at least the portion of the organization that is in-scope for the BCP/DRP project), or individual threat analyses can be performed on each process. Either way, the procedure for performing a threat analysis is pretty much the same:

1. Identify every threat that can reasonably materialize and adversely affect the process.
2. Identify the probability that the threat can actually occur.
3. Identify mitigating actions that can be taken to reduce the identified threats.

Risk Analysis A **risk analysis** is the process of identifying risks and weaknesses in a process or system.

A risk analysis can be performed on each process, group of processes, or the entire organization, depending upon the nature of the business and the needs of the BCP/DRP project. The procedure for performing a risk analysis is:

1. Identify every risk that has a reasonable chance of materializing and adversely affecting a process.
2. Estimate the probability that the risk can materialize into an event that can adversely affect a process.
3. Identify mitigating actions that can be taken to reduce significant risks.

An organization that periodically conducts risk and threat analyses may be able to appropriate most or all of an existing general-purpose risk and threat analysis, instead of performing one separately for a BCP/DRP project. There is nothing inherently unique about a risk assessment in support of a BCP/DRP project that would require a separate one be performed. Risk and threat analysis are covered in more detail in Chapter 1, "Information Security and Risk Management."

Determine Maximum Tolerable Downtime (MTD) Once every business process has been identified and placed on the big spreadsheet, an important metric must be assigned to it: **maximum tolerable downtime** (**MTD**). This is defined as the period of time after which the organization would suffer considerable pain were the process unavailable for that period of time.

The units of measurement for MTD may be minutes, hours, days, or longer, depending upon the nature of the business.

Determining MTD is a process all by itself that will probably undergo several revisions. It is suggested that the project team take a first-pass at educated-guess MTD values for each process, and then have the sponsoring executives review, update, and approve the MTD figures established for each process.

While the project team may establish some other means for documenting the MTD for each process, it is suggested that a column be added to the process worksheet and the MTD value for each process placed there.

Even then, it's likely that at least some MTD values will be changed again, later on in the project. Still, it is important to have a good set of educated-guess figures before moving on to the next phase of the project.

Develop Statements of Impact For each process, a **statement of impact** needs to be developed that describes the impact on the organization if a process is incapacitated. Examples might include: *inability to process payments*, *inability to produce invoices*, or *inability to support customers*. This information will be needed later in the project.

Recording Other Key Metrics The project team or the sponsoring executives may wish to record other metrics for each process in scope. Some possible metrics that could be used include:

- Cost to operate the process
- Cost of process downtime
- Profit derived from the process

These metrics may be helpful later on in the project in a phase known as the **Criticality Analysis**.

Ascertain Current Continuity and Recovery Capabilities Many organizations aren't starting with a completely clean slate: there are some BCP or DRP capabilities or plans in place already. These capabilities need to be taken into account. For each process there will be three outcomes:

- **Adequate**. The current BCP/DRP capability exists and is still adequate.
- **Inadequate**. The current BCP/DRP capability exists but no longer meets the needs of the business. Current capabilities are either defective (implemented incorrectly) or provide recovery at a lesser level of capability.
- **Non-existent**. No BCP/DRP capability exists.

Developing Key Recovery Targets

When Maximum Tolerable Downtime (MTD) and other figures have been established, the next step in the process is to determine two key recovery targets. These targets will directly determine any improvements that must take place in processes and supporting IT systems, so that the targets are achievable. The two targets are:

- Recovery Point Objective (RPO)
- Recovery Time Objective (RTO)

Recovery Time Objective (RTO) **Recovery Time Objective (RTO)**, is the maximum period of time that a business process or IT system will be unavailable during a disaster. RTO is expressed in units of time and can be minutes, hours, days, or longer, depending upon the needs of the organization.

The project team needs to establish an RTO for every process that is in scope for the project. The Maximum Tolerable Downtime (MTD) target should be a guide to the RTO value.

When setting RTO targets for processes, project teams need to realize that low values for RTOs are more expensive to achieve than higher values. This is true whether the target is being express for a manual business process or an IT system. While every IT application, system, and organization is different, Table 4-2 gives an approximation of the types of technologies and capabilities that are needed for different ranges of RTO.

In addition to additional equipment and potentially expensive software for clustering and replication, shorter RTOs also require more staff and facilities to support the more aggressive targets.

Project team members and executives need to quantify and compare the value of a business process to the potential cost of upgrading a system to meet a more aggressive RTO. Often, DRP/BCP project teams scale back their RTOs once they discover how expensive their targets really are. One acceptable approach is a multi-year investment in the necessary software and equipment to reach RTO targets.

Recovery Point Objective (RPO) The **Recovery Point Objective (RPO)**, expressed in units of time, is the maximum acceptable amount of data loss or work loss for a given process. One pragmatic way of understanding RPO is to ask, how much re-keying will be

RTO	Technology required
8–14 days	New equipment, data recovery from backup
4–7 days	Cold systems, data recovery from backup
2–3 days	Warm systems, data recovery from backup
12–24 hours	Warm systems, recovery from high speed backup media
6–12 hours	Hot systems, data recovery from high speed backup media
3–6 hours	Hot systems, data replication
1–3 hours	Clustering, data replication
<1 hour	Clustering, near real time data replication

Table 4-2 Capabilities required to support various RTOs

required once a system or application has been recovered and is back up and running? Here is an example:

The database management system supporting an IT application exports data to a flat file every two hours. The RTO for the application is 24 hours, which means that within 24 hours of a disaster, the application will be available again. When the application is recovered, the IT department will recover data from backups and from the flat file exports. The RPO for the application is two hours, because the maximum data loss in this example is two hours.

Criticality Analysis When the MTD, RPO, and RTO targets have been established for each process, all of the processes can be compared to each other based upon these criteria. The point of the criticality analysis is to identify which processes in the organization are the most critical, based upon the objective measures that have been identified thus far in the Business Impact Analysis. Here are several ways in which processes can be compared:

- **Ranked by MTD**. Those processes with the lowest MTD values may be the most time-sensitive in the organization.
- **Ranked by RTO**. Processes with low RTO values are probably also time-sensitive.
- **Ranked by RPO**. Processes with low RPO values are probably time-sensitive and also high-value or labor intensive.
- **Ranked by revenue per hour/day/month**. Processes with high revenue rates are probably among the most valuable in the organization.
- **Ranked by cost per hour/day/month**. Processes with a high cost may be the most valuable in the organization.
- **Ranked by customer visibility**. A company that relies on its customer service image may consider customer-facing services and systems at a higher criticality than others.

Establishing Ranking Criteria The project team, together with sponsoring executives, will need to establish process ranking criteria that are appropriate for the organization. Knowing which processes and systems are the most critical may be a simple case of ranking

them by one of the already-identified figures such as MTD or RTO, or it may be a little more complicated. In the end, the ranking criteria need to meet the needs of the business, and not the other way around.

Complete the Criticality Analysis Once the ranking criteria are chosen, it is applied against the entire list of processes in the Business Impact Assessment. The result will be the final rank-ordered list of processes and systems in the organization. At the top of the list will be those processes and systems that are most vital to the organization's ongoing viability.

Improving System and Process Resilience

The results of the Business Impact Analysis (BIA) provide the team with the most critical processes and systems in the organization, and how quickly each needs to be recovered.

From a strict security perspective, the rank-ordered result of the BIA also provides security personnel with a valuable list of which processes and systems require the most protection.

Identifying Risk Factors The section "Threat and Risk Analysis" earlier in this chapter describes the important steps of identifying threats and risks associated with business processes. Now it is time to examine the results of those analyses, particularly for the most critical processes and systems in the organization.

The threat and risk analysis suggests one or more mitigating controls that will reduce either the probability, frequency, or impact of a threat or risk. Further analysis is needed to determine whether the mitigating controls are *feasible*. These mitigating controls need to be analyzed to determine:

- Whether the mitigating control will reduce risk at a reasonable cost (*it's not reasonable to spend $100,000 to protect a $10,000 asset*)
- Whether the mitigating control can be reasonably implemented and operated in a production system or process environment
- Whether mitigating controls from several systems can be consolidated into a simpler control that protects against multiple threats/risks or can protect multiple systems or processes
- Whether the mitigating control represents a best practice or a common practice

Developing Business Continuity and Disaster Recovery Plans

After the BIA, criticality analysis, and recovery targets have been established and approved by executive management, response and recovery plans can be developed and tested. This section discusses the steps required in these plans, which for most organizations include:

- Selecting recovery team members
- Emergency response
- Damage assessment and salvage
- Notification
- Personnel safety
- Communications

- Public utilities and infrastructure
- Logistics and supplies
- Fire protection
- Business resumption planning
- Restoration and recovery

Selecting Recovery Team Members When a disaster occurs, trained individuals need to respond. The recovery team members need to be familiar with recovery procedures and be available to carry them out.

The first tendency is to choose the individuals who have the most expertise and experience with the processes and systems being recovered. While this is a logical choice, those persons may not be available for one of several possible reasons:

- **Unable to respond.** A recovery team member cannot respond for one of several possible reasons:
  - Transportation outages prevent travel
  - Team member injured in the disaster
  - Team member deceased
- **Unwilling to respond.** A recovery team member is not willing to respond for one of these reasons:
  - Team member caring for injured relatives
  - Team member unwilling to leave residence

When choosing recovery team members, many alternates need to be identified, to ensure that enough qualified and/or trained personnel will be on-hand to carry out the recovery.

In addition to choosing the staff members with the most direct experience, other factors should be taken into account when choosing recovery team members;

- **Location.** Members live near the recovery site.
- **Experience.** While they may not have experience on particular systems or teams, staff members who have general experience with systems or processes would be good alternates.
- **Health.** Staff members who are in better health and physical condition will tend to be more available to respond during a disaster.
- **Family.** One can argue that a staff member who is single will be more apt to be available in a disaster than one who has family members to care for.
- **Own transportation.** Staff members who own their own vehicles will be more likely to respond than those who rely upon mass transit that may be interrupted in a disaster.

Different types of disasters have different effects on a region. For this reason it may be wise to identify two or three times the number of staff members for a recovery team than are actually required in a disaster. This way, the required minimum level of staff is more likely to actually show up.

Emergency Response The emergency response plan is an organization's "first responders" plan that carries out a number of key tasks, including:

- **Personnel safety**. When workers are on-site when a disaster strikes, emergency response personnel make sure that workers are safe. Depending upon the situation, this could include administering first aid, searching for all personnel, and so on.
- **Evacuation**. Emergency response personnel should have established building, plant, and premises evacuation procedures so that all personnel can be cleared from a facility that could be damaged or present any hazard to workers.
- **Asset protection**. After ensuring the safety of personnel, the emergency response team should ensure that company assets continue to be protected after the disaster. This could include buildings, vehicles, and equipment. Mechanisms that secure these assets could be damaged or inoperative during a disaster.
- **Damage assessment**. The emergency response team needs to be able to perform a damage assessment. This could involve outside structural engineers to assess potential damage to buildings and equipment.
- **Emergency notification**. The emergency response team needs to be able to notify each other as well as initiate any emergency "call tree" or other means for communicating with staff in the organization.

Many of the tasks in this section will transition to longer-term and more formal response that is described in the remaining sections below.

A disaster response plan should always emphasize the highest priority on the safety of all personnel.

Damage Assessment and Salvage Formal assessment of all significant assets needs to take place in order to determine what assets are still usable and which are not.

For the most part, damage assessment needs to be performed by personnel who are familiar with the equipment being examined. Sure, it's easy for even a lay person to tell if some equipment is damaged and not immediately useful, but skilled personnel are needed to determine whether any latent (not obvious) damage has occurred.

Similarly, some equipment can be salvaged. Depending upon the equipment, perhaps it can be dismantled and its still-working components can be used as spares elsewhere. Or, equipment known to be damaged beyond repair can be moved away from the work area so that replacement equipment can be installed.

Notification When a disaster occurs, affected parties need to know the condition of the organization. The parties involved may include:

- **Employees**. The organization's workers need to know whether they should report to work and, if so, when and where.
- **Suppliers**. The organization's suppliers need to know whether they should continue delivering supplies to the organization, or if quantities or delivery schedules should be changed.

- **Customers**. Customers and patrons will need to know whether the organization is operating at normal or reduced capacity, operating hours, and locations.
- **Regulators**. In many industries, regulators must be notified of any disaster situations.
- **Authorities**. Law enforcement and public safety organizations may need to be informed of an organization's "ready for business" status during and after a disaster.
- **Shareholders**. The organization's stockholders and shareholders may need to be notified of a disaster.

The nature of the organization, and of the disaster itself, will help to determine how all of these parties should be notified (and it may very well be a different method for each group). Some of the possibilities for notification include:

- **Telephone**. This could be through call trees or automatic outbound calling.
- **Web site**. A temporary announcement could be placed on the organization's web site. For employees, messages on the Intranet can be used to inform employees of the disaster.
- **Signage**. An organization may need to post signs to inform visitors of the status of the organization's operations.
- **Media**. Newspaper and television stations may need to be notified, as an efficient means for notifying the public.

An Emergency Communications Plan needs to be developed to accommodate some or all of the notification and communications needs described here.

Because of the unpredictable nature of disasters, alternative means of communication should be developed and tested.

Personnel Safety The safety of all workers should be the highest priority in any disaster response scenario. Emergency response plans should put worker safety first, and ahead of all other concerns. Organizations (such as retail locations) with visitors should put visitor safety on par with worker safety, although the procedures for protecting visitors may vary somewhat from workers.

Emergency response plans should include several personnel safety measures including:

- **Emergency evacuation**. Procedures should be developed and regularly tested to evacuate personnel and visitors from a work facility. These procedures may involve the use of several trained safety personnel—workers who are trained to make sure that personnel in work areas are able to locate and use exits.
- **Medical aid**. First aid supplies should be on hand to treat injured workers and visitors.
- **Emergency supplies**. Work facilities should have a supply of emergency drinking water, food rations, blankets, and so on if a disaster results in workers being "stranded" at work locations. Supplies may also be needed for emergency response personnel should they need to remain in a work facility for several days.

Communications During a disaster, communications is both more important and more difficult. Communications is more difficult because some communications facilities may be damaged or unavailable, and some team members will be unavailable. During a disaster it's just going to be harder to find other team members to coordinate activities.

Communications is more important during a disaster because disaster operations are, by nature, less predictable than everyday operations. This requires people to be in closer contact with one another until they are familiar with disaster operations that are taking place. In other words, during a disaster people need to communicate more until they understand what's going on.

Because some communications networks may be impaired (or just congested) during a disaster, more than one means for voice and data communications are needed, to improve the likelihood that at least one will actually work. Some considerations when selecting alternate communications include:

- **Avoid common infrastructure**. Alternate communications should avoid carriers that share the same local or regional wiring plants. If the backbone fiber rings that many providers use are damaged, then chances are all of the providers' networks will not be working.
- **Diversify mobile services**. Recovery and response teams should diversify their mobile network providers. Most regions in North America have at least three mobility networks. If different team members use different networks, then an outage by one of the networks will not render the team's communication incapacitated.
- **Consider two-way radios**. Short-distance two-way radios may be a viable alternative to cellular communications if mobility infrastructure is congested or damaged.
- **Consider satellite phones**. In a severe disaster situation, all terrestrial-based communications systems (landline, mobile) may be damaged or impaired. While more expensive, satellite phones are more likely to work during a disaster since they do not depend on local communications infrastructure.
- **Consider amateur radio**. In a significant disaster, amateur radio may be the only way to communicate important information with the outside world.

Public Utilities and Infrastructure

A disaster may temporarily impair or interrupt the delivery of public utility services such as electricity, natural gas, water, and steam. In a severe disaster, one or more of these utilities may be unavailable for many days. Organizations located in a disaster-stricken area will need to develop contingency plans for going without various utilities for a time.

Electricity

Short interruptions in electric power are not uncommon in most areas. The impact of a power outage on an organization has a lot to do with its reliance on a continuous supply of electricity. Because most organizations have some reliance on information systems, a growing number of organizations have one or two phase contingency plans for generating their own electric power during an outage. These plans usually include:

- **Uninterruptible Power Supply (UPS)**. Computer equipment has no tolerance for interruptions in electric power. A UPS system provides continuous electric power through the use of storage batteries. Depending upon the needs of an organization, a UPS can provide electric power for as little as several minutes and as long as several hours.
- **Electric generator**. Powered by diesel fuel, gasoline, or natural gas, an electric generator can provide electricity for as little as a few hours and as long as many days. Generators

can also be refueled, extending the time that they can provide electric power. Generators usually take several seconds to a minute or longer to start and provide electric power, so generators are usually used in coordination with UPSes to provide a long-term steady supply of electricity to a facility that has a high reliance on electricity.

Water Earthquakes, landslides, and other events can damage water mains, interrupting water supplies to businesses. In severe disasters, emergency water supplies are often brought in by truck or even airplane.

The first concern for a supply of water is emergency drinking water for personnel. Organizations can maintain a supply of emergency drinking water in bottles or tanks. However, since water is also used for sanitation and fire suppression, in most locations government authorities (usually a fire marshal or health inspector) will not permit an organization to continue operations in a building that has no reliable water supply.

Natural Gas Earthquakes and other disasters can damage natural gas lines, resulting in service interruptions. Natural gas is used for heating, cooling, cooking, and other functions.

Several factors make it impractical to employ an emergency or alternative gaseous fuel supply, and few organizations do so. Contingency and response plans need to include steps to be taken if the natural gas supply is interrupted for long periods of time.

Wastewater Treatment In most areas, organizations rely upon centralized sanitary sewage treatment systems for wastewater treatment. If a disaster has damaged wastewater treatment plants or major piping systems, an organization may have to stop utilizing incoming water. Health authorities may require the evacuation of the facility.

Steam Also known as *district heating*, steam heat services in cities provides heat for buildings. A disaster can cause interruptions in steam heat for hours to days. Organizations heated with steam heat need to develop contingency plans for events that may cause interruptions in heating service.

Logistics and Supplies Emergency response procedures require considerable advance planning, to ensure that essential supplies and staff needed for evacuations, assessments, salvage, and recovery are at-hand or readily available. Supplies that may be needed include:

- **Food and drinking water**. Emergency response teams that may need to remain for several days at a work facility will need food and drinking water for sustenance. Blankets and sleeping cots may also be needed if there is no nearby lodging available.
- **Sanitation**. Toilets, showers, and so on.
- **Tools**. Whatever tools that are needed for salvage and repairs of buildings and business equipment.
- **Spare parts**. Parts and whatever is needed to repair buildings and business equipment. When a disaster occurs, transportation may be hampered and needed parts will be in short supply and difficult and costly to obtain.
- **Waste bins**. Receptacles for damaged goods, as well as waste generated during salvage and repair operations.

- **Information.**
- **Communications.**

The specific nature of an organization will add color and depth to the logistics and supplies needed for adequate emergency response.

Fire Protection Fire prevention capabilities are required in virtually locale in the world. Required systems in business locations include one or more of the following:

- Fire extinguishers
- Smoke detectors
- Automatic sprinkler systems
- Fire alarm systems

Business Resumption Planning When a disaster strikes, one of the most vital activities to be undertaken is the resumption of critical business processes. Whether or not they are supported by IT applications, business processes are the vital activities in organizations. The whole point of business continuity planning is to figure out how to keep the most vital processes operating, even when a disaster strikes.

Of course, where a business process relies upon an IT application to function, then that IT application needs to have its own recovery capability to meet the needs of the process(es) it supports.

The Business Impact Analysis (BIA) should explore each process thoroughly enough to determine where the critical activities are in each process. It is then up to BCP team members to develop a contingency plan for each critical process that will enable it to meet the RPO and RTO targets that were established during the BIA.

Depending upon the nature of the business process, one or more of these considerations may be required during the development of contingency plans:

- **Alternate location.** Depending upon the nature of the process and the business, alternate locations for critical processes may need to be identified before a disaster takes place. The alternate location may need to be stocked with supplies, procedures, and records so that the process can be quickly resumed.
- **Alternate personnel.** If the alternate location is some distance away from the primary location, it may be more reasonable for alternate personnel to perform duties there. The source of these alternate personnel might be a temp agency or employees in another work location.
- **Communications.** Personnel operating out of another location will probably need communications capabilities—voice, data, or both, in order to support the critical processes performed there.
- **Standby assets and equipment.** Equipment and machinery required to support the process need to be acquired timely, to meet the recovery targets.

- **Access to procedures**. Personnel in the alternate location need access to work procedures so that they know how to perform their duties.
- **Access to records**. Personnel may need to have access to business records in order to perform their duties.

Restoration and Recovery The point of business continuity planning and disaster recovery planning is getting the business up on its feet after a disaster. The organization's emergency response will be multi-faceted in order to manage all aspects of a disaster, including personnel safety, damage assessment, and the recovery of facilities and assets to once-again support business operations. This section is concerned with the restoration of business operations in a work facility.

When a disaster first strikes, emergency response is concerned primarily with personnel safety and evacuation, followed by damage assessment and salvage. Once the extent of the damage to facilities and equipment are known, efforts to restore business operations can begin.

Depending upon the extent of damage, restoration may consist of minor repair, major repairs, or (in extreme situations) a complete replacement of facilities and assets. Any staff or assets that able to remain in the facility may need to relocate during repair or rebuilding operations—business continuity plans need to allow for this possibility.

Remember that restoration and recovery operations are completely separate from business continuity efforts that focus on the continued delivery of services.

When repairs have been completed, business operations need to be transitioned back into the repaired and recovered facility. This may require interruptions in service as personnel and equipment are relocated from a temporary work location. This relocation will need to be scheduled and announced, so that any interruptions in service can be anticipated and planned around.

Improving System Resilience and Recovery

During the Business Impact Analysis (BIA), two important recovery targets were established: Recovery Time Objective (RTO) and Recovery Point Objective (RPO). For each IT system, an analysis needs to be made to determine whether the system is currently able to meet those objectives, or whether changes in architecture are required. If improvements in RPO and RTO are needed, one or more of the following architectures and technologies may be needed:

- Off-site media storage
- Server clusters
- Data replication

Off-Site Media Storage Backups of critical data should be performed frequently. The rule-of-thumb starting point for a backup strategy is a full backup once per week and an incremental backup daily. Actual business and recovery needs will determine whether full and incremental backups need to be performed more or less frequently than this.

Backup media should be stored off-site in a secure facility. The means of transport to and from the off-site facility should itself be secure. Detailed and accurate records of all media moved to and from the off-site storage facility should be available. The off-site media storage

facility should be audited for adequacy and integrity of security and recordkeeping controls and should be free of security incidents.

Server Clusters In cases where RPO and RTO values are less than a one hour, there probably will not be sufficient time for staff members to build and ready backup servers. Server **clusters** should be considered for applications with high-availability needs, even in the event of a severe disaster that makes a primary server unavailable for any reason.

Clusters permit an application to operate on two or more servers. In a cluster, one server can be taken offline without interrupting the application. A **failover** occurs when production workload is transferred from one server to another server in a cluster.

Two types of cluster configurations are:

- **Active-Active**. In an active-active cluster, all servers in the cluster are providing service.
- **Active-Passive**. In an active-passive cluster, one or more *active* servers in a cluster are providing service, while one or more *passive* servers are in standby mode, ready to provide service if needed.

A **geographic cluster**, or geo-cluster, is a cluster in which the cluster members are located hundreds or thousands of miles apart and communicate via WAN connections. Geo-clusters may be needed for applications with very low RPO and RTO targets.

Another advantage of server clusters is that unexpected software or hardware failures result in little or no downtime, as other cluster members can take over application workload with little or no administrative intervention.

Data Replication Data **replication** refers to any mechanism that copies data in real-time or near-real-time from one storage system to another. The storage systems can be located in the same room or thousands of miles apart.

Data replication can be performed in several ways, including:

- **Application**. The application can be programmed to store information on two different databases that can be located near each other or great distances apart. This method is not often used, since changes in remote storage may require changes to the application logic.
- **Database Management System (DBMS)**. Database management systems can be configured to replicate database transactions to a remote database. This is a common replication solution that has been in use since the 1990s.
- **Operating system**. The operating system can force disk transactions to be sent to two different storage systems. When used, this is usually a part of a clustering solution.
- **Storage hardware**. The RAID, SAN, or NAS hardware platform can itself replicate disk transactions to a counterpart hardware platform in the same location or in a different location.

The advantage to data replication is that application data can be "ready" on a backup storage system in near-real-time, even in a location that is far away from the main production facility. This provides very good RPO targets for applications that tolerate very little data loss even in a disaster.

Training Staff on Business Continuity and Disaster Recovery Procedures

Organizations that invest time and resources in the development of a business continuity and disaster recovery plan need to remember that the ultimate success of a BCP and DRP plan is only as good as its employees are able to carry it out. Training on disaster response and recovery procedures is an essential and necessary part of a complete BCP and DRP project.

Training can take many forms, including:

- **Participation in testing**. Staff members will become more familiar with emergency response and disaster recovery procedures when they participate in the various types of tests that should be regularly performed. Testing is discussed in detail in the next section.
- **Formal training sessions**. Training on emergency response and disaster recovery procedures in classroom or web-based training settings will help staff members better understand how these procedures are supposed to be carried out. This type of training is especially important when new DRP/BCP plans and procedures have been developed.

Testing Business Continuity and Disaster Recovery Plans

When BCP and DRP plans have been developed, they need to be tested. The five types of testing that are available include:

- Document review
- Walkthrough
- Simulation
- Parallel test
- Cutover test

Testing is also a part of plan maintenance, which is discussed in the next section.

Document Review

In this first step of testing, **document review**, emergency response and recovery procedure documents are circulated to subject matter experts in the organization for review and comment. Those who review the documents may or may not be on response teams, and reviewers could even include outside experts.

Walkthrough

A **walkthrough** test is similar to document review, but it's performed by groups instead of individuals. A facilitator will step the group through a recovery or response procedure, evoking discussion and questions along the way. Group discussion helps to identify issues that individuals might not consider.

Several hours of uninterrupted time needs to be scheduled for a walkthrough, so that the review team can get all the way through procedure documents. The continuity of thought helps to improve the quality of the walkthrough.

Simulation

A **simulation** is similar to a walkthrough, but with an added twist: the walkthrough is performed as though a real disaster was taking place. Usually scheduled to take place over an entire workday, a simulation begins with a facilitator reading some announcements describing a disaster that is unfolding in real-time. Over the course of the day, the facilitator will read additional announcements, simulating a real disaster and the news that trickles in over time.

A simulation helps the team to better imagine that a disaster is taking place *right now*, and it helps them to step through emergency response procedures with realism that is not present in a walkthrough.

A well run simulation usually takes considerable advance planning in order to make it realistic and valuable.

Parallel Test

A **parallel test** is an actual test of recovery procedures and systems. As the name implies, regular business operations continue operating, and recovery processes and systems are initiated *as though* a disaster were taking place.

The advantage of a parallel test is the actual use of disaster recovery and/or emergency response procedures. Because the recovery processes and systems are run in parallel to production processes and systems, a failure of a test does not threaten actual business operations.

It is important to perform very detailed recordkeeping during a parallel test, and then to compare the results of the parallel test with actual business operations, to see if the recovery procedures and systems are operating correctly.

Cutover Test

A **cutover test** is the ultimate test of emergency response and disaster recovery procedures. In a cutover test, actual production systems and/or processes are shut down and those functions are supported entirely by DR procedures and systems.

The failure of the DR system places actual business processes at risk. If the disaster recovery processes or systems do not function correctly, actual business processes will be interrupted until the DR systems are fixed or the business resumed on normal production systems.

A successful test gives confidence that the DR system can actually support the business. This may include not only the correct processing of business processes but also the fact that DR systems are able to handle production levels of work.

Maintaining Business Continuity and Disaster Recovery Plans

DRP and BCP plans are like software: after their initial versions have been designed, built, and tested, they will enter a "maintenance mode" where they will be periodically updated over a period of several years. DRP and BCP have a life cycle that is very similar to the software development life cycle.

Some of the events that necessitate review and modification of DRP and BCP procedures include:

- Changes in business processes and procedures
- Changes to IT systems and applications
- Changes in IT architecture
- Additions to IT applications
- Changes in service providers
- Changes in organizational structure

Personnel who are responsible for maintaining BCP and DRP processes and procedures should kept "in the loop" whenever changes in IT systems, business processes, or suppliers are considered. This will help to avoid situations where disaster response procedures suddenly become outdated and ineffective. Organizations that employ formal projects to make changes to systems and processes should include BCP and DRP personnel in those projects to ensure that changes will not threaten the organization's ability to recover systems and processes in the event of a disaster.

Chapter Summary

- A disaster is a natural or man-caused event that damages property and assets, injures or kills people, and impairs the ability for organizations to continue operating.
- Disasters affect businesses by directly damage business assets; disasters often damage transportation and public utilities, which indirectly affects businesses.
- Natural disasters include earthquakes, volcanoes, tsunamis, landslides, hurricanes, tornadoes, wind storms, ice storms, snow storms, lightning, avalanches, fires, and floods.
- Man-made disasters include strikes and other work slowdowns, war, terrorism, sabotage, vandalism, civil unrest, cyber attacks, blockades, chemical spills, power failures, communications outages, water supply shortages, fuel shortages, and radioactive fallout.
- Disasters affect businesses by interrupting the supply of necessary materials, personnel, services, and other factors necessary for continued business operations.
- BCP and DRP support security by protecting the *availability* of information and services even during a disaster.
- Industry standards related to BCP and DRP include ISO17799, BS25999, NIST 800-34, NFPA 1600/1620, and HIPAA.
- The benefits of business continuity and disaster recovery planning are reduced risk, improved processes, elevated organizational maturity, improved availability and reliability, and marketplace advantage.
- Steps taken at the onset of a BCP/DRP project include gaining executive support, defining scope, choosing team members, and developing a project plan.
- The first main step in a BCP/DRP project is the development of a Business Impact Analysis (BIA), which documents the effects on the organization of the failure of each important business process. The steps to creating a BIA are surveying business processes, performing a risk analysis, determining maximum tolerable downtime, and establishing key recovery milestones.

- Maximum Tolerable Downtime (MTD) is the period of time after which the organization would suffer considerable pain were the process unavailable for that period of time.
- Recovery Time Objective (RTO) is the maximum period of time that a business process or IT system will be unavailable during a disaster.
- Recovery Point Objective (RPO) is the maximum acceptable amount of data loss or work loss for a given process.
- Criticality Analysis is the process of ranking business processes in order of criticality to the organization. The processes listed first would be considered the most critical, while those further down the list would be less critical.
- Recovery team selection needs to take into account not only the expertise that each team member has in a particular functional area, but also the likelihood that he or she will actually be able to respond in a disaster.
- The initial stages of Emergency Response is primarily concerned with personnel safety, evacuation, and initial damage assessment.
- Damage Assessment and Salvage activities determine the extent of damage and which assets or equipment can be salvaged.
- Communications is a vital part of disaster response and includes communications to staff, suppliers, customers, regulators, shareholders, and authorities.
- Disaster recovery and business continuity plans need to take into account the possibility of long-term interruptions in public transportation and utilities.
- Restoration and recovery is primarily concerned with repairing facilities and equipment to permit the resumption of business operations in the primary work locations.
- Staff members, particularly those who are identified as response personnel, need to be trained on response and recovery procedures.
- The types of BCP and DRP testing are document review, walkthrough, simulation, parallel test, and cutover test.
- After BCP and DRP plans have been developed and tested, they need to be periodically examined and maintained so that they remain up to date and effective.

Key Terms

Business Continuity Planning (BCP) the activities required to ensure the continuation of critical business processes in an organization.

Business Impact Analysis (BIA) the task of identifying the business impact that results from the interruption of a specific business process.

Cluster a group of two or more servers that operate functionally as a single logical server, and will continue operating as a single logical server in the event that one of the servers fails.

Criticality Analysis the process of ranking business processes according to their criticality to the organization.

Cutover test a test of a disaster recovery or business continuity plan in which backup or recovery systems or processes are operated in place of normal business operations.

Data Replication See *replication*

Disaster any event that disrupts the operations of a business in such a significant way that a considerable and coordinated effort is required to achieve a recovery.

Disaster Recovery Planning (DRP) the activities concerned with the assessment, salvage, repair, and restoration of damaged facilities and assets.

Document review a review of a business continuity or disaster recovery procedure in which a single individual reviews procedures.

Electric Generator See *generator*.

Failover an event in a server cluster where production workload is transferred from one server to another.

Generator a backup power source that derives its power from a fossil-fuel powered electric generator.

Geographic cluster a cluster whose members are dispersed over a wide geographic area.

IT Service continuity the process of ensuring the continuity of IT-provided services and systems.

Man-made disaster a disaster caused by people or organizations.

Maximum Tolerable Downtime (MTD) the period of time after which the organization would suffer considerable pain were the process unavailable for that period of time.

Natural disaster a disaster caused by a natural event such as an earthquake or flood.

Parallel test a test of a disaster recovery or business continuity plan in which backup or recovery systems or processes are operated alongside normal business operations.

Recovery Point Objective (RPO) the maximum acceptable amount of data loss or work loss for a given process.

Recovery Time Objective (RTO) the maximum period of time that a business process or IT system will be unavailable during a disaster.

Replication an operation concerning the data on a storage system, where additions and changes to the data are transmitted to a counterpart storage system where the same additions and changes take place.

Risk analysis the process of identifying risks, their probability of occurrence, impact, and mitigating steps to reduce probability or impact.

Simulation a review of a disaster recovery or business continuity procedure that is performed in a pretend disaster scenario.

Statement of impact a document that describes the impact that an interrupted business process would have on an organization.

Threat analysis the process of identifying potential threats, their probability of occurrence, impact, and mitigating steps to reduce probability or impact.

Uninterruptible Power Supply (UPS) a short-term backup power source that derives its power from storage batteries.

Walkthrough a review of a business continuity or disaster recovery procedure in which a group of individuals review and discuss procedures.

Review Questions

1. The purpose of a Business Impact Analysis (BIA) is to determine:
   a. The impact of a disaster
   b. The extent of damage in a disaster
   c. Which business processes are the most critical
   d. Which processes depend on IT systems
2. During the early phases of a disaster recovery project, the project team needs to identify the disaster scenarios that can jeopardize the ongoing viability of the organization. The team should perform:
   a. A business impact analysis
   b. A threat analysis
   c. A walkthrough test
   d. A failover test
3. Maximum Tolerable Downtime (MTD) should be determined by:
   a. The project manager
   b. The risk manager
   c. Senior management
   d. The threat modeling tool
4. Recovery Time Objective (RTO) is defined as:
   a. The maximum length of time that a business process will be unavailable during a disaster
   b. The maximum amount of data loss during a disaster
   c. The point-in-time when a recovery is initiated after a disaster
   d. The maximum period of time that a business can tolerate downtime during a disaster
5. Recovery Point Objective (RPO) is defined as:
   a. The maximum length of time that a business process will be unavailable during a disaster
   b. The maximum amount of data loss during a disaster
   c. The point-in-time when a recovery is initiated after a disaster
   d. The maximum point in time that a business can tolerate downtime during a disaster
6. The purpose of a criticality analysis is:
   a. Develop a rank ordered list of the most critical threats
   b. Develop a rank ordered list of the most critical business processes
   c. Develop a rank ordered list of the most critical vulnerabilities
   d. Develop a rank ordered list of the most critical staff

7. Because of limited resources, Company A cannot develop disaster recovery plans for all of its process. What should Company A use to determine which processes require recovery plans?
   a. Those that are ranked highest in the criticality analysis
   b. Those with the lowest MTD values
   c. Those with the highest MTD values
   d. Those that are ranked lowest in the criticality analysis
8. Which should be protected first during a disaster:
   a. Critical business records
   b. Critical systems
   c. Backup media for critical systems
   d. Personnel
9. The purpose of UPS is:
   a. Filter electric power created by an electric generator
   b. Delivery of critical supplies during a disaster
   c. Protection of electric generators during a power failure
   d. Continuous electric power during a power failure
10. Over a period of several years, an organization has exceeded the capacity of its emergency electric generator. The organization should:
    a. Increase UPS capacity to make up the difference
    b. Purchase a larger generator that can handle the entire workload
    c. Purchase an additional generator so that the old and new generators together will generate enough power
    d. Decrease UPS capacity to make up the difference
11. An organization is experiencing a large number of spikes, surges, and noise on its incoming electric power. The organization should consider:
    a. An electric generator
    b. An uninterruptible power supply (UPS)
    c. A line conditioner
    d. A power distribution unit
12. An organization has just completed development of a disaster recovery plan. The first test of the plan that should be performed is:
    a. Parallel
    b. Simulation
    c. Walkthrough
    d. Cutover

13. A company has determined that its Recovery Time Objective (RTO) for a critical system is three minutes. In order to ensure the continuous availability of its critical systems, the company should consider:
    a. An active-passive geographic server cluster
    b. An active-active local server cluster
    c. An active-passive local server cluster
    d. An active-active geographic server cluster
14. A company has determined that its Recovery Time Objective (RTO) for critical systems is two hours. In order to facilitate a timely resumption of critical applications, the company should consider:
    a. Data replication to servers in a hot site
    b. Data replication to servers in a warm site
    c. Clustered servers
    d. Disk to disk backup
15. The risk associated with a cutover test is:
    a. A failure will result in a service interruption
    b. A failure will result in data loss
    c. A failure will result in data corruption
    d. Adverse publicity

Hands-On Projects

Project 4-1: Develop a Personal Disaster Plan

In this project you will develop a personal disaster preparedness plan.

1. Determine which types of natural disasters are the most common for the region in which you live.
2. Find out which government or private agencies and organizations have information on disasters for your area.
3. Develop a written plan for how you will prepare in advance for the most likely disaster(s) that may occur in your area.
4. Develop a written plan for how you will communicate with others during the most likely disaster(s) in your area. Identify who you will communicate with, and why.
5. Develop a written plan for what you will do after a disaster strikes.
6. Include in your written plans a process for teaching the plan to other family members, and how the plan will be periodically updated.

Project 4-2: Improve a Contingency Plan

In this project you will analyze an existing contingency planning document and make recommendations for improvement.

1. Go to the U.S. Department of Health & Human Services web site and download the Business Pandemic Influenza Planning Checklist at http://www.pandemicflu.gov/plan/pdf/businesschecklist.pdf.
2. Imagine that you are responsible for emergency planning in your organization. Is this plan adequate? Can this plan be implemented in your organization?
3. Make any recommendations for how the plans in the publication can be implemented, as well as any changes that should be made.

Case Projects

Case Project 4-1: Set RPO and RTO Objectives for a Web-Based e-mail Application

As a consultant with the Ace Security Consulting Co., you have been hired to establish RPO and RTO objectives for a web-based e-mail application that is used by the Smith Chemical Company.

Smith Chemical does not have the analytical skills to make proper and reasonable determinations for RPO and RTO. Your objective is to establish reasonable RPO and RTO targets and justify them by comparing the value of the application against any additional costs required with achieving the RPO and RTO targets.

Case Project 4-2: Evaluate NIST 800-34

As a consultant with the Ace Security Consulting Co., you have been asked to evaluate the use of NIST 800-34 as a framework and guide to contingency planning for a medium sized business.

NIST 800-34 can be downloaded from http://www.nist.gov/.

Answer the following questions:

1. Does NIST 800-34 adequately address the issue of protecting sensitive data during recovery operations?
2. Have any technology advances since the publication of this document made contingency considerations outdated?

chapter 5

Cryptography

Topics in this Chapter:

- Applications and Uses of Cryptography
- Encryption Methodologies
- Cryptanalysis
- Management of Cryptography
- Key Management

The (ISC)^2 *Common Body of Knowledge* (CBK) defines the key areas of knowledge for Cryptography in this way:

The candidate will be expected to know basic concepts within cryptography; public and private key algorithms in terms of their applications and uses; algorithm construction, key distribution and management, and methods of attack; and the applications, construction and use of digital signatures to provide authenticity of electronic transactions, and on-repudiation of the parties involved.

Key areas of knowledge:

- *Understand the application and use of cryptography (e.g., confidentiality, availability, and integrity)*
- *Understand methods of encryption (e.g., one-time pads, substitutions, permutations)*
- *Understand types of encryption (e.g., stream, block)*
- *Understand initialization vectors (IV)*
- *Understand cryptographic systems*
- *Understand the use and employ key management techniques*
- *Understand message digests/hashing (e.g., MD5, SHA, HMAC)*
- *Understand digital signatures*
- *Understand non-repudiation*
- *Understand methods of cryptanalytic attack*
- *Employ cryptography in network security (e.g., SSL)*
- *Use cryptography to maintain e-mail security (e.g., PGP, S/MIME)*
- *Understand Public Key Infrastructure (PKI) (e.g., certification authorities, etc.)*
- *Understand alternatives (e.g., steganography, watermarking)*

Applications and Uses of Cryptography

Cryptography is the science of hiding information, in order to conceal it from unauthorized parties.

An early use of cryptography was employed in the first century B.C. to **encipher** secret messages during military conflicts. The so-called Caesar Cipher (depicted in Figure 5-1) consisted of letters in the message being shifted three to the right, so that the message:

ATTACK AT ONCE VIA NORTH BRIDGE

… would appear as:

DWWDFN DW RQFH YLD QRUWK EULGJH

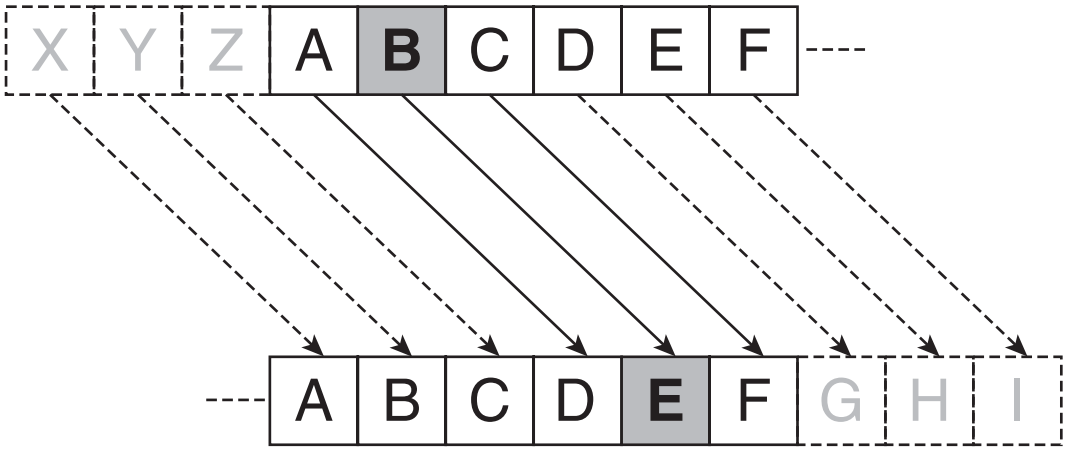


Figure 5-1 Caesar substitution cipher

Source: Course Technology/Cengage Learning

The science of cryptography has steadily improved from ancient times to the present day with increasingly complex methods.

Encryption Terms and Operations

Cryptography has a language all its own that is explained in this section.

Plaintext **Plaintext** is an original message. Plaintext may literally *be* a message, or it may be a document, data file, image, or any other type of digital information.

Encryption **Plaintext** is transformed into **ciphertext** through the process of encryption or **encipherment** (the terms **encrypt** and **encipher** have the same meaning). The process of encryption requires the use of a **key**.

An encrypted message can be safely transmitted to another party, even using means that may permit third parties to read the ciphertext.

Decryption When the recipient receives the **ciphertext** message, the recipient **decrypts** (or **deciphers**) the message, which yields the original **plaintext**.

Encryption Key Both the sender and the recipient must have an encryption **key**. This key is used to **encrypt** and **decrypt** the message. The key must be carefully guarded; if any third party is able to obtain the key, that third party can **decrypt** messages, and the third party can also create encrypted messages.

The operations used to this point are illustrated in Figure 5-2.

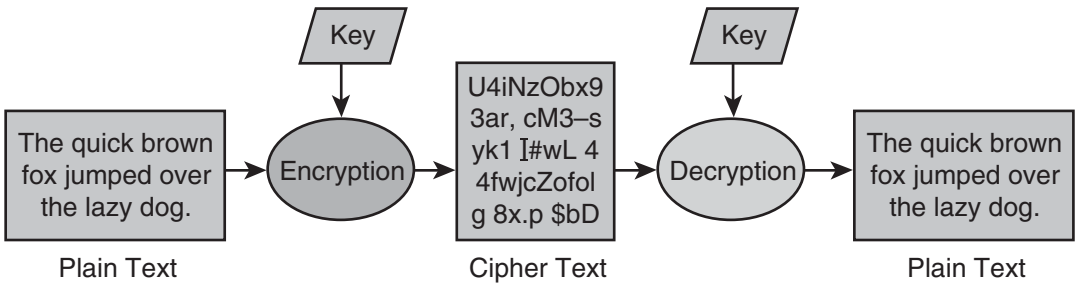


Figure 5-2 Typical encryption and decryption operations

Source: Course Technology/Cengage Learning

Encryption Methodologies

There are several forms of encryption in use. The discussions in this section center around three concepts:

- **Methods of encryption.** These are the ways in which plaintext is transformed into ciphertext.
- **Types of encryption.** The two types of encryption are **stream ciphers** and **block ciphers**.
- **Types of encryption keys.** The two types of keys are **symmetric** and **asymmetric**.

Methods of Encryption

There are several ways in which a plaintext message can be transformed into ciphertext. Some of these methods are pretty simple while others get pretty complicated. The methods of encryption discussed here are:

- Substitution
- Transposition
- Monoalphabetic
- Polyalphabetic
- Running-key
- One time pads

Substitution A **substitution cipher** employs some scheme of character substitution. For instance, every instance of "A" in plaintext is changed to "r" in ciphertext, "B" is changed to "8," and so on, using a pattern or algorithm that is known to both the sender and recipient of a message.

The *Caesar Cipher*, used in the first century B.C., was an early substitution cipher, in which plaintext characters were shifted three to the right to yield ciphertext. *ROT13* is another simple substitution cipher in which English alphabet letters are shifted 13 to the right.

Transposition A **transposition cipher**—also known as **permutation cipher**—is one in which the characters in a plaintext message are rearranged—or *transposed*—to form the ciphertext.

The characters in a plaintext message still appear in the ciphertext, but in different order. This makes a transposition cipher vulnerable to **frequency analysis**—a type of attack against a cryptosystem where the frequency of occurrence of the characters in ciphertext is examined.

An early transposition cipher is rectangular substitution. Using the example used previously:

ATTACK AT ONCE VIA NORTH BRIDGE

The encryption would first write the characters into a rectangle pattern such as:

A	K	C	N	B
T	A	E	O	R
T	T	V	R	I
A	O	I	T	D
C	N	A	H	G

… and then read the characters out of the table by reading across, giving the following ciphertext:

AKCNBTAEORTTVRIAOITDCNAHG

The secret to effective transposition cipher is a more-complex method of transposing characters than the simple example used here.

Monoalphabetic A **monoalphabetic cipher** is a type of substitution cipher where one alphabetic character is substituted for another. In the example of the Caesar Cipher, letters are shifted by three:

A	B	C	D	E	F	G	H	I	J	…	Z
D	E	F	G	H	I	J	K	L	M	…	C

The substitution can be more "random" instead of just a shift to the left or right. For example:

A	B	C	D	E	F	G	H	I	J	…	Z
W	E	R	T	B	N	P	Q	C	U	…	X

Using this key, the plaintext word CAGED would be encrypted as RWPBT.

Like a transposition cipher, a monoalphabetic cipher is subject to a **frequency analysis** attack.

Polyalphabetic The problem with a monoalphabetic cipher is the vulnerability to frequency analysis. A more advanced form of an alphabetic substitution cipher is the **polyalphabetic cipher**. This cipher uses two or more substitution alphabets to encipher plaintext. Here is an example.

Plaintext	A	B	C	D	E	F	G	H	I	…	Z
Alpha 1	W	E	R	T	B	N	P	Q	C	…	X
Alpha 2	R	B	I	K	Q	D	X	U	N	…	E
Alpha 3	V	B	D	R	H	W	A	X	I	…	U
Alpha 4	M	U	T	X	D	G	P	O	W	…	F
Alpha 5	Y	D	V	B	J	I	K	E	Z	…	O

Each letter of plaintext is substituted with the letter from its column in each successive row. In this example, the plaintext message CAGED becomes RRADB. Note that the letter R appears twice in the ciphertext, but we note there are no repeated letters in the plaintext. Frequency analysis will be nearly fruitless against this cipher.

Running Key Cipher A **running key cipher** is a practical application on how a substitution cipher is applied to typical messages that are usually many times longer than an encryption key.

Running key ciphers and other encryption algorithms utilize modular mathematics, where alphabetic characters are converted to numeric values, typically A=0, B=1, C=2, . . . , Z=25. When the sum of these numeric values are greater than 26, we subtract 26 until the sum is less than or equal to 26—this is known as *Modulo Arithmetic*.

For example, if a message is encrypted with the key SECRET, the encryption is carried out by adding the values of the plaintext to the values of the running (repeating) key, yielding the ciphertext:

Plaintext	A	T	T	A	C	K	A	T	O	N	C	E	V	I	A	N
Key	S	E	C	R	E	T	S	E	C	R	E	T	S	E	C	R
Plaintext	0	19	19	0	2	10	0	19	14	13	2	4	21	8	0	13
Key	18	4	2	17	4	19	18	4	2	17	4	19	18	4	2	17
Sum	18	23	21	17	6	3	18	23	16	4	7	23	11	12	2	4
Ciphertext	S	X	V	R	G	D	S	X	Q	E	H	X	L	M	C	E

The ciphertext in this example is SXVRGDSXQEHXLMCE.

The process of decryption is the reverse: subtracting the values of the keys from the ciphertext, yielding the original plaintext. And in modulo arithmetic, where ciphertext−key < zero, we add 26 to the result.

One-Time Pads Also known as a **Vernam cipher, one-time pad** encryption operates like a running key cipher in terms of the process of adding the values of the ciphertext characters and the key characters using modulo arithmetic. The differences between a running key cipher and one-time pad are:

- The key is as long as the message
- The key is used only one time and then destroyed

Continuing the ATTACK AT ONCE VIA NORTH BRIDGE example, a random key is generated and is equal to XVGJERIOQWJPEKAFANIOPSNERJ. The encryption operation is:

Plaintext	A	T	T	A	C	K	A	T	O	N	C	E	V	I	A	N
Key	X	V	G	J	E	R	I	O	Q	W	J	P	E	K	A	F
Plaintext	0	19	19	0	2	10	0	19	14	13	2	4	21	8	0	13
Key	23	21	6	9	3	17	8	14	16	22	9	15	4	10	0	5
Sum	23	14	25	9	5	1	8	7	4	9	11	19	25	18	0	18
Ciphertext	X	O	Z	J	F	B	I	H	E	J	L	T	Z	U	A	U

A one-time pad is considered unbreakable by most means, but the administration of a one-time pad makes it impractical for use in information systems.

Types of Encryption

Information systems utilize cryptography in two principle settings: when storing data, and when transmitting data. Two types of encryption have arisen from these two contexts: **block ciphers** and **stream ciphers**, respectively.

Block Ciphers A **block cipher** is used to encrypt and decrypt a block of data such as a message, document, or data file. A typical block size is 128 bits. Typical uses of block ciphers include:

- File encryption
- Web browser communications sessions
- SSH (secure shell)
- VPN (virtual private networks)

Some of the block cipher algorithms are:

- DES
- 3DES
- AES
- CAST
- Twofish
- Blowfish
- Serpent

Block Cipher Modes of Operation Several modes of operation have been developed for block ciphers. These modes have to do with the way that plaintext blocks are brought into the cipher and encrypted. The modes are:

- Electronic codebook (ECB)
- Cipher-block chaining (CBC)

- **Cipher feedback (CFB)**
- **Output feedback (OFB)**
- **Counter (CTR)**

These modes are discussed in this section—but first it is necessary to discuss initialization vectors.

An **Initialization Vector (IV)** is a starting block of information that is required for several block cipher modes. The IV is used as a part of the input data needed to encrypt the first block in the plaintext message. In order for the encryption to be secure, the IV must be random and can never be re-used.

Electronic Codebook (ECB) The **electronic codebook (ECB)** mode is the simplest mode of block cipher operation. In ECB, each block is encrypted separately. The disadvantage of ECB is that each identical plaintext block encrypts into an identical ciphertext block, making it relatively easy to attack the cipher. ECB is shown in Figure 5-3.

Cipher-block Chaining (CBC) **Cipher-block chaining (CBC)** uses the ciphertext output from each encrypted plaintext block in the encryption used for the next block. Specifically the plaintext for block N is **XOR**'d with the ciphertext for block N-1. For the first block, since there is no previous block's ciphertext to work with, the plaintext is XOR'd with the initialization vector (IV). This is illustrated in Figure 5-4.

Cipher Feedback (CFB) **Cipher feedback (CFB)** is similar to cipher-block chaining, where the result of encrypting a block of plaintext is used to encrypt the next block. In CFB, the plaintext for block N is XOR'd with the ciphertext from block N-1. In the first block, the plaintext XOR'd with the encrypted IV. This is shown in Figure 5-5.

Output Feedback (OFB) **Output feedback (OFB)** mode is similar to CBC and CFB where the results of the previous plaintext block are used in the encryption of the next block. With OFB, plaintext is XOR'd with the encrypted material in the previous block to produce ciphertext. This is illustrated in Figure 5-6.

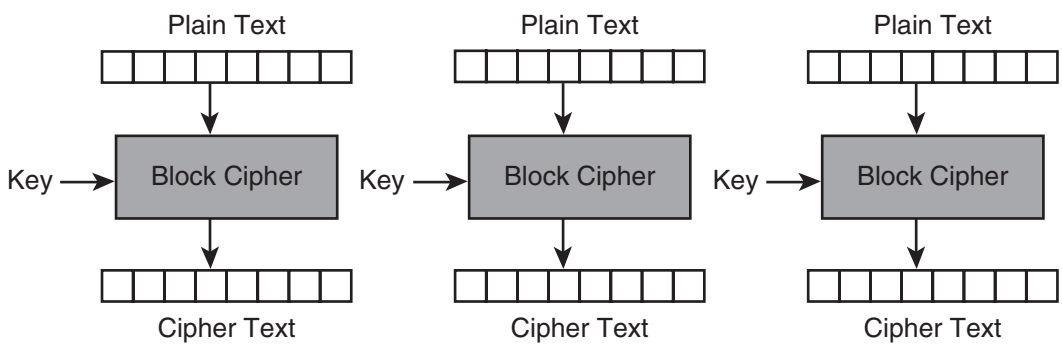


Figure 5-3 Electronic codebook (ECB) mode block cipher

Source: Course Technology/Cengage Learning

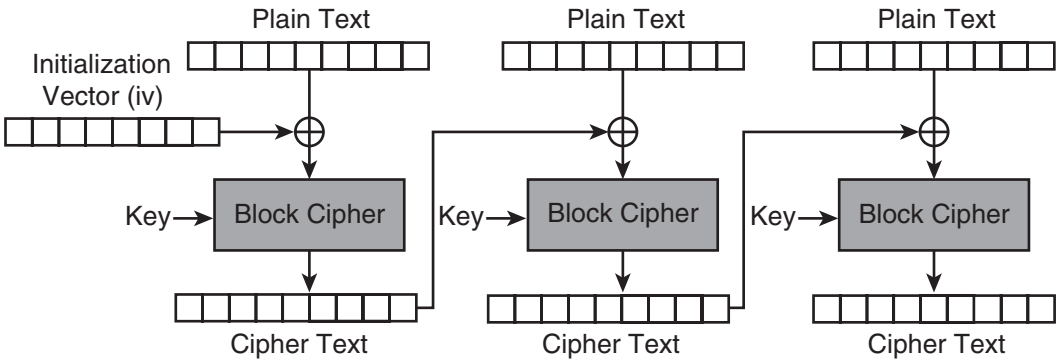


Figure 5-4 Cipher-block chaining (CBC) mode block cipher

Source: Course Technology/Cengage Learning

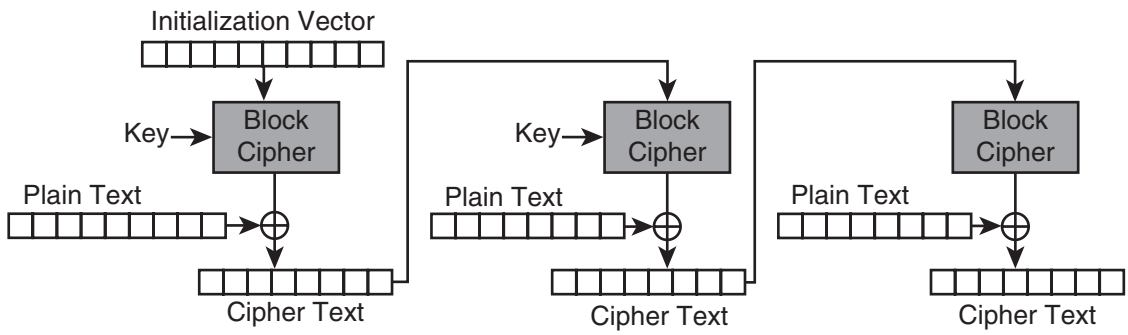


Figure 5-5 Cipher feedback (CFB) mode block cipher

Source: Course Technology/Cengage Learning

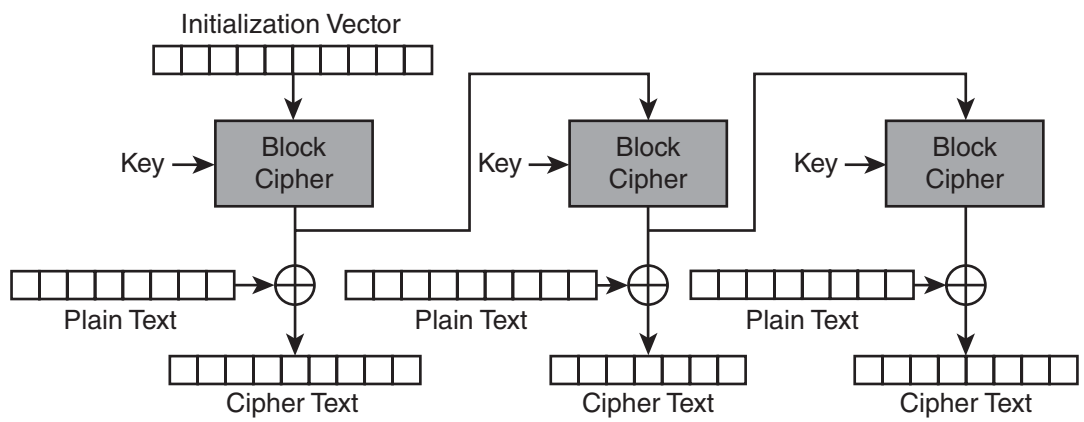


Figure 5-6 Output feedback (OFB) mode block cipher

Source: Course Technology/Cengage Learning

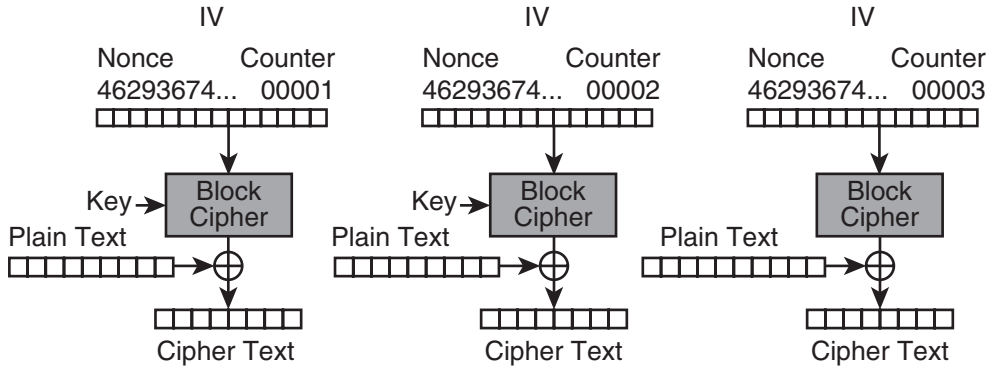


Figure 5-7 Counter (CTR) mode block cipher

Source: Course Technology/Cengage Learning

Counter (CTR) **Counter** (**CTR**) mode uses a "nonce" (a random number that is used once) that is concatenated with a counter or other simple function, which is encrypted by the block cipher, and the output XOR'd with the plaintext block to product the ciphertext block.

Figure 5-7 illustrates CTR encryption. In this case the IV is a simple counter, but other non-repeating functions can also be used to create the IV.

Stream Ciphers As the name may suggest, a **stream cipher** is an encryption algorithm that operates on a continuous stream of information, such as a video or audio communications channel.

A stream cipher is a substitution cipher that typically uses an exclusive-or (**XOR**) operation that can be performed very quickly by a computer.

A exclusive-or (XOR) is a binary operation. When the values are different, e.g., 1 + 0 or 0 + 1, the result is 1. When the values are the same, e.g., 0 + 0 or 1 + 1, the result is 0.

Here is an example of a stream cipher. Plaintext, the encryption key, and the ciphertext are all shown in binary so that the XOR operations can be easily seen.

Plaintext	1	1	0	1	0	0	1	1	0	1	0	0	1	1	0	0
Key	0	1	1	0	1	0	0	1	0	1	1	0	1	0	1	0
Ciphertext	1	0	1	1	1	0	1	0	0	0	1	0	0	1	1	0

To decrypt the ciphertext, we just XOR it with the same key to yield the plaintext:

Ciphertext	1	0	1	1	1	0	1	0	0	0	1	0	0	1	1	0
Key	0	1	1	0	1	0	0	1	0	1	1	0	1	0	1	0
Plaintext	1	1	0	1	0	0	1	1	0	1	0	0	1	1	0	0

The most common stream cipher algorithm in use is **RC4**. Other steam ciphers in use include A5/1, A5/2, FISH, Phelix1, ISAAC, MUGI, Panama, Phelix, Pike, Sapphire-II, SEAL, SOBER-128 and WAKE.

Types of Encryption Keys

Historically the only type of encryption key that was available was the *shared secret*. Both parties had to have the encryption key in their possession in order to be able to encrypt and decrypt messages.

A relatively recent innovation in cryptography is public key cryptography, described later in this section.

Symmetric Keys

Symmetric cryptography implies the use of a shared secret—that is, both parties must have possession of the same encryption key in order to be able to send encrypted messages to each other.

Both parties must robustly protect their symmetric encryption keys: if any third party is able to obtain a symmetric encryption key, that party will be able to decrypt any encrypted message exchanged between the original parties, and the third party will also be able to create new encrypted messages that the original parties may believe originated from the other party.

Some of the well known encryption algorithms that use symmetric keys include:

- **DES (Data Encryption Standard).** Developed in 1976 by IBM and designed as the U.S. NSA (National Security Agency) official cryptographic standard. DES uses a 56-bit key, considered short by today's standards. DES uses the **Digital Encryption Algorithm (DEA)**.
- **3DES.** Known as triple-DES, this extension to the original DES algorithm effectively increases the key length to 168 bits.
- **AES (Advanced Encryption Standard).** A replacement for the aging DES standard, designated in 2000. AES uses the **Rijndael** cipher.
- **Twofish.**
- **Blowfish.**
- **IDEA (International Data Encryption Algorithm).** A block cipher that is not in wide use because it is patented.
- **RC5.**

Asymmetric Key Cryptography

The classic problem in cryptography is the exchange of keys between parties that have not communicated previously. Parties that have not communicated before do not possess a common shared secret. Establishing secured communications between two parties can be a challenge, since there is sometimes no convenient means available for securely exchanging encryption keys.

Enter **asymmetric cryptography**, which is more often known as **public key cryptography**. It is so-named because a user's public key can be disclosed to the entire world with no risk that any third party will be able to decrypt a message that is encrypted using this technique.

In public key cryptography, each user has two keys: a **public key** and a **private key**. These keys are mathematically related to each other. The advantage of public key cryptography is that a user's public key can be distributed to a wide audience, and yet there is no way for any third party to derive or calculate a user's private key when they know the value of that

user's public key. A user must, however, protect their private key with the same rigor that would used to protect a symmetric key.

If a sender encrypts a message with *only* the recipient's public key, the sender will not be able to decrypt it (nor will any other party). If a sender wishes to be able to decrypt a message that he or she sends, the message must *also* be encrypted with the sender's public key!

Public key cryptography can best be illustrated through several use cases as follows:

- **Encrypt message to recipient.** An individual can publish his or her public encryption key which says, in effect, "send me a private message." Anyone can retrieve the recipient's public key, encrypt a message and send it to the recipient. No one but the recipient will be able to decrypt the message, even if they have the recipient's public key. After receiving the message, the recipient decrypts the message with his or her private key.
- **Sign message.** A user who wishes to assert authenticity and integrity of a message can sign it with his or her private key, creating a **digital signature**. Any recipient can confirm the authenticity and integrity of the message by retrieving the sender's public key and verifying the digital signature.
- **Sign and encrypt message.** A user can perform both the encryption and the digital signature operations simultaneously. The user would encrypt a message using the public key(s) of the message recipient(s) and digitally sign the message using his or her own private key. Recipients would decrypt the message using their own respective private keys, and verify the digital signature of the message using the sender's public key.

These use cases are illustrated in Figure 5-8.

Some of the well known asymmetric key encryption algorithms in use include:

- **RSA.** A key transport algorithm based upon factors of large prime numbers.
- **El Gamal.** Based upon discrete logarithms.
- **Elliptic Curve.** A new and stronger method for factoring prime numbers based upon elliptic curves.

Key Exchange Protocols

One of the problems with symmetric cryptography is the matter of transmitting a shared secret (symmetric key) to another party. A symmetric key cannot be transmitted in the clear, or else an eavesdropper will be able to intercept the key and decrypt any subsequent communications encrypted with the key. If the two parties are communicating with each other for the first time and they have no other means for communicating, then getting an encryption key to another party can be difficult.

Diffie-Hellman Key Exchange

The **Diffie-Hellman (D-H) key exchange** protocol is a means for two parties with no prior knowledge of each other to securely establish a symmetric (shared secret) encryption key.

Diffie-Hellman key exchange works like this:

1. Jane and Tom agree to a large prime number p and a base integer g. The values p and g may be transmitted over the network in the clear.

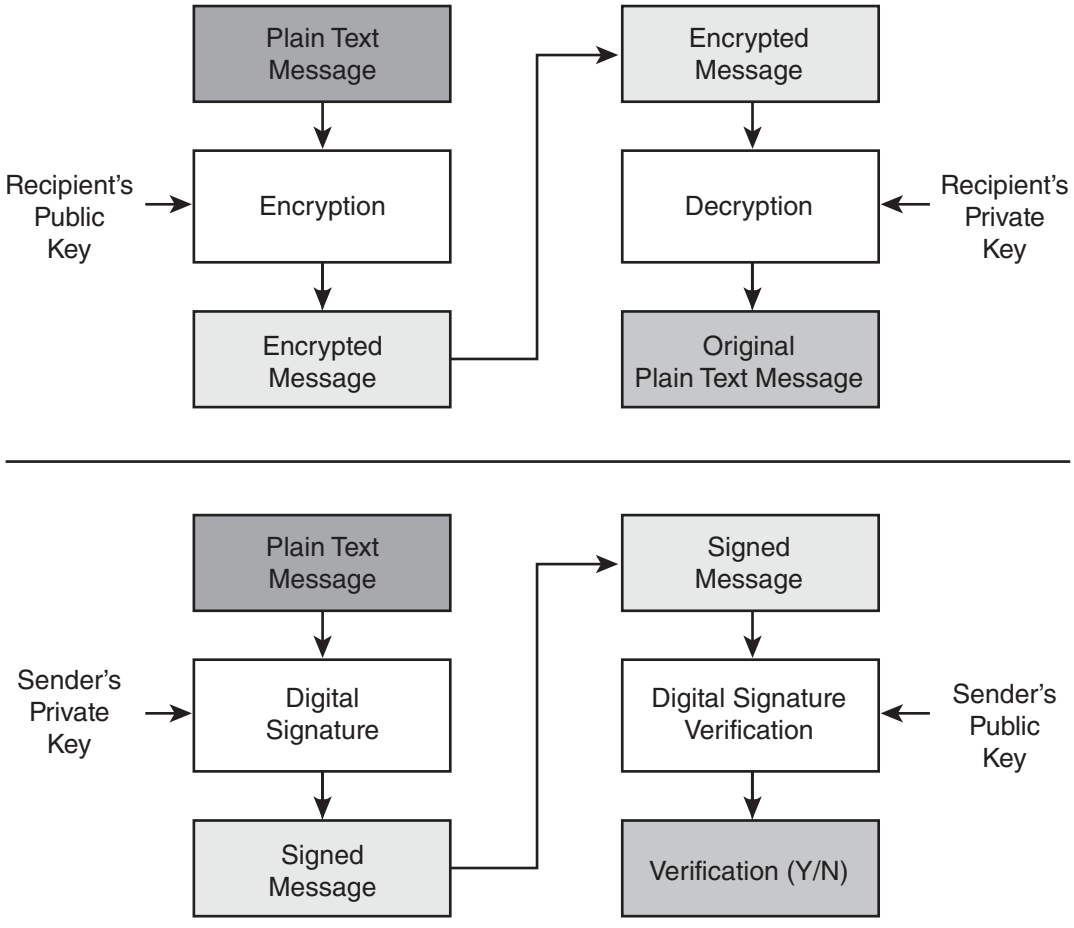


Figure 5-8 Uses of public key cryptography

Source: Course Technology/Cengage Learning

2. Jane picks a secret integer a, then calculates $g^a \bmod p$ and sends the result to Tom.
3. Tom picks a secret integer b, then calculates $g^b \bmod p$ and sends the result to Jane.
4. Jane computes $k=(g^b \bmod p)^a \bmod p$.
5. Tom computes $k=(g^a \bmod p)^b \bmod p$.

The result k in steps 4 and 5 that Jane and Tom calculate are the same, and can be used as a symmetric encryption key.

Here is a real example:

Jane and Tom agree to p = 53 and g = 16. Jane picks secret integer a = 14 and Tom picks secret integer b = 11.

Jane calculates $16^{14} \bmod 53 = 16$ and sends the result (16) to Tom.

Tom calculates $16^{11} \bmod 53 = 47$ and sends the result (47) to Jane.

Tom then calculates $16^{11} \bmod 53 = 47$.

Jane then calculates $47^{14} \bmod 53 = 47$.

The secret key that Jane and Tom have calculated is 47.

Typically, the value p will be a prime number of at least 300 digits, and the integers a and b will be at least 100 digits in length. With numbers of this size, it is computationally infeasible to break the D-H protocol even with all of mankind's computing power.

The *mod* function used above is the remainder after division. For example, 79 mod 14 = 9. In other words, 9 is the remainder after the calculation of 79 divided by 14.

Length of Encryption Keys The value of an encryption algorithm is its ability to resist attack. The strength of an encryption algorithm is based on two factors: the quality of the algorithm itself, and the length of the encryption key used.

For example, SSL encryption in the mid 1990s used a key length of 56 bits, which was considered adequate at the time. More recently, however, improving computing power made attacks of 56-bit SSL more feasible, and the new recommended minimum key length is 128 bits. Encryption keys of 256 and 512 bits are also available in SSL.

Why not just use super-long 512 or 1024 bit encryption keys in the first place? Longer encryption keys, while they result in extremely strong encryption, also require considerably more computer power. The end result is usually an encryption key length that provides reasonably secure encryption while avoiding a significant performance penalty that translates into sluggish performance and lower throughput.

There is no "magic" key length for all algorithms that are equally adequate. Remember that the algorithm itself plays a role in the strength of the encryption. If you need to select key lengths for encryption, you will need to consult with current practices to determine adequate key sizes.

Protection of Encryption Keys The secrecy of encrypted communications relies upon the strength of the encryption algorithm and the protection of encryption keys.

A defense in depth strategy should always be used to protect encryption keys. A single means of protection should not be relied upon.

Protecting Symmetric Keys In symmetric cryptography, the encryption key must be protected from unauthorized access by any third party. In some instances, the encryption key is accessed via a software program and controlled by a password. Protection of the key will in part depend upon the strength of that password. In other instances, the encryption key is contained in a stored file. Permissions on the file, and on the directory that contains the file, should be limited so that only the owner of the encryption key can access the directory or the file.

Protecting Public Cryptography Keys In public key cryptography, a user's public key needs less protection than a symmetric key. To this end, the public key can be published to a wide audience. However, while the user can publish his or her public key to the world, he or

she must ensure that no one else is able to overwrite the key with an imposter. Thus, a user's public key will need to be verified, to ensure the authenticity of the claimed individual. Typically a public key is verified by an out-of-band communication such as a telephone call, where the person verifying a public key.

A user's private key requires the same level of protection as a symmetric key. A private key must be protected with a password and/or file and directory permissions. To protect against loss, both the public and private keys should be backed up, and the backup media protected against theft or other loss.

Protecting Encryption Keys Used by Applications Encryption is frequently used by applications to encrypt and decrypt stored data. Whereas an end user can protect his or her encryption key with a password, protecting an encryption key that is used by an application is somewhat more difficult: if the application stores an encryption key's password, then the security of the encrypted data is really no stronger than just the simple password that can be found in the application.

Think about it. If an application can access an encryption key (whether a registry value, a flat file, a field in a database, or a variable in the application itself), then so can an intruder, right?

More complex means are needed to protect an encryption key used in an application, including:

- **Utilize separation of duties.** For instance, if encrypted data resides in a database, hide the encryption key in a file that the DBA cannot read. Further, permissions to the data should be set so that system administrators cannot read the data. The application itself should use a third account that neither DBAs nor system administrators can use.
- **Store encryption keys in hardware. Key management** appliances can be used to store and retrieve encryption keys.
- **Use a key encrypting key.** The actual **key** used to encrypt and decrypt data can itself be encrypted by another key called the key encrypting key.

A combination of these methods may also be used in order to provide the required level of protection.

Cryptanalysis—Attacks on Cryptography

Cryptanalysis is the study of deciphering an encrypted message without access to the encryption key. The need to decipher encrypted messages dates back to the 9th century when Arabian mathematician Abu Yusuf Yaqub ibn Ishaq al-Sabbah Al-Kindi published a manuscript on techniques for deciphering messages.

There are several modern methods used in cryptanalysis, including:

- Frequency analysis
- Birthday attacks
- Ciphertext only attack
- Chosen plaintext attack

- Chosen ciphertext attack
- Known plaintext attack
- Man in the middle attack
- Replay attack

Frequency Analysis **Frequency analysis** is the study of the frequency of occurrence of characters in a message ciphertext. If a message is encrypted using a substitution cipher, then the frequency of occurrence of the characters in the ciphertext can be used to discover the original plaintext.

Birthday Attacks The *birthday paradox* states that in a group of 23 or more randomly chosen people, there is a 50% probability that two of the people share the same birthday. This paradox leads to the **birthday attack** on a **hashing** (**message digest**) algorithm, where the attacker attempts to find messages that result in the same hash value. When two messages are found to compute the same hash value, this is known as a **collision**.

Ciphertext Only Attack A **ciphertext-only attack** (**COA**) is a cryptanalysis where the attacker has only ciphertext to work with. A COA attack can be successful by using frequency analysis and other means to either deduce the encryption key or the plaintext itself.

A well known ciphertext-only attack exploited weaknesses in the **Wired Equivalent Privacy** (**WEP**) protocol, the first encryption protocol used for WiFi.

Chosen Plaintext Attack In a **chosen plaintext attack** (**CPA**), the attacker is able to choose known plaintext messages, get them encrypted, and obtain ciphertexts for those plaintexts.

Chosen Ciphertext Attack An attacker in a **chosen ciphertext attack** (**CCA**) can choose ciphertext, have it decrypted, and obtain the plaintext. This is a trial-and-error attack that requires many decryption operations before the attacker can begin to deduce the key and/or the decryption algorithm.

Known Plaintext Attack An attacker who possesses both plaintext and corresponding ciphertext messages can analyze both in order to obtain the encryption key. This will enable the attacker to be able to decrypt all encrypted message. This type of attack is called the **known plaintext attack** (**KPA**).

Man in the Middle Attack A **man in the middle attack** (**MITM**) is a cryptanalysis attack where the attacker is able to read, insert, and modify communications between two parties with those parties' knowledge or awareness. MITM can be effective against public key cryptography and Diffie-Hellman (D-H) key exchange.

A MITM attack can be used to conduct several other types of cryptanalysis including known-plaintext (KPA), chosen ciphertext (CCA), ciphertext only (COA), and frequency analysis.

Replay Attack In a **replay attack**, the attacker intercepts and records network transmissions, for the purpose of replaying or repeating the transmissions at a later time. An

eavesdropper who records a **TELNET** (a point to point command line interface) or **FTP** (**File Transfer Protocol,** a TCP/IP protocol used to copy files from one system to another) login sequence can use the intercepted userid and password pair at a later time in an attempt to masquerade as the original party.

Application and Management of Cryptography

Cryptography is used in several ways to protect information from disclosure to unauthorized parties. Practically everywhere information is stored or transmitted, encryption can be used to provide protection against disclosure. In some instances, cryptography is used as an *additional* source of protection as part of a defense in depth information protection strategy. However, in some contexts such as the transmission of information over a public network, cryptography is often the only means available for protecting information.

Uses for Cryptography

The settings where encryption is often used are:

- Files and directories
- Entire disks and volumes
- E-mail
- Web browsing
- Remote network access

File Encryption Encryption is one form of access control that can be used to determine who is permitted to access files. When a file—even when it is present on a public file server—is encrypted, only individuals who possess the encryption key can access its contents. File encryption can also be used to protect the contents of a file when it is transmitted over a public network with e-mail or FTP.

Tools used to encrypt files include:

- **EFS (Encrypting File System).** This is the file and directory encryption capability that is built-in to Windows 2000, Windows XP, and Windows Vista. EFS protects files in-place, protecting them from access by other users on the workstation. Both files and directories can be encrypted with EFS. When a directory is encrypted with EFS, new files and subdirectories created within the encrypted directory will be automatically encrypted.
- **PGP (Pretty Good Privacy).** This popular tool can be used to encrypt files using one or more recipient public keys, or symmetric encryption using a shared secret. Unlike EFS, PGP does not encrypt files in-place; instead, it is used to create a separate encrypted file that can be left in place or sent to another party who can decrypt it.
- **GPG (Gnu Privacy Guard).** This public domain tool is compatible with most PGP functions.
- **WinZip.** This popular file archiving tool can also encrypt the contents of archives using AES.
- **Crypt.** This is a standard UNIX/Linux encryption tool that creates an encrypted copy of a file.

Disk Encryption An entire hard disk or volume (a logical subset of a hard disk) can be encrypted. Tools available for encrypting an entire volume include:

- **PGP (Pretty Good Privacy).** Commercial versions of PGP includes PGP Disk, a tool used to create an encrypted volume on a computer's hard drive.
- **TrueCrypt.** This is a public domain tool that can be used on Windows and Linux systems to encrypt the entire hard drive or create an encrypted volume.
- **BitLocker.** This tool is built into premium versions of Microsoft Windows Vista, and is used to create an encrypted disk volume that contains the operating system and user files.
- **SafeBoot.** A commercial disk encryption tool for Windows systems and PDA/smartphone platforms.

E-mail Security Parties that communicate with each other via e-mail will sometimes wish to protect their messages with encryption. Some of the methods for protecting e-mail messages are:

- S/Mime
- PGP
- PEM
- MOSS

Secure/Multipurpose Internet Mail Extensions (S/MIME) **Secure/Multipurpose Internet Mail Extensions (S/MIME)** is a certificate-based e-mail encryption standard, used to encrypt and/or digitally sign e-mail messages. S/MIME has been incorporated into many popular e-mail programs such as Outlook, Thunderbird, and Lotus Notes.

PGP **PGP (Pretty Good Privacy)** and its public domain cousin, GPG (Gnu Privacy Guard) can be used to encrypt e-mail messages that are sent to other recipients.

PGP has a tool called *PGPKeys* that is used to manage the user's private and public keys, as well as the public keys of recipients. Commercial versions of PGP (as well as the public domain GPG) have integrations with popular e-mail programs such as Microsoft Outlook that make it easy for a recipient to encrypt e-mail messages without having to perform manual encryption.

PEM **Privacy-Enhanced Mail**, or PEM, is an older standard for e-mail encryption using public key cryptography. PEM is not widely used because it depends upon the existence of a hierarchical PKI with a single root. Such a PKI has never been globally implemented.

MOSS **MIME Object Security Services (MOSS)** is a standard protocol that provides confidentiality, authentication, and **non-repudiation** using message digests and public key encryption. MOSS has never been widely used.

Secure Point to Point Communications Encryption can be used to protect communications between any two systems—two servers, two workstations, or a workstation and a server, for instance. Some of the technologies available are:

- SSH
- IPSec
- SSL/TLS

SSH **Secure Shell**, usually abbreviated as SSH, is a replacement for many of the first-generation tools that are now considered unsafe, specifically TELNET, FTP, and **rsh** (a network protocol used to establish a command line session on another system).

IPSec **IPSec** is an IP-based point-to-point communications protocol used to provide secure traffic between two endpoints. IPSec can run in one of two modes: transport mode or tunnel mode. In transport mode, each packet's payload is encrypted. In tunnel mode, a tunnel is set up between the endpoints and the entire contents of each packet (headers plus payload) are encrypted.

Security Associations (SAs) are necessary to facilitate the use of IPSec. A security association is a one-way trust relationship between two endpoints. In a one-way association, only one endpoint may initiate communications to the other endpoint. Two SAs are required if either endpoint is to be able to initiate communications.

IPSec runs in one of two modes: Authentication Header (AH), which provides authentication, integrity, and non-repudiation; and Encapsulating Security Payload (ESP), which provides encryption and limited authentication. A security association (SA) between two endpoints must specify whether IPSec will run in AH or ESP mode.

SSL and TLS **Secure Sockets Layer (SSL)** is a TCP encapsulation protocol used to provide secure communications. SSL has been superseded by **Transport Layer Security (TLS)**, although the term SSL is still in common use. In secured mode, Web browsers communicate typically via TCP port 443. The URL in a secured session will always start with "https." The traffic between the Web browser and the server will be encapsulated using the SSL or TLS protocol, using an encryption algorithm that is negotiated between the browser and the server at the start of the session. The strength of the encryption that is negotiated may be as low as a 56 bit key or as strong as a 512 bit key.

SSL/TLS are also discussed in Chapter 10, "Telecommunications and Network Security."

Web Browser and e-Commerce Security Web browsers are client programs that access Web-based applications in an organization or across the Internet. Web browsers communicate with Web servers using the HyperText Transport Protocol (HTTP) in either a secured or non-secured mode.

In non-secured mode, the Web browser communicates to the server, typically using TCP port 80. The URL in a non-secured session will start with "http." In secured mode, the URL will start with "https."

It is perfectly possible (and commonplace) to have an "http" URL with an "https" post method which ensures that data typed into form fields are sent back to the server using SSL/TLS encryption. However, on such a form, the user will not see a "padlock" signifying a secure page, which will lead them to think that the sensitive data being requested on the form will not be encrypted. It is therefore more common for web sites to encrypt a page with sensitive form fields, forcing the padlock to appear and give the user the assurance that their data will be sent back encrypted.

In e-commerce applications (that is, any web-based application in which sensitive information is displayed or exchanged such as banking, credit card, and personal information such as address, social security, and other identifying numbers), most or all data transmitted between the application and the user's browser will be encrypted. Further, session cookies will also be encrypted in order to make it more difficult for an attacker to hijack a user's session.

The discussion of e-commerce security has a lot to do with application security. This entire topic is discussed in more detail in Chapter 3, "Application Security." A secure e-commerce application requires a lot more than just a secure application, however. Virtually every chapter in this book addresses one or more topics that are related to the protection of an e-commerce application and its supporting infrastructure.

Secure Hypertext Transfer Protocol (S-HTTP) **Secure Hypertext Transfer Protocol** (**S-HTTP**) is a connectionless protocol used to encrypt and authenticate data being sent from a server to a client. It utilizes public key cryptography for authentication and non-repudiation, symmetric encryption for payload protection, and message digests for message integrity.

The main distinction between S-HTTP and SSL is that SSL encrypts an entire session, whereas S-HTTP encrypts only single requests within a session.

S-HTTP and SSL are sometimes confused for one another. S-HTTP uses the URL shttp: whereas SSL uses https:.

Secure Electronic Transaction (SET) Developed jointly by MasterCard and VISA, **Secure Electronic Transaction** (**SET**) is designed for secure electronic commerce, utilizing **X.509 digital certificates** and symmetric encryption. SET has fallen out of favor and has been replaced by SSL/TLS.

Cookies: Used for Session and Identity Management The http and https protocols do not provide session management. Http and https requests are essentially connectionless—from one click to the next, browsers and web servers have no concept of a user's logical session. From one request to the next, a Web server has no way to tell whether a subsequent request originating from an IP address is coming form the same workstation that sent a previous request. **Cookies** are typically used to identify a specific session id when a Web browser is communicating with a Web application.

Cookies contain several elements including:

- **Domain name.** This is the domain of origin for the cookie.
- **Name-Value pair.** Thought of as a variable name and contents of the variable. This is often used to identify a userid or session ID during a user's logical session with a web

application. Applications will frequently use an encrypted value, to protect against tampering and risks associated with such mischief as cookie theft. An example name-value pair is `YLID=ANm6O0cniLMAALc7R9.6AAAniLMAr7E7R9`. In this example, the variable name is YLID, and its value is `ANm6O0cniLMAALc7R9.6AAAniLMAr7E7R9`. This value could be an encrypted or hashed session ID or user ID.

- **Path.** An optional directory pathname value.
- **Expiration date.** The date when the cookie expires.
- **Secure flag.** Specifies whether the cookie should be sent over an ordinary (unencrypted) or secure (encrypted) channel.

Each time a Web application communicates with a browser, the application will request the browser's cookie. Values in the cookie will uniquely identify the individual browser and, hence, the user's session.

Virtual Private Networks A **virtual private network (VPN)** is a logical network connection between two points. All network traffic in a VPN connection is encapsulated in a "tunnel," and the traffic is encrypted, protecting the contents of the traffic from disclosure to eavesdroppers.

VPNs can be used for remote access; when VPN technology is used, the remote access session is protected from eavesdroppers.

VPNs can be used to encrypt the traffic between two separate networks. This permits two networks to communicate with each other over the public Internet with no risk of disclosure through eavesdropping. A router in each network can be configured to encrypt all traffic destined for the other network.

Both of these methods are shown in Figure 5-9.

The two prevalent technologies used to encrypt VPNs are SSL and IPSec.

An IPSec VPN requires a client program, which adds a little administrative overhead, since this VPN program must be installed and maintained on all VPN users' workstations.

SSL encryption allows so-called "clientless" VPN connections that utilize SSL capabilities that are built-in to virtually every workstation. This provides a VPN capability on a workstation without the need to install and maintain separate VPN client software.

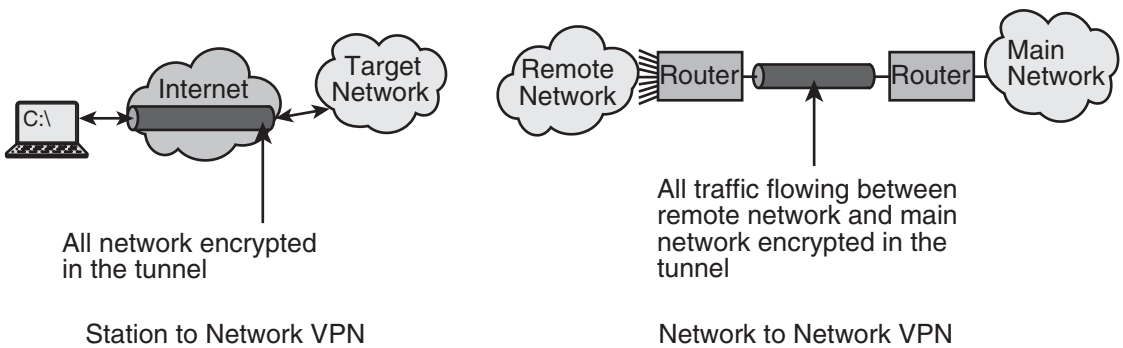


Figure 5-9 Virtual Private Networks

Source: Course Technology/Cengage Learning

Key Management

The protection of encrypted information is only as strong as its weakest link. Here, the protection factors are the strength of the encryption algorithm and **key management**, the activities related to the management of encryption keys.

The level of effort taken to protect an encryption key should correspond to the value of the information that is encrypted with the key. If an encryption key is compromised, then the ciphertext (if the intruder can find it) can also be compromised. It may be reasonable to assert the same level of protection for a key as one would for the original data in an unencrypted state.

The life cycle of encryption keys includes these activities:

- Key creation
- Key protection and custody
- Key rotation
- Key destruction
- Key escrow

Key Creation The creation of random encryption keys should be performed on a secure server, so that an intruder is not able to observe or re-create the key generation process or intercept generated encryption keys.

Key Protection and Custody Access to private keys and symmetric encryption keys must be tightly controlled. Confidentiality of encrypted information is only as good as the protection of encryption keys.

Organizations managing sensitive data may opt to employ *split custody* of encryption keys, where two or more persons are required to access an encryption key. Two or more people may have a portion of the key itself, or the password used to access the password. This prevents any single individual from being able to access or alter sensitive data that is protected with an encryption key.

Key Rotation Regulation or prudence necessitates the occasional rotation of encryption keys.

An organization that encrypts sensitive information should have formal procedures to be followed in the event that an encryption key is compromised.

Key Destruction When an encryption key is no longer needed, it should be destroyed securely. This means that the key must be destroyed in all locations where it was stored. Further, effective key destruction requires that the key be *erased* (overwritten with patterns of data so that it cannot be recovered through data remanence), not merely deleted (in many operating systems a deleted data file can be easily recovered).

In some cases, key destruction is the only way to "delete" encrypted data. For instance, data that is encrypted by several different keys is written to a backup tape. When it is time for some of the data is to be destroyed, the organization can destroy the encryption key, which effectively deletes the corresponding information from the backup tape.

Key Escrow A business arrangement can be established where a trusted third party will hold encryption keys in escrow. The typical purpose for key escrow is the greater certainty that data can be recovered, even in the event that the organization that encrypted the information experienced a disaster that destroyed its encryption keys, or upon the failure of the organization resulting in the destruction of its information including encryption keys.

Message Digests and Hashing

A **message digest**, or hash, is the result of a cryptographic operation on a message or file. A cryptographic hashing algorithm will read the entire contents of a message or file and produce a fixed-length *digest*. A message digest is used to confirm that a message or file has not been altered.

A typical use of a message digest is the posting of a hash of a downloadable software program. A user who downloads the program can perform a hash of the program to confirm that the program is genuine. This technique requires that the web site containing the stated hash value be well protected so that an intruder is not able to alter the program and the stated hash value.

The principles of message digests are:

- It should not be possible to re-create the original message from the digest.
- It should be impossible (well, computationally *infeasible*) to create messages that will result in a given message digest.
- No two messages should result in the same message digest.
- A message digest should be the result of the *entire* message, not a portion of it.

Message digest algorithms include:

- **MD5.** A fast and robust message digest algorithm that is widely used.
- **SHA-1 (Secure Hash Algorithm).** A robust message digest algorithm that has weakened somewhat. Developers considering using a hashing algorithm are advised to use MD5 instead.
- **HMAC (Hashed Message Authentication Code).** An algorithm that utilizes a digest together with a secret key.

A message digest does not authenticate (prove the origin of) the message or file. If a user needs to verity the authenticity and origin of a message or file, then **digital signatures** should be used instead of (or in addition to) hashing.

Digital Signatures

A **digital signature** is a method used to verify the authenticity and integrity of a message or document.

To create a digital signature, the creator or sender will "sign" a document using a program that employs a digital signature algorithm. The program will read the entire contents of the message or file, and combine it cryptographically with the private key of the person signing

the document. This creates the "digital signature," which is a string of characters that may either be embedded in the document or be stored separately.

When the recipient receives the document and the digital signature, the recipient can verify the integrity of the digital signature. This requires the sender's public encryption key. The recipient uses a digital signature verification program, which examines the original document and the digital signature, and cryptographically compares this to the originator's public encryption key. If the verification is confirmed, the recipient knows that a) the document was really signed by the originator, and b) the document has not been altered since it was signed. Thus, the recipient has confidence that the document is authentic.

Use of a digital signature alone provides document integrity and origination only; a digital signature does not provide any confidentiality by protecting the document against viewing by any third party. Encryption should be used if the parties wish to prevent any third party from viewing a document or message.

Some of the algorithms used for digital signatures are:

- Digital Signature Algorithm (DSA)
- El Gamal
- Elliptic Curve DSA (ECDSA)

Digital Certificates

A digital certificate is an electronic document that contains an individual's public encryption key together with identifying information such as the person's name and contact information. The digital certificate includes a digital signature of the public key and identifying information. Typically the certificate is signed by a trusted certificate authority (CA), which will provide a level of confidence in the identifying information in the certificate.

The most common form of a digital certificate is **X.509**, an ITU (International Telecommunication Union) standard. The structure of an X.509v3 digital certificate is:

- Version (usually a "3" for X.509v3)
- Serial Number
- Algorithm ID (the encryption algorithm used)
- Issuer (the organization that signed the certificate)
- Validity
  - Not Before (date)
  - Not After (date)
- Subject (identifying information about the certificate user)
- Subject Public Key Info
  - Public Key Algorithm (the algorithm used)
  - Subject Public Key (the actual public key)

- Issuer Unique Identifier (Optional)
- Subject Unique Identifier (Optional)
- Extensions (Optional)
- Certificate Signature Algorithm (the actual digital algorithm)
- Certificate Signature (the actual digital signature)

Non-Repudiation

The use of digital signatures and other factors such as strong authentication give rise to situations where it can become difficult for an individual to reasonably deny that he or she performed a transaction. This ability for a system to prove that an individual actually performed a transaction is known as **non-repudiation**. In other words, a user is unable to repudiate the performance of a transaction, because of the strength of the tools and algorithms used to perform or support the transaction.

Public Key Infrastructure (PKI)

A **public key infrastructure** (**PKI**) is an online facility where parties' public keys can be easily retrieved. For instance, an e-mail system can store the public encryption keys for a community of recipients on a central server, where e-mail programs can easily retrieve them, permitting encryption of messages for selected recipients.

A PKI can store other information in addition to public encryption keys, and serve multiple purposes in an identity management service. For instance, the PKI can also be used as an enterprise authentication server or **certificate authority** (**CA**). The LDAP (Lightweight Directory Access Protocol) standard is the most widely used directory standard and a popular platform for PKIs. Microsoft Active Directory is a popular commercial PKI platform.

Encryption Alternatives

There are other means available for protecting information, primarily watermarking and steganography.

Steganography

Steganography, which is also known as "stego," is the practice of hiding a message in another medium. For instance, a message can be hidden in an image file, where the inclusion of a message—interspersed throughout the image—is unlikely to be noticed by someone viewing the image. In steganography, a message can be hidden in an image, a sound file, a video clip, or other human-read medium where the inclusion of the message will produce slight variations that may not be noticeable. Messages can also be hidden in a file's slack space and other places where others may not look.

A classic example of text-based steganography is a written message that was sent to a condemned prisoner, a Sir John, a Royalist during a civil war in England. The message to the

prisoner appeared to be a rambling letter, but the third letter after each punctuation mark formed a secret message, which gave the prisoner a valuable clue that permitted him to escape through a hidden door in a prayer chapel that supposedly contained only one entrance and exit.

The message: *Worthy Sir John: Hope, alas, cannot, I fear, help you now. So bravely have you endured your fate, I regret there is nothing more to be done. I thought: friends would come to your rescue, find you in prison. And, what result? Only that you will soon, go to your untimely, deadly fate. Perhaps, in some better future, able, bright, undaunted men will meet, ever certain their cause was—just.*

The hidden message: *panel behind altar slides.*

In stego, a message may or may not be encrypted. If the method used to hide a message can be discovered, then the contents of the message will be compromised.

Watermarking

Often considered the visible form of steganography, **watermarking** is the practice of inserting a mark, image, or message onto a file as a means of claiming or asserting ownership of the file. Often this is done as a means for protecting intellectual property.

Examples of watermarking include:

- Asserting a claim of ownership on an audio or video medium such as a song or movie.
- Visibly marking a sample image that is for sale.
- An example of watermarking to protect an image from illegal copying is shown in Figure 5-10.

Figure 5-10 Example of watermarking

Course Technology/Cengage Learning

Chapter Summary

- Cryptography is the science of hiding information, usually through the use of algorithms-based upon mathematical operations.
- Encryption is the process of transforming original plaintext into unreadable ciphertext. Encryption typically involves the use of an encryption key, which is a block of text that is kept secret.
- The methods of encryption are substitution, transposition, monoalphabetic, polyalphabetic, running-key, and one time pads.
- The types of encryption are block ciphers and stream ciphers. Block ciphers are used to encrypt messages and files. Stream ciphers are used to encrypt continuous streams of data, such as video or audio.
- The modes of operation for a block cipher are electronic codebook (ECB), cipher-block chaining (CBC), cipher feedback (CFB), output feedback (OFB), and counter (CTR).
- An Initialization Vector (IV) is a randomly generated block of data that is required by several of the modes used by block ciphers.
- The two types of encryption keys are symmetric keys and asymmetric keys. Symmetric keys are also known as "shared secrets". Asymmetric keys cryptography is more commonly referred to as *public key cryptography*.
- The Diffie-Hellman key exchange protocol is a method that two parties can use to develop an encryption key over an unsecure channel.
- Cryptanalysis is the process of attacking a cryptosystem in order to discover its method of operation. Some of the well known methods used in cryptanalysis are frequency analysis, birthday attacks, ciphertext only attack, chosen plaintext attack, chosen ciphertext attack, known plaintext attack, man in the middle attack, and replay attack.
- Cryptography is often used to encrypt files, directories, disk volumes, e-mail messages, and communications between persons and network in contexts such as Web-based applications and remote access.
- Key management encompasses several procedures and safeguards used to create, manage, protect, use, and (eventually) destroy encryption keys.
- Hashing is the process of using a cryptographic algorithm to create a message digest of a file or message, used to ensure the integrity of a message.
- Non-repudiation is the concept of ensuring that a person cannot later deny having performed some action.
- A public-key infrastructure (PKI) is a network-based service used to store digital certificates or public encryption keys of individuals in a community.
- Steganography is used to hide information within some other media, such as an image, audio file, video stream, or slack space in a file.
- Watermarking is a visible form of steganography that is used to "label" a document, image, or data.

Key Terms

Advanced Encryption Standard (AES) the encryption standard established in 2001 by the U.S. government. AES uses the Rijndael algorithm.

Asymmetric cryptography a class of cryptographic algorithms that utilize public-private encryption keys.

Block cipher an encryption algorithm that operates on fixed blocks of data.

Birthday attack a cryptanalysis attack against a message digest.

Certificate Authority (CA) an entity that issues digital certificates.

Chosen Plaintext Attack (CPA) a cryptanalysis attack where the attacker is able to have chosen plaintexts encrypted and obtain the ciphertext results.

Chosen ciphertext attack (CCA) a cryptanalysis attack where the attacker has chosen ciphertexts decrypted and obtain cleartext results.

Cipher Feedback (CFB) a block cipher mode where the result of encrypting a block of plaintext is used to encrypt the next block.

Cipher-Block Chaining (CBC) a block cipher mode where ciphertext output from each encrypted plaintext block is used in the encryption of the next block.

Ciphertext the result of applying an encryption algorithm to plaintext.

Ciphertext-Only Attack (COA) a cryptanalysis attack where the attacker has only ciphertext.

Collision an occurrence where two different messages are found to compute to the same hash value.

Cookie a mechanism used to store identifying information, such as a session ID, on a web client system.

Counter (CTR) a block cipher mode that uses a one-time random number and a sequential counter.

Cryptanalysis the process of attacking a cryptosystem in order to discover its method of operation and/or its encryption and decryption keys.

Cryptography the science of hiding information, usually through the use of algorithms-based upon mathematical operations.

Decipher another word for decrypt.

Decryption the process of turning ciphertext back into original plaintext.

Diffie-Hellman (D-H) key exchange a secure mechanism for two parties with no prior knowledge of each other to jointly establish a shared symmetric encryption key.

Digital Encryption Algorithm (DEA) the data encryption algorithm chosen in 1976 as the new Digital Encryption Standard (DES).

Data Encryption Standard (DES) the data encryption standard established in 1976 by the U.S. government. DES uses the Digital Encryption Algorithm (DEA) algorithm.

Digital signature the result of cryptographic functions used to verify the integrity and authenticity of a message.

Electronic Codebook (ECB) a block cipher mode wherein each plaintext block is encrypted separately.

Encipher another word for *encrypt*.

Frequency analysis a cryptanalysis attack where the frequency of occurrence of the characters in ciphertext are examined.

FTP (File Transfer Protocol) a protocol used to transfer files from one system to another.

GPG (Gnu Privacy Guard) an open source software program that implements the PGP (Pretty Good Privacy) encryption standard.

HMAC (Hashed Message Authentication Code) a message digest (hashing) algorithm.

Initialization vector (IV) a random block of data that is used by some cryptographic functions.

IPSec a tunneling protocol used to protect communications between two systems.

Key a block of information that is used in an encryption algorithm.

Key management processes and procedures used to create, protect, and destroy encryption keys.

Known Plaintext Attack (KPA) a cryptanalysis attack where the attacker has samples of plaintext and corresponding ciphertext messages.

Man In The Middle attack (MITM) a cryptanalysis attack in which the attacker is able to read, insert, and modify messages passing between two parties' without their knowledge.

MD5 a message digest (hashing) algorithm.

Message digest a fixed length block of data that is the result of a hash function. See also *hash*.

MIME Object Security Services (MOSS) a protocol that provides confidentiality, authentication, and non-repudiation.

Monoalphabetic cipher a cipher in which plaintext characters are substituted for ciphertext characters according to a single alphabetic table.

Non-repudiation the concept of ensuring that a person cannot later deny having performed some action.

One-time pad an encryption algorithm where the key is the same size as the message and is used only once.

One-way hash See *message digest*.

Output Feedback (OFB) a block cipher mode where the results of the previous plaintext block are used in the encryption of the next block.

Permutation cipher See *transposition cipher*.

Plaintext data that is not encrypted.

Polyalphabetic cipher a cipher in which plaintext characters are substituted for ciphertext characters according to a multiple alphabet table.

Pretty Good Privacy (PGP) a popular computer program, as well as a published standard for encryption, that is used to encrypt and decrypt data.

Privacy Enhanced Mail (PEM) a standard for encrypting e-mail that depends upon a global PKI.

Private key an encryption key used in public key cryptography that is kept private by its owner.

Public key an encryption key used in public key cryptography that can be widely distributed to users.

Public key cryptography a class of cryptographic algorithms that utilize public-private encryption keys.

Public Key Infrastructure (PKI) a network-based service in which public encryption keys or certificates are stored and available for retrieval.

RC4 a common stream cipher.

Replay attack a cryptanalysis attack where the attacker records transmissions and replays them at a later time, usually to masquerade as one of the parties whose transmissions were recorded.

Rijndael the data encryption algorithm chosen in 2001 as the new Advanced Encryption Standard.

rsh (remote shell) an unsecure protocol used to establish a command line session on another system over a network.

Running key cipher a cryptography technique used when plaintext is longer than the key.

Secure Electronic Transaction (SET) a protocol used to protect electronic transactions. SET is not widely used, and has been replaced by SSL and TLS.

Secure/Multipurpose Internet Mail Extensions (S/MIME) a protocol used for protecting e-mail message through encryption and digital signatures.

Secure Shell (SSH) a TCP/IP layer 5 tunneling protocol used for secure remote management of systems. Supersedes Rsh, Rcp, Rlogin, and Telnet.

Secure Sockets Layer (SSL) a TCP/IP layer 5 tunneling protocol used to protect network traffic through encryption. Superseded by TLS. See also *TLS*.

SHA-1 (Secure Hash Algorithm) a message digest (hashing) algorithm.

S-HTTP (Secure Hypertext Transfer Protocol) a connectionless protocol used to encrypt and authenticate data being sent from a server to a client.

Steganography the practice of hiding a message in another medium, such as an image or sound file.

Stream cipher an encryption algorithm that operates on a continuous stream of data, such as a video or audio feed.

Substitution cipher an encryption algorithm where characters are substituted for others.

Symmetric cryptography a method of cryptography where each party is in possession of an encryption key.

TELNET a TCP/IP layer 5 protocol that is used to establish a raw TCP session over a network to a service on another computer.

Transport Layer Security (TLS) a TCP/IP layer 5 tunneling protocol that protects network traffic through encryption. TLS supersedes SSL.

Transposition cipher an encryption method where characters in plaintext are rearranged to form ciphertext.

Vernam cipher See *one-time pad*.

Virtual Private Network (VPN) an encrypted communications channel that is used for secure remote access or for protecting the traffic between two networks.

Watermarking the process of placing in image or mark in a file for identification purposes.

Wired Equivalent Privacy (WEP) a standard for encrypting packets on a Wi-Fi wireless network. Superseded by WPA and WPA2.

X.509 the prevailing digital certificate standard. See also *digital certificate*.

XOR a logical operation on two operands, where the return value is TRUE only if one of the two operands (but not both) is TRUE.

Review Questions

1. A secret message has been encrypted with a key that is as long as the message itself. The key will be used for only this message. The type of encryption used here is:
   a. Running key cipher
   b. Substitution cipher
   c. One-time pad
   d. Diffie-Hellman
2. The weakness of a monoalphabetic cipher is:
   a. It is vulnerable to frequency analysis
   b. It requires excessive computing resources
   c. The key is embedded in the ciphertext
   d. The key is too short
3. DES, AES, and CAST are examples of:
   a. SSL encryption algorithms
   b. Public key cryptography algorithms
   c. Stream cipher algorithms
   d. Block cipher algorithms
4. Advanced Encryption Standard uses the:
   a. Twofish cipher
   b. Reykjavík cipher

c. Rijndael cipher
d. 3DES cipher

5. The disadvantage of Electronic Codebook is:
   a. It is a manual encryption algorithm not suited for use in computers
   b. It is a patented encryption algorithm
   c. Each identical plaintext block encrypts into an identical ciphertext block
   d. It uses a 56-bit encryption key that is considered too short
6. RC4 is an example of a:
   a. Message digest
   b. Stream cipher
   c. Block cipher
   d. Key exchange
7. SHA-1 is an example of a:
   a. Message digest
   b. Stream cipher
   c. Block cipher
   d. Key exchange
8. Public key cryptography is so-named because:
   a. It is highly popular
   b. Its use is not restricted by patents
   c. It utilizes an open source encryption algorithm
   d. The key that is used to encrypt a message does not need to be kept a secret, but can be made public
9. Two parties wish to exchange encrypted messages using symmetric key cryptography. The parties do not have an out-of-band method for exchanging keys. The parties should use:
   a. A stream cipher
   b. Message digests
   c. Public key cryptography
   d. Diffie-Hellman key exchange
10. Frequency analysis refers to:
   a. Analyzing the rate of occurrence of characters in ciphertext
   b. Eavesdropping on spread-spectrum radio frequency transmission in order to harvest encryption keys
   c. Analyzing the rate of occurrence of characters in plaintext
   d. Analysis of emanations in order to harvest encryption keys

11. An attacker is trying to crack an encryption scheme in order to discover secret information. The attacker is able to get his own plaintext messages encrypted by the same mechanism used to protect the secret information he is trying to obtain. This method of attack is known as:
    a. Chosen plaintext attack
    b. Chosen ciphertext attack
    c. Cryptanalysis
    d. Man in the middle

12. An attacker is trying to discover the contents of encrypted messages that he can easily intercept. The attacker attempts to break messages by intercepting and substituting his own messages in a communications stream between two parties. This type of attack is known as:
    a. Unknown plaintext
    b. Known ciphertext
    c. Man in the middle
    d. Replay
13. An administrator wants to have all traffic between two servers encrypted. The administrator should use:
    a. SSH
    b. IPSec in transport mode
    c. IPSec in tunnel mode
    d. SSL
14. Cookies are suited for session management:
    a. When the session or user ID is encrypted
    b. If the session is encrypted with SSL/TLS
    c. Only as a last resort
    d. Only on a protected LAN or VPN
15. VPNs can be used to protect network traffic:
    a. Between any nodes on two different networks
    b. Between a station and any node on a network
    c. Between two stations
    d. All of the above

Hands-On Projects

Project 5-1: EFS Encryption on a Multi-User Workstation

In this project you will encrypt files and directories using Microsoft Windows EFS (Encrypting File System).

Required for this project:

- Windows XP Pro or Windows Vista.
- Administrative access to the Windows operating system.
- Ability to create other user accounts.

1. Create some text files in a directory. Encrypt these files using EFS through one of the following methods:

- In Windows Explorer, right-click the file and select **Encrypt**.
- In Windows Explorer, right-click the file and select **Properties**. Then select **Advanced**, and then select **Encrypt contents to secure data**. Click **OK**.

2. The file(s) you encrypted should be shown in green text instead of black text, signifying that the files are encrypted.
3. If needed, Share the file(s) (or their parent directory) so that they may be viewed by other users.
4. Log out of Windows and log in as another user.
5. Using Windows Explorer, navigate to the directory containing the file(s) encrypted in step 1.
6. Attempt to read the text file(s) that were encrypted in Step 1. What happens, and why?

Project 5-2: Encrypt Data with WinZip

In this project you will create archives containing encrypted files and make some observations about the archives.

Required for this project:

- Windows 2000, XP, or Vista.
- Administrative access to the Windows operating system for purposes of installing software.

1. Obtain a copy of WinZip software, version 9 or newer.
2. Create a new directory on the desktop or another location.
3. Create some text files in the directory created in step 2.
4. Create a new ordinary Zip archive and place the files created in step 3 into the archive.

5. Create a second Zip archive. When placing files into the archive, choose AES encryption. You will be asked to supply a password. See Figure 5-11.

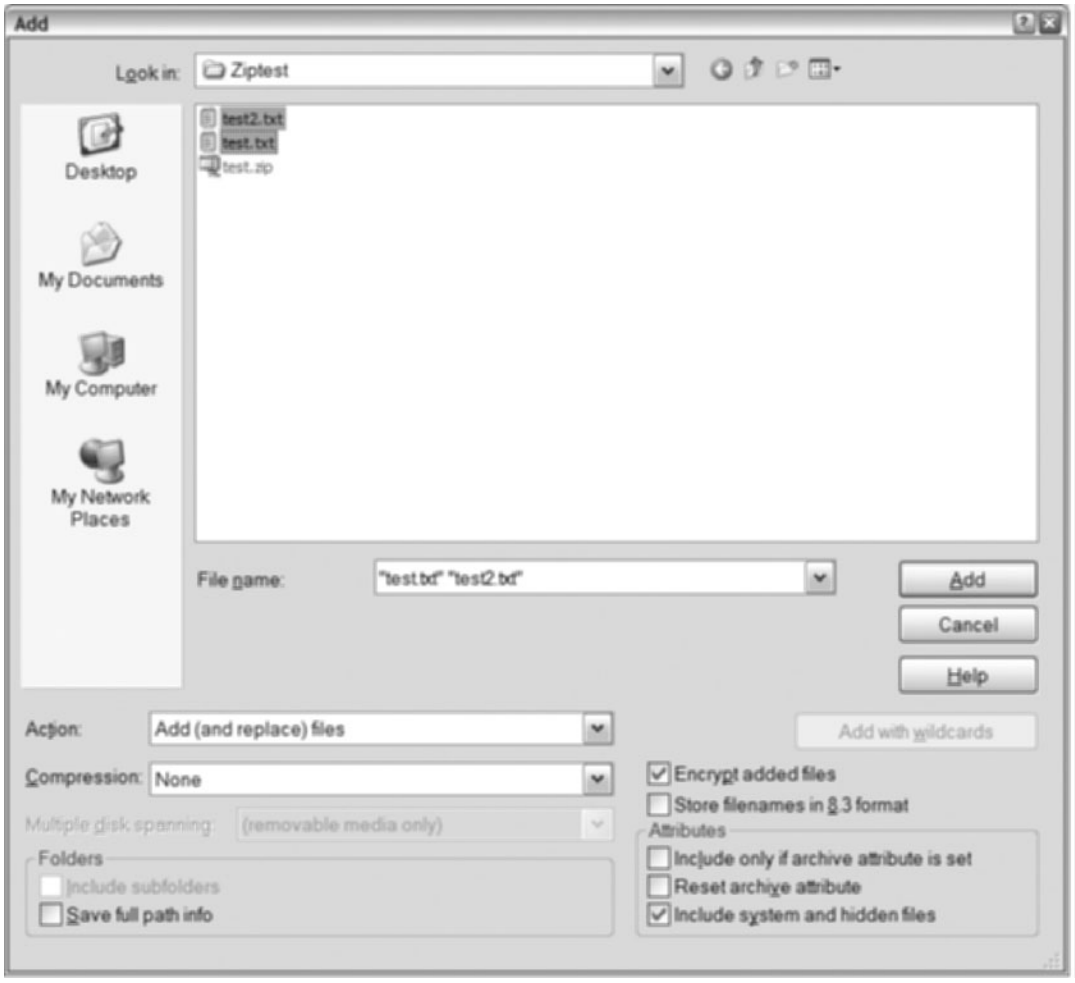


Figure 5-11 Creating a WinZip archive using AES encryption

Source: Course Technology/Cengage Learning

6. Place one or more additional files into the Zip archive, this time using a different password.
7. Close the Zip archives.
8. Open the Zip archive created in step 5. What do you observe?
9. Attempt to extract files from the Zip archive. What do you observe?
10. Open the Zip archive created in step 5 (See figure 5-12). with Notepad or other program that shows plain text. What do you observe?

Figure 5-12 A WinZip archive contains files encrypted with AES

Source: Course Technology/Cengage Learning

Project 5-3: Create an Encrypted Disk Volume

In this project you will create an encrypted disk volume that can be used to store directories and files.

Required for this project:

- Windows 2000, XP, or Vista; OpenSuSE or Ubuntu Linux
- Administrative access to the Windows operating system for purposes of installing software

1. Obtain a copy of TrueCrypt. You can obtain it from http://www.truecrypt.org/
2. Install TrueCrypt on your system.
3. Create a small encrypted volume. See Figure 5-13.

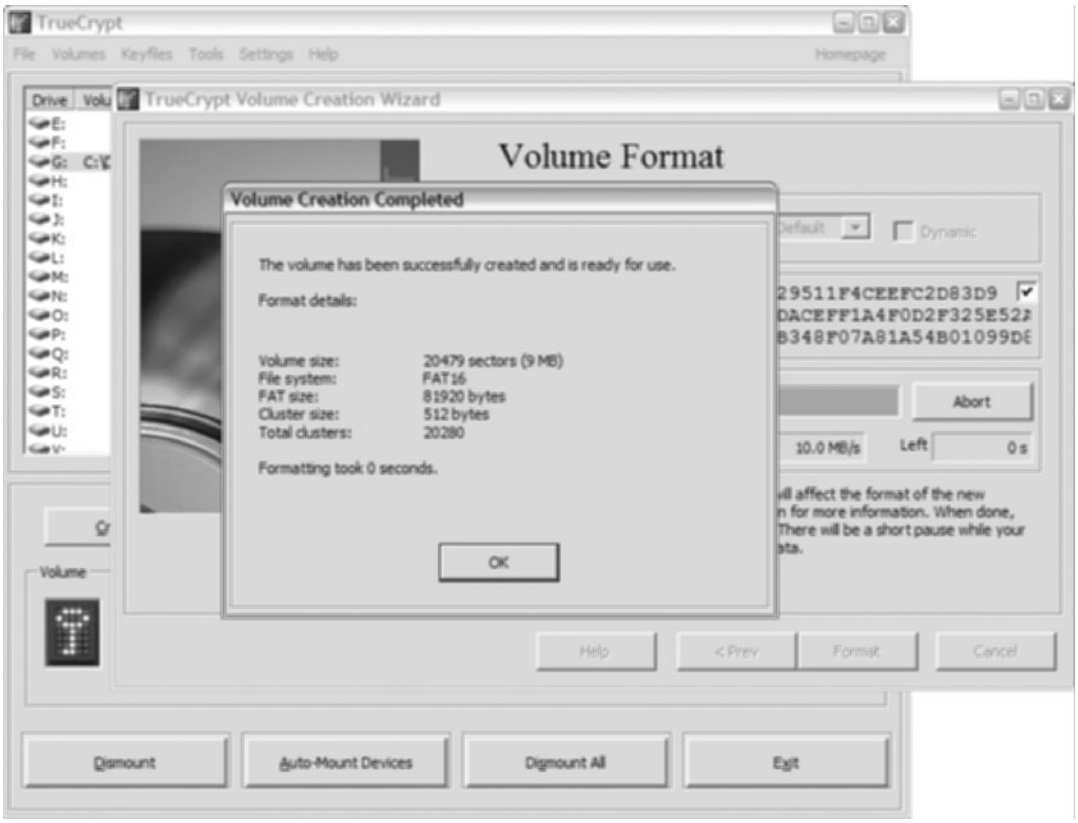


Figure 5-13 Creating a logical disk volume with TrueCrypt

Source: Course Technology/Cengage Learning

4. Mount the encrypted volume
5. Create some files and directories in the volume. What are your observations?
6. If your volume is small enough, give it to another person who has TrueCrypt and ask them to try and mount it (do not give them your password). What are your observations?

Project 5-4: Encrypt e-mail Messages

In this project you will send and receive encrypted e-mail messages.

Required for this project:

- Windows 2000, XP, or Vista
- Administrative access to the Windows operating system for purposes of installing software

1. Obtain a copy of GnuPG (GPG), the freeware version of PGP. You can obtain it from http://www.gnupg.org/

2. Install GnuPG on your system. Find another person who will do the same on their system, so that you can exchange messages.
3. Create a private-public key pair, per the instructions. See Figure 5-14.

Figure 5-14 Creating a public-private keypair using GnuPG

Source: Course Technology/Cengage Learning

4. Send your public key to another person. Have the other person send their public key to you
5. Import the other person's public key using the **Keys>Import** command. See Figure 5-15.

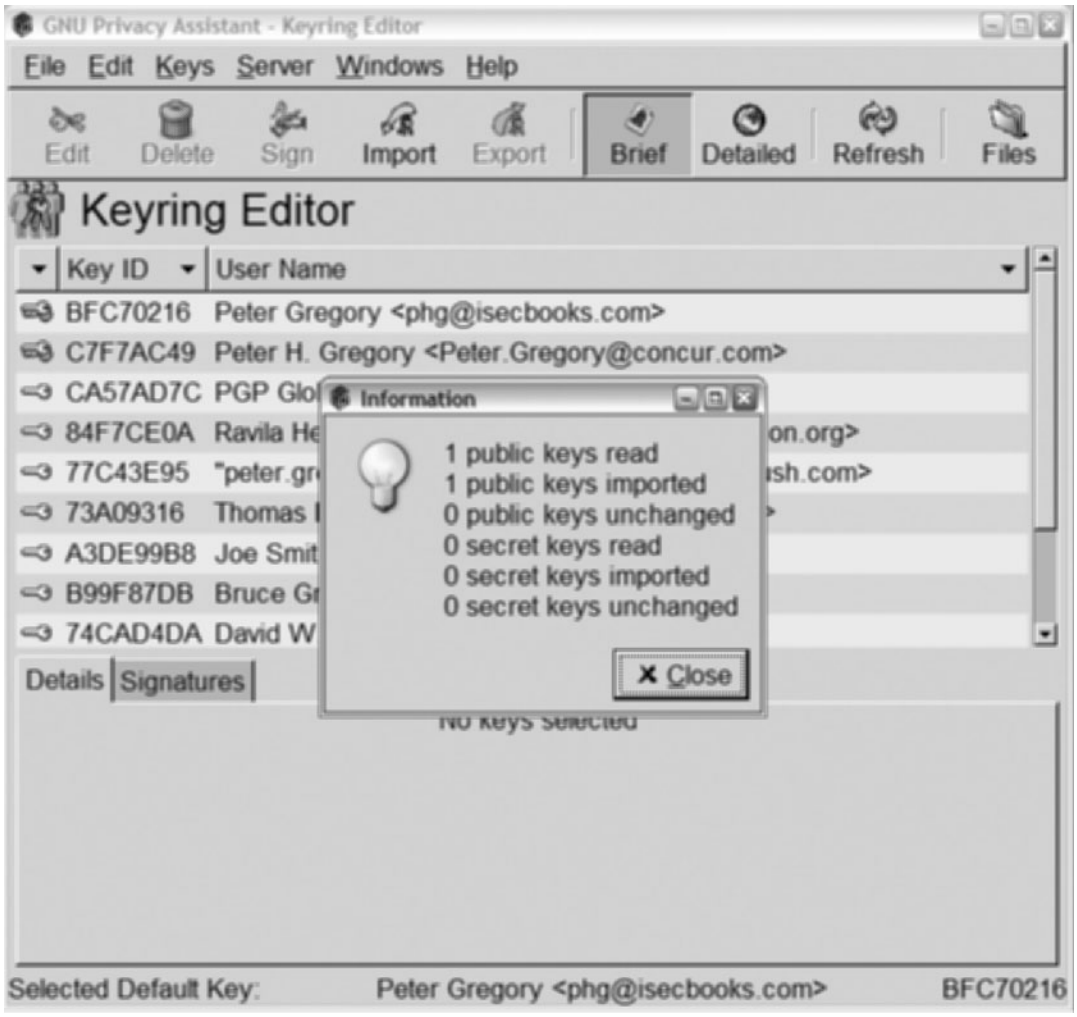


Figure 5-15 Importing a public key using GnuPG

Source: Course Technology/Cengage Learning

6. Using your local e-mail program (Outlook, etc.) create an encrypted e-mail message. Alternately, encrypt a file using the other party's public key. Have the other person encrypt a file or message with your public key. Send the encrypted files/messages to each other
7. Open the message/file sent from the other person. What are your observations?
8. If available, have a third person encrypt a file with their public key and send to you. Try to open the file. What are your observations?

Project 5-5: Steganography

In this project you will use steganography to hide messages in image files.

Required for this project:

- Windows 2000, XP, or Vista

1. Obtain a copy of Gifshuffle, a command line steganography tool. You can obtain it from http://www.darkside.com.au/gifshuffle/
2. Create a new directory and unzip the Gifshuffle archive into the directory
3. Copy one or more GIF files into the directory
4. Insert a hidden message into the GIF file. For example, if are going to place a message into the GIF file *in.gif*, creating the new GIF file *out.gif*:

```
C:\tem> gifshuf -m "now is the time for all good men to
come to the aid of their country" in.gif out.gif
C:\tem>
```

5. View the "before" and "after" versions of the GIF file. Can you discern any differences in the appearance of the file?
6. Extract the hidden message from the GIF file. Continuing the example from step 4:

```
C:\tem> gifshuf out.gif
now is the time for all good men to come to the aid of
their country
C:\tem>
```

Case Projects

Case Project 5-1: Establish Secured-Mail Communications

As a consultant with the Ace Security Consulting Co., you have been asked to design and implement secure e-mail for two hundred users at the Big City Insurance Company. Users at Big City use a Linux-based POP and SMTP-based e-mail server, and users use Mozilla Thunderbird, Microsoft Outlook, or Microsoft Outlook Express.

Among the solutions you can choose:

- GnuPG
- S/MIME with digital certificates obtained from Thawte (www.thawte.com)
- PGP

Which of these solutions do you expect will be the easiest to implement? Which do you think will be the easiest to maintain? Which will result in the fewest support calls from users? What other factors will influence your decision?

Case Project 5-2: Make Encrypted Files Available to Employees in a Large Organization

As a consultant with the Ace Security Consulting Co., you have been asked to determine how encrypted documents containing sensitive information can be made available to several hundred office workers in the Very Good Software Company.

The encrypted files can be downloaded from an internal web site at Very Good Software.

What considerations and methods can be used to ensure easy downloading and reading of the encrypted documents while minimizing the risk of compromise?

Case Project 5-3: Implement TrueCrypt Disk Encryption on User Workstations

As a consultant with the Ace Security Consulting Co., you have been asked to develop a plan to implement disk encryption using TrueCrypt on about fifty users' laptop workstations. You should assume the following:

- PC technicians will install and configure the software
- Users are not technical

The primary business objectives supporting the use of TrueCrypt are:

- Protection of business information in the event a laptop computer is lost or stolen
- Low cost

Develop a plan for implementing TrueCrypt on the user workstations. What issues do you anticipate during and after implementation? What can be done to manage these issues?

This page intentionally left blank

chapter 6

Legal, Regulations, Compliance, and Investigations

Topics in this Chapter:

- Computer Related Crime
- Categories of Law and Computer Crime Laws in the U.S. and Other Countries
- Security Incident Response
- Investigations
- Computer Forensics
- Ethical Issues

The (ISC)^2 *Common Body of Knowledge* (CBK) defines the key areas of knowledge for Legal, Regulations, Compliance, and Investigations in this way:

The Legal, Regulations, Compliance, and Investigations domain addresses computer crime laws and regulations; the investigative measures and techniques which can be used to determine if a crime has been committed, methods to gather evidence if it has, as well as the ethical issues and code of conduct for the security professional.

Incident handling provides the ability to react quickly and efficiently to malicious technical threats or incidents.

The candidate will be expected to know the methods for determining whether a computer crime has been committed; the laws that would be applicable for the crime; laws prohibiting specific types of computer crime; methods to gather and preserve evidence of a computer crime, investigative methods and techniques; and ways in which RFC 1087 and the (ISC)^2 Code of Ethics can be applied to resolve ethical dilemmas.

Key areas of knowledge:

- *Understand common elements of international laws that pertain to information systems security*
- *Understand and support investigations*
- *Understand forensic procedures*

Computers and Crime

Computers are increasingly involved in criminal activities of nearly every kind. This section explores the roles of computers in crimes, and the types of computer crimes.

The Role of Computers in Crime

Because individuals use computers to communicate, maintain records, and conduct business, quite often a computer is involved in the crime, whether it is the target of the crime, an instrument (or weapon) used to commit a crime, or it contains evidence related to the crime.

There are three ways in which computers are associated with crimes:

- **Target**. A computer or other system is the target of a crime. The following activities are examples of crimes where a computer—or the data stored in a computer—are the target of a crime:
  - **Equipment theft**. Computer or network hardware is stolen.
  - **Equipment vandalism**. Computer or other hardware is damaged or defaced.
  - **Data theft**. Data stored on a computer is stolen.
  - **Data vandalism**. Data (which can include software) stored on a computer is changed, damaged, or destroyed.
  - **Trespass**. A party logically enters a computer or other system without authorization.

- **Instrument**. A computer is used to commit a crime. Examples of computer-aided crimes include:
  - **Data theft and vandalism**. A criminal uses a computer as a tool to access another party's computer in order to change, damage, or destroy data stored there.
  - **Trespass**. A criminal uses a computer to trespass onto a computer or other type of system owned by another party.
  - **Harassment**. A criminal uses a computer to intentionally harass another person.
  - **Spam**. A criminal uses a computer to create, control, and/or monitor spam (unsolicited commercial e-mail).
  - **Child pornography**. A criminal may use a computer to create, distribute, control, or monitor child pornography or other illegal content.
  - **Libel and slander**. An individual uses a computer to libel or slander another individual.
  - **Fraud**. A criminal uses a computer as a tool to defraud another party.
  - **Eavesdrop**. A criminal may use a computer as a means to eavesdrop on communications between other parties.
  - **Espionage**. A criminal may use a computer as a means to commit **espionage**—obtaining secrets from an organization or government without its permission.
- **Support**. A computer is used in support of criminal activities. Examples of computers in support of crimes include:
  - **Recordkeeping**. A criminal may use a computer to track or support criminal activities.
  - **Conspiracy**. Two or more individuals may conspire to commit a crime, using computers as the means to communicate and plan the crime.
  - **Aid and abet**. A party may aid and abet criminals through the use of a computer, for instance, by providing information via e-mail or sending funds via e-mail or an online service.

The three major categories above are not exclusive. Often a computer-related crime will involve more than just one of the major categories above. For instance, computer trespass involves the use of a computer used as an instrument to trespass onto a victim's computer.

The increase in the involvement of computers in criminal activities has put a strain on law enforcement agencies and the private sector: an acute shortage of people with computer **forensics** skills has resulted in a large body of computer-related evidence being collected improperly or ignored altogether.

The Trend of Increased Threats in Computer Crimes

Computer crime has moved steadily from the realm of the lone hacker and **script kiddie** to sophisticated and resourceful organizations sponsored by nation-states. At the same time, the skills required to launch a devastating wide-scale attack has steadily decreased. Indeed, an entirely new economic ecosystem has been developed: **botnets** are available for rent by the hour, and increasingly sophisticated phishing sites that can evade capture are developed

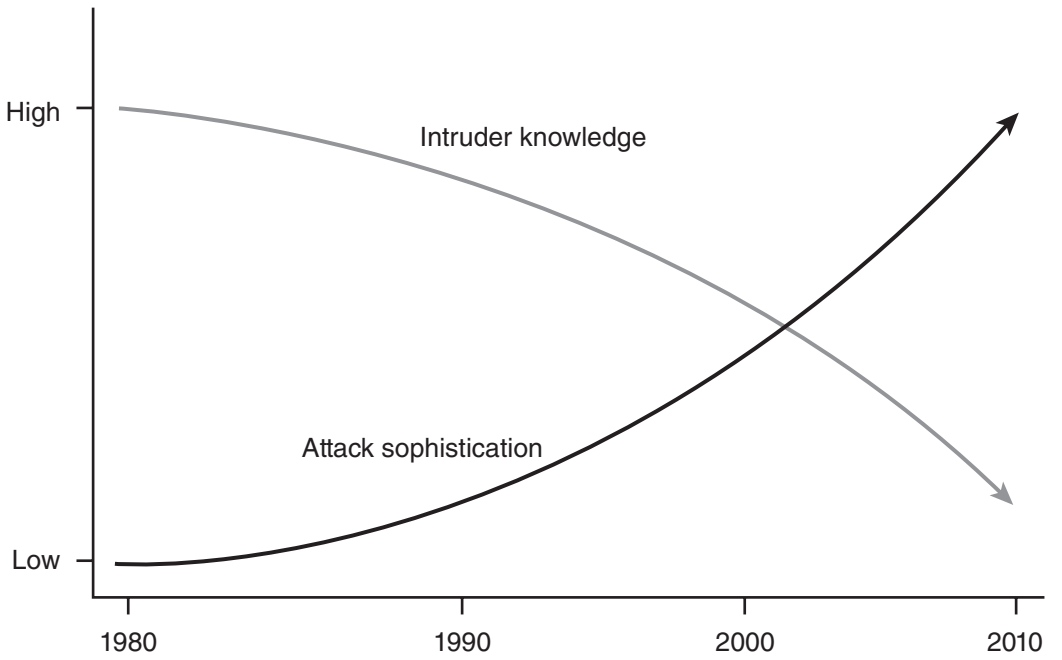


Figure 6-1 Increasingly sophisticated attacks require less knowledge

Source: Course Technology/Cengage Learning

with turn-key development kits. Organized crime is making more money from cyber-related criminal activities than from the illegal drug trade (and that is not because of any decrease in the use of illegal drugs!). Figure 6-1 shows the inverse relationship between the knowledge required to launch attacks of growing sophistication.

Categories of Computer Crimes

There are several reasons why an individual or group will perpetrate a crime against a computer system. The major categories of computer related crimes are:

- Military and intelligence
- Financial
- Business
- Grudge
- "Fun"
- Terrorist

Military and Intelligence **Military attacks** are carried out against military organizations and governments for the purpose of discovering military or government secrets. These attacks can also be carried out against private companies, especially those that perform services for the military and for governments.

These attacks may be carried out by the military or by governments, terrorist organizations, volunteer "militia" groups, and other independents who feel compelled to take up international politics and warfare on their own.

Financial **Financial attacks** are directed at computers and applications that will yield profits in one of the following ways:

- **Direct access to funds**. Direct attacks on financial services organizations can be used in an attempt to transfer funds to locations accessible by the attacker. One of the most famous such attacks is the 1994 attack by Russian hacker Vladimir Levin, who reportedly accessed Citibank's cash management system using stolen credentials (and possibly insider help) to distribute over US$10 million to himself and his accomplices.
- **Access to credit card and bank account information**. Attacks can target databases containing transactions or account numbers that can later be used in attempts to withdraw or transfer funds.
- **Embezzlement**. Insiders can conduct attacks on their own organizations' computers in order to embezzle funds for personal gain.
- **Extortion/Blackmail**. Attackers can cripple an organization's activities in a variety of ways, with demands for payments in order to stop the attack.
- **Identity information**. Attacks can be used to steal private information on private citizens with the intent to conduct **identity theft**, a crime that involves the illegal use of another person's identity.

Business **Business attacks** are attacks that target computer systems owned by private organizations. Attacks on businesses are carried out for a variety of reasons, including:

- **Competitive intelligence**. Individuals want to discover secrets about an organization's products, services, financials, or other business secrets.
- **Financial gain**. See the earlier section on Financial Attacks.
- **Denial of Service**. Individuals may wish to harm or disable an organization's computer-based operations.

Businesses are often attractive targets for computer-based attacks for several reasons, including:

- Businesses will often not report the attack to law enforcement in order to avoid embarrassing, potentially damaging news reports.
- Businesses often lack the required expertise to carry out forensic investigations that can be used to collect damages from the attacker.
- Businesses often lack the required resources to properly address the incident.

In many jurisdictions, businesses are not required by law to report computer-related crimes; instead, businesses can often choose to keep the crime a private matter. Businesses are finding this more difficult, however, as many jurisdictions have passed laws that require the disclosure of security breaches involving the loss or exposure of citizens' personal information. This is discussed later in this chapter.

Grudge A **grudge attack** is motivated by feelings of anger or hostility towards an organization. The attacker may be a customer or patron of the organization, or, worse yet, may be a former employee who may possess much "insider" information that potentially makes such an attack easier to carry out.

Often, a grudge attack is easier to prosecute because in many cases the attacker is known to the organization (a former employee, contractor, or customer). Also, the pattern of the attack will

leave valuable clues that reveal what the attacker knew. For instance, if an attacker exploits a vulnerability in a system or application, then the attacker may be someone who used to work with that application or system and learned about the vulnerability while still an employee.

"Fun" **Fun attacks** are carried out by thrill seekers and those who attack computers for entertainment. Often these attacks are performed by "script kiddies," persons of little skill who are able to obtain easy-to-use attack tools developed by others.

Fun attacks often end in disaster, as attackers are compelled to tell their friends and associates about their latest conquests. Sooner or later an attacker's loyalty will be swayed by a financial reward or knowledge that it is the "right thing" to turn in the attacker so that he or she will face justice.

Terrorist These attacks are perpetrated by terrorist organizations that are typically motivated by the desire to harm other countries' governments or citizens. Known as **cyberterrorism**, these attacks are directed at a wide variety of targets including:

- Government systems
- Military systems
- Public utilities
- Public health organizations
- Communications and media organizations
- Transportation systems
- Financial services organizations

The U.S. National Conference of State Legislatures (NCSL) defines **cyberterrorism** as: "*the use of information technology by terrorist groups and individuals to further their agenda. This can include use of information technology to organize and execute attacks against networks, computer systems and telecommunications infrastructures, or for exchanging information or making threats electronically. Examples are hacking into computer systems, introducing viruses to vulnerable networks, web site defacing, denial-of-service attacks, or terroristic threats made via electronic communication.*"

(http://www.ncsl.org/programs/lis/CIP/cyberterrorism.htm)

The U.S. Federal Bureau of Investigation (FBI) defines **cyberterrorism** as any "*premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents.*" (U.S. Department of Justice, *Terrorism in the United States*, Washington, DC: Federal Bureau of Investigation, 1998.)

Terrorist attacks and cyberterrorism is also known by the term **information warfare.**

Computer Crime Laws and Regulations

Criminal activities and enterprises seem to move into every new domain, institution, nook, and cranny that is developed. Like many technologies and inventions, computers and the Internet were invented for the benefit of business and society but have also become the

means to commit crimes against others. As the rate and style of criminal activities increased, it soon became apparent that the set of laws and regulations in place were insufficient to address the often-abstract concepts of theft, vandalism, or trespass when they occur within computers and networks. In response, most countries have added new laws and regulations to specifically address crimes that involve the use of computers in one way or another.

Categories of U.S. Laws

The U.S. legal system consists of three categories of laws that cover all of the different types of circumstances that can bring parties to the courtroom to air their grievances. They are:

- **Criminal law**. This includes laws of public order against persons such as assault, arson, theft, burglary, deception, obstruction of justice, bribery, and perjury. Law enforcement agencies are responsible for enforcing criminal laws. Criminal laws in the United States are published in the **United States Code** (**U.S.C.**).
- **Civil law**. This includes contract law, tort law, property law, employment law, and corporate law. Civil law is the branch of laws that generally involve two parties that have a grievance that needs to be settled. Law enforcement agencies generally have little to do with civil laws. Civil laws in the United States are published in the United States Code (U.S.C.).
- **Administrative law**. These laws form the framework for the operation of U.S. government agencies such as the Federal Trade Commission, the Department of Agriculture, and the Federal Communications Commission. Administrative law in the United States in the **U.S. Code of Federal Regulations**, commonly known as the **C.F.R**.

U.S. Laws

There are several categories of laws that protect networks, computers, and information stored on computers. These categories protect different types of activities and information used by individuals and businesses. They are:

- Intellectual property law
- Privacy law
- Computer crime law

U.S. Intellectual Property Law

Intellectual property is the product of creation such as information, architecture, inventions, music, images, and design. **Intellectual property laws** in the United States protect the results of creative endeavors by individuals and organizations. The categories of intellectual property protected by these laws are:

- **Copyrights**. Copyrights, symbolized by "©," represent the creator's claim of exclusive rights on a wide variety of works including literary works, movies, dances, musical compositions, audio recordings, paintings and drawings, sculptures, photographs, radio and television broadcasts, software, and industrial designs.
- **Trademarks**. Trademarks, symbolized by "®," "TM," and "SM," represent a creator's claim on names, slogans, and logos that represent the creator's product or service. The creator of a product or service name, slogan, or logo must register it with the U.S. Patent and Trademark Office (USPTO). The creator of a work can affix a "TM" or "SM" on a product or service name, respectively, immediately upon first use. When the creator files and receives the trademark from the USPTO, the creator can affix the "®" mark on it.

- **Patents**. The intellectual property rights of inventors are protected by patents. **Patents** protect the designs of machinery, processes, and software. A patent protects a design or process from being copied by another person or company, but the main disadvantage of a patent is that the product or process is made public and is no longer secret.
- **Trade secrets**. Organizations can choose to not register their secrets as trademarks or patents, but instead decide to keep their secrets closely guarded.

Noteworthy laws in the United States that protect intellectual property laws include:

- **Economic Espionage Act of 1996**. This law makes it a crime to steal trade secrets for commercial or economic purposes, or for the benefit of a foreign power.
- **Digital Millennium Copyright Act (DMCA) of 1998**. DMCA is a copyright law that criminalizes any means that can be used to circumvent copy protection and other access controls for copyrighted works. DMCA also criminalizes the circumvention of an access control, even when there is no infringement of copyright itself. DMCA also defines and increases penalties for copyright infringement on the Internet.
- **No Electronic Theft (NET) Act**. This law defines criminal penalties when copyright violations are committed through the use of computers and networks.

U.S. Privacy Law Privacy has become a "lightning rod" issue in the United States and elsewhere in recent years. Personal information about virtually every citizen in industrialized countries is circulating among government and corporate information systems, most of it beyond the knowledge and control of most citizens. If this weren't alarming enough, news of security breaches numbering in the tens or hundreds of thousands surface every week. Stolen laptops, lost backup tapes, and hacking attacks are the majority of security breaches.

There is an added dimension to privacy that concerns many citizens: the misuse of sensitive or private information that further erodes citizens' civil rights and freedoms. For example, citizens fear that employers will discriminate against workers with health problems, now that a vast amount of health-related information is present on a relatively small number of health insurance company systems. In the absence of legal barriers, some corporations would consider screening employees based on health history if they were permitted to. In the United States this would be a flagrant violation of the right to privacy.

Several laws address privacy rights, including:

- **Fourth Amendment**. The basis for privacy rights in the United States, the fourth amendment to the Constitution states, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." In other words, law enforcement may only search the private residence of an individual when there is probable cause that a crime has occurred and when a search warrant has been signed by a judge. The fourth amendment has been extended into cyberspace in case law through specific laws, including some listed in this section.
- **Privacy Act of 1974**. Following privacy abuses perpetrated by the Nixon administration, this law forbids U.S. federal agencies from sending private information on citizens to other persons or agencies without those citizens' request or consent.

- **Electronic Communications Act of 1986.** This law provides protections for stored electronic communications.
- **Electronic Communications Privacy Act (ECPA) of 1986.** This law extended restrictions on telephone wiretaps to also include similar restrictions on wiretaps of electronic communications among computers. Requirements for obtaining warrants for wiretaps of electronic communications are defined in this law.
- **Computer Matching and Privacy Protection Act of 1988.** An amendment of the Privacy Act of 1974, this law put restrictions on the 1980s practice of computer matching of citizens' private information.
- **Communications Assistance for Law Enforcement Act (CALEA) of 1994.** This law requires telecommunications carriers to cooperate with law enforcement agencies' requests for wiretaps of subscribers' telephones. The law also requires the manufacturers of telecommunications equipment to provide the means for legal wiretaps. Wiretaps require a signed warrant.
- **Economic and Protection of Proprietary Information Act of 1996.** Addressing espionage, this law defines information and trade secrets as property, making theft of trade secrets and information a crime.
- **Health Insurance Portability and Accountability Act (HIPAA) of 1996.** This comprehensive law requires greater uniformity in health information data, which allows it to be more easily transmitted between health-related organizations (such as health care providers and insurance companies for claims purposes), but also protects health information from unauthorized disclosure. HIPAA's "Security Rule" imposes many requirements on the security of Electronic Patient Health Information (EPHI).
- **Children's Online Privacy Protection Act (COPPA) of 1998.** This law restricts online services' ability to collect information from children under the age of 13.
- **Identity Theft and Assumption Deterrence Act of 1998.** This law strengthened the law regarding fraud and related activity in connection with identification documents, authentication features, and information.
- **Gramm-Leach-Bliley Act (GLBA) of 1999.** The Financial Privacy Rule and the Safeguards Rule require financial services organizations to disclose privacy policies to customers and to provide adequate safeguards to protect customers' private information.
- **Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001.** The Patriot Act, as it is commonly known, expanded the authority of U.S. law enforcement agencies for the intention of fighting terrorism in the United States and abroad. The Patriot Act gave law enforcement agencies greater ability to search telephone and e-mail communications and medical, financial, and other records.

U.S. Computer Crime Law Several laws have been passed in the United States that further define lawful and unlawful acts. With the widespread use of computers by government and private organizations, protection of computers and the information stored on

them was ambiguous at times, and activities that were pretty clearly criminal in nature were sometimes difficult to prosecute. Notable U.S. cybercrime laws include:

- **Access Device Fraud, 1984**. This law codifies criminal activities related to the fraudulent use of "access devices," which generally is associated with the fraudulent use of credit and debit cards, ATMs, computer passwords and PINs, and cellular phones.
- **Computer Fraud and Abuse Act of 1984**. This law was the first to define "computer trespass" by making it illegal to knowingly access a computer without authorization for purposes of obtaining national secrets or information with an intent to defraud. This was the first real anti-hacking law in the United States. Previously, it was difficult to prosecute hackers who accessed computers without authorization.
- **Computer Security Act of 1987**. This law improves the protection of private information when stored on U.S. federal information systems. This law also assigned to the National Institute of Standards and Technology (NIST) the task of developing standards for security practices for federal information systems.
- **Sarbanes-Oxley Act of 2002**. Also known as the Public Company Accounting Reform and Investor Protection Act of 2002, or just SOx, this law requires U.S. public companies to implement a comprehensive control framework around its financial accounting, including supporting IT systems and infrastructure. This has resulted in a significant increase in security controls in most public companies.
- **Federal Information Security Management Act of 2002 (FISMA)**. This law extended the Computer Security Act of 1987 by requiring annual audits of Federal information systems as well as those of affiliated parties (typically U.S. government contractors).
- **Controlling The Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003**. This law made it illegal to send unsolicited commercial e-mail (UCE—but more often known as "spam") to individuals without their consent.
- **Identity Theft and Assumption Deterrence Act of 2003**. This act updated the law on "fraud related to activity in connection with identification documents, authentication features, and information" by making it illegal to possess of any "means of identification" used to "knowingly transfer, possess, or use without lawful authority."
- **State laws regarding information disclosure**. The majority of U.S. states have passed laws that require organizations to disclose security breaches that involve the unauthorized disclosure of personally sensitive information. The states have done so because the U.S. federal government has not yet passed such a law. These state laws require an organization to notify citizens in writing when their personally sensitive information has been compromised. Each state's laws vary somewhat, although many are modeled after the first such law, California's SB-1386.

Canadian Laws

Canada has passed laws defining many activities involving computers and networks as crimes, including:

- **Interception of Communications (Criminal Code of Canada, § 184)**. This law makes it illegal to intercept any private communication over any medium.
- **Unauthorized User of Computer (Criminal Code of Canada, § 342.1)**. This law criminalizes unauthorized uses of computers.

- **Privacy Act, 1983**. This law placed restrictions on the Canadian government on the collection, storage, and use of private information.
- **Personal Information Protection and Electronic Documents Act (PIPEDA)**. This law restricts the collection, storage, and use of citizen's private information by private companies in Canada.

European Laws

The European Union, as well as many of its member countries, has developed laws to protect computer systems and information. The basis of laws and cultural differences between Europe and the United States has resulted in laws that sometimes take a different approach to the protection of information.

- **Computer Misuse Act 1990 (CMA)**. This UK law defines unauthorized access to a computer as a crime, as well as the use of hacking tools against a computer, whether or not successful.
- **The Regulation of Investigatory Powers Act 2000**. This is a controversial UK law that permits wiretapping and surveillance, and can in some circumstances force an individual to surrender an encryption key to government authorities.
- **Anti-terrorism, Crime and Security Act 2001**. This UK law was passed shortly after the September 11, 2001 attacks on the United States. The law gives the government additional powers regarding seizure and freezing of terrorist funds. It also allows for the deportation of suspected terrorists and others who are threats to national security. Other parts of the law make changes in airline security, hate crimes, police powers, bribery, weapons of mass destruction, and retention of data by telephone companies and Internet service providers.
- **Data Protection Act 1998 (DPA)**. This is a pivotal UK privacy law that governs the protection of personal data. The law defines eight principles of data protection that are:
  1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—
     (a) at least one of the conditions in Schedule 2 is met, and
     (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
  2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
  3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
  4. Personal data shall be accurate and, where necessary, kept up to date.
  5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
  6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

- **Fraud Act 2006**. This UK law defines three categories of fraud—fraud by false representation, fraud by failing to disclose information, and fraud by abuse of position. This law makes identity theft and activities related to it unlawful, because identity theft is a form of fraud.
- **Police and Justice Act 2006**. A part of this law amended the Computer Misuse Act 1990 by criminalizing acts that have the intent to impair the operation of a computer.
- **Privacy and Electronic Communications Regulations 2003**. This is a UK law that makes it illegal to use equipment to make automated telephone calls that play recorded messages. This is similar to the U.S.-based "do not call" laws.
- **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**. This 1981 treaty signed by the Council of Europe was the first move towards protecting citizens' private data that was, at the time, being processed by computers. This treaty obligated the signatories to enact laws to protect private information.
- **Directive on the Protection of Personal Data**. This European Union law is also known by its number, *95/46/EC*. This is a wide-sweeping privacy law that applies to all of Europe and is used to protect the flow of information related to European private citizens.

Laws in Other Countries

Practically every other country in the world has enacted one or more laws that define various activities as crimes. By far the most common activities classified as crimes are:

- **Unauthorized entry**. In many countries it is now a crime to access a computer when one is not authorized to do so.
- **Creation or distribution of malware**. Many countries now make it illegal to create, release, or distribute malware.

Managing Compliance

Organizations in many countries and in most industrial and government sectors are required to comply with laws and regulations that are related with the protection of information and information systems. In many cases, such as with financial institutions in the United States organizations are subject to multiple sets of laws and regulations. This can prove to be quite challenging with regards to coordinating and tracking activities to ensure that they are compliant.

Organizations usually approach this issue by adopting or developing a framework of controls that can help to organize business and security controls into a logical arrangement. Control frameworks that are most often adapted include:

- **COBIT** (Control Objectives for Information and related Technology). Developed by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1996 and updated several times since, the COBIT framework consists of key control objectives and a life cycle of planning and internal audit.
- **COSO**. Originally developed in 1994, the COSO control framework was developed by the Committee of Sponsoring Organizations of the Treadway Commission, a private organization sponsored by American Institute of Certified Public Accountants (AICPA), American Accounting Association (AAA), Financial Executives International (FEI), the Institute of Internal Auditors (IIA) and the Institute of Management Accountants (IMA). The COSO controls framework was developed in response to new U.S. laws aimed at improving corporate financial reporting and eliminating fraud and corruption. COSO was updated in 2004 as a result of the Sarbanes-Oxley Act, which imposed further controls on corporate financial reporting as a result of the Enron scandal.
- **ISO 27002:2005**. Formally entitled the Code of Practice for Information Security Management, ISO 27002:2005 is a framework of controls covering the entire spectrum of security management.

Organizations generally use one of these frameworks as a starting point and then develop additional controls that reflect the results of risk analysis or specific laws and regulations.

The life cycle activities for these and other frameworks resemble the Plan-Do-Check-Act process lifecycle shown in Figure 6-2. The activities are described here:

- **Plan**. Establish policies, processes, procedures, architectures, and so on.
- **Do**. Implement and perform the processes and procedures.

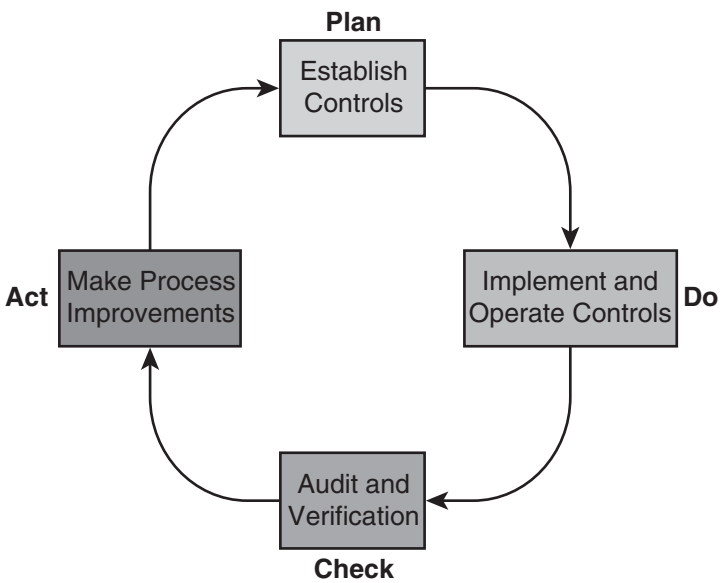


Figure 6-2 The process-based controls life cycle

Source: Course Technology/Cengage Learning

- **Check**. Periodically verify the correct operation and implementation of processes and architectures through internal or external audit and control testing.
- **Act**. Make improvements to processes and architectures based upon the results of internal and external audits.

Security Incident Response

Security incident response is the discipline of creating coordinated response plans in advance of an incident.

A **security incident** is defined as a violation of security policy. For example, if security policy states that users are forbidden from sharing computer passwords and it is learned that a user has shared a password with another person (deliberately or not), an **incident** has occurred. If the other person has used the employee's computer account, this would be a somewhat more significant incident, and it would be more significant still if it were discovered that this other person was an outsider who accessed company or personal information. As you can see from this example, an incident can vary in criticality, scope, and impact, as well as the actual response required.

Security incident response should follow a structured model, so that staff and management will not overlook important steps as the incident plays out. The phases of security incident response are:

- Incident declaration
- Triage
- Investigation
- Analysis
- Containment
- Recovery
- Debriefing

The activities triage, investigation, and analysis may occur in a continuum without distinct boundaries. As the following sections explain, triage is the search for evidence, investigation is the focus on the evidence, and analysis is the process of determining what happened.

Incident Declaration

A security incident will be declared when trained individuals become aware that a policy violation has occurred. But the trouble is, incidents are often unrecognized in their early stages and instead thought to be non-security in nature.

Security incidents can be triggered by several events including:

- **Apparent malfunctions or outages**. System malfunctions, slowness, or failures that are initially attributed to defects may actually be the actions of malware or an attacker. Only after an engineer has been dispatched to determine the cause of a problem does the organization realize that malicious activity is the problem's root cause.

- **Threat or vulnerability alerts**. The nature of a specific threat or vulnerability alert received from a product vendor or security organization may prompt the declaration of a security incident, if the threat is thought to be active or imminent.
- **News media**. On occasion, an organization learns about a security incident in its own environment through the news media.
- **Customer notification**. A user or customer may be experiencing difficulties that may be caused by a security policy violation.

Triage

When a security incident has been declared, designated and trained staff members and management should initiate incident triage procedures. In the context of security incident management, the triage process involves the search for—and examination of—clues that will hopefully lead to a root cause and the ability to apply corrective measures.

The origins of the term *triage* are best described in Merriam Webster's definition: "*the sorting of and allocation of treatment to patients and especially battle and disaster victims according to a system of priorities designed to maximize the number of survivors*." In an emergency room setting, a triage nurse quickly sorts through patients according to the urgency of their need for care. Back in the context of security incident response, staff members searching for clues that will lead them closer to the cause of the incident will briefly examine each bit of information and, like a triage nurse, prioritize the clue as to its likelihood to be associated with the incident or not.

Incident handlers need to use some caution when searching for information. Because of the possibility that the systems that they are examining may literally be a crime scene, non-invasive techniques need to be used as much as possible, according to computer forensics practices, which are discussed later in this chapter. It is highly likely that a security incident will not be declared until the triage stage of what is thought to be a non-security-related incident. Often, only after staff members begin to understand why a particular incident is occurring will they come to the realization that they are not looking at an ordinary malfunction, but a security incident.

Investigation

The triage and investigative phases can almost be thought of as one continuous activity. Both are concerned with the identification of evidence that will lead the response team closer to knowledge of the incident's root cause. Investigation is the closer study of information that is thought to be related to the cause of the incident. Where triage is the search for substantive information, investigation is the deeper study of the *right* information.

Analysis

As the incident unfolds and triage leads to investigation, so investigation leads to analysis. Analysis is a deeper study of the information that is directly related to the incident. Analysis helps to answer one or more of the following questions about the incident:

- What happened?
- How did this happen?
- What is the scope of the incident?

Another important objective of analysis is the determination of the steps needed to begin containment and recovery operations.

Containment

As the nature of the security incident becomes known, the response team must take steps to contain the incident—that is, to halt the incident and to prevent its spread. If the incident is of the type where the unwanted activity is still ongoing, the team needs to figure out how to make it stop. If the unwanted activity has ceased, measures must be taken to prevent its recurrence.

Every incident is different. In some cases, containment may be performed in stages, sometimes early in the incident in the form of disconnecting a system from the network, and again later on in the form of stopping unwanted processes, for instance.

Sometimes containment will be the first active steps taken on a system where staff members are making actual changes to the way the system is behaving (for instance, halting unwanted programs). The response team may need to take its last forensic samples prior to commencing containment activities that may alter the "pristine" (pre-action) state of the system.

Recovery

Recovery is the process of restoring a system to its pre-incident condition. Depending upon the nature of the incident, recovery may involve one or more of the following activities:

- Repairing or replacing hardware
- Reinstalling operating system or application software
- Reconfiguring operating system or application software
- Removing unwanted programs and data
- Restoring damaged or missing data from backup media

Like other phases in security incident management, containment and recovery have blurred lines—or one may be more dominant than the other, depending upon the type of incident. With some types of incidents, containment and recovery may be one and the same, while in others they are distinctly separate activities.

Work done during the investigative and analysis stages of the incident response may also include measures that need to take place to prevent the recurrence of this or a similar incident. Recovery operations may also include these additional measures, but sometimes these measures are not determined until the next stage of incident response, **debriefing**.

Debriefing

The final step of security incident response is a **debriefing** of the response team and management. The purpose of the debriefing is to reflect on the incident itself and the organization's

response to it, in order to learn from these activities. Some of the improvements that can be identified in the debriefing include:

- **Technical architecture**. An incident may have revealed weaknesses in some aspect of the technical architecture that, when improved, will reduce the probability or the impact of recurrence.
- **Technical controls**. An incident may have uncovered the absence or a defect in a technical control that would have minimized or prevented the incident.
- **Processes and procedures**. Sometimes an incident is caused not by a weakness in technology but a weakness in a business process or procedure. For example, an incident caused by a disgruntled employee's actions may reveal that the process and procedures associated with terminating employee access had some holes.
- **Security incident response**. The response team may reflect on the handling of the incident and discover improvements that will make subsequent responses more effective.

Incident Management Preventive Measures

A mature security incident program should include a preventive component. If the impact or scope of an incident can be reduced or prevented altogether, then the effort expended in investigation and recovery will similarly be reduced.

Primarily, incident prevention consists of two components:

- **Creation of a vulnerability and threat awareness capability**. Many types of incidents can be minimized or avoided altogether if personnel are aware of an active threat or vulnerability. Such awareness is available from both internal and external sources including:
  - *Security alerts from US-CERT, Secunia, SANS, anti-virus vendors, and suppliers*. These alerts include security advisories regarding vulnerabilities and threats that give organizations time to prepare for emerging threats.
  - *Company internal events, such as terminations*. Because many events are the results of actions carried out by current and former employees, awareness of terminations can give the organization an opportunity to take any measures necessary to thwart a former employee's attempt to inflict damage on the organization.
  - *Events detected by Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)*. IDS and IPS can detect an emerging threat that may be contained through the enactment of additional preventive measures.
- **Implementation of a defense in depth strategy to protect assets**. The results of risk assessments ought to indicate characteristics in an environment where defenses can be improved in order to reduce the probability, impact, or scope of a threat or vulnerability. The addition of detective, preventive, or deterrent controls will either make an incident less likely to happen or reduce the impact of a threat if it is realized.

Incident Response Training, Testing, and Maintenance

To effectively manage an incident, the staff members who will likely be involved in a security incident need to know how they are expected to respond when a real incident occurs. Incident response training can involve one or more of the following activities:

- **Procedure review**. Staff members can become acquainted with incident handling by reading the response procedures.
- **Formal training**. Staff members can attend formal training sessions that review response procedures and provide opportunities for group discussion and questions.
- **Incident walkthrough**. The security incident response team can perform a security incident walkthrough. Primarily this involves a step-by-step review of security incident procedures, discussing possible scenarios, responses, and issues at each step. A walkthrough is also considered a test of incident response procedures.
- **Incident simulation**. More involved than a walkthrough, a simulation is the acting out of the procedures by response personnel as though a real incident were playing out. A simulation provides more realism than a walkthrough and usually includes a facilitator who orchestrates the event by providing regular "updates" as the simulated event unfolds. A simulation is both an excellent way to test incident response procedures as well as a training opportunity by giving incident handlers some "experience" at performing incident procedures.

In order to maintain the ongoing effectiveness of the incident response team, training needs to be considered an ongoing regularly-scheduled activity. Changes in the makeup and management of teams, procedures, and technologies should necessitate a periodic review of incident response procedures to make sure that they will remain effective while these expected changes take place over time.

Incident Response Models

Organizations that want to develop their own security incident response capability can adopt the model described in this text or develop one of their own. There are also several incident response models available from well-respected security organizations including:

- **CERT Coordination Center** (**CERT/CC**). Formed in 1988 after the Morris Worm Incident, CERT/CC has developed and published a wealth of information on the development of security incident response capabilities. www.cert.org/csirts/
- **Forum of Incident Response and Security Teams** (**FIRST**). Founded in 1990, FIRST has several documents including the Best Practice Guide Library (BPGL) and CERT-in-a-Box. www.first.org
- **National Institute of Standards and Technology** (**NIST**) special publication 800-61, Computer Security Incident Handling Guide. www.nist.gov

Reporting Incidents to Management

An organization's security policy should include the requirement that its staff report security incidents at once. Doing so will result in an appropriate response that can be started sooner, often resulting in less damage or disruption to the organization. Employees should be directed to not attempt to manage security events on their own, regardless of the circumstances.

Event Type	Investigation	Incident Response
Employee misconduct	Pornography, harassment	Sabotage, disclosure of sensitive information to outsider
Malware	Isolated to individual system or as a result of misuse	Malware infection that results in business disruption
Stolen asset	Stolen laptop	Information stolen by outsider where there is a threat or fear of disclosure
Violation of acceptable use policy	Misuse of company assets	Misuse of company assets that results in material impact to the organization

Table 6-1 Incident response versus and investigations: examples

Investigations

Some security professionals may be responsible for conducting or guiding security-related investigations. There is a distinction between security incident that require a coordinated and well orchestrated response from teams, and small isolated events that do not require a team effort.

There is not a well recognized and distinct boundary between the types of events that require an incident team response and those that can be handled by an individual security professional. Criteria that separate the two capabilities that work for one organization may not work in another. Still, a general distinction is made in Table 6-1.

An investigator's work must have integrity in several key areas, including:

- **Evidence collection**. A simple case such as employee misconduct can result in the employee's dismissal that may be followed by a wrongful-termination lawsuit. This is discussed in detail later in this chapter.
- **Consistent procedures**. Every security matter should be handled in a consistent manner, so that there is no hint of favoritism or bias.
- **Recordkeeping**. Every investigation should be documented in the event that it plays a part in a larger incident or investigation in the future.
- **Management review**. All incidents should be reviewed by management, so that they have visibility into events that provide a clearer view of overall risk in the organization.

Involving Law Enforcement Authorities

When an incident or issue has taken place, response procedures and policies should require the person(s) responsible for business or data security determine whether a crime has been committed. This is a simple and obvious task when a tangible asset such as a laptop computer has been stolen, but decidedly less clear when other types of events take place.

Many organizations often consider unauthorized entry into a computer system as a private matter and do not contact law enforcement authorities for several reasons including:

- **Embarrassment**. Organizations wish to avoid the public humiliation and embarrassment of a computer crime, as it may lead many to conclude that the organization cannot properly manage or secure its systems.
- **Disruption of services**. Organizations fear that reporting computer-related crimes will cause disruptions in computer-provided services if law enforcement agencies will wish to confiscate affected computers as evidence.
- **Difficulty of prosecution**. Often when a computer-related crime takes place, law enforcement may make no effort to identify or prosecute the perpetrator, but if they do, prosecution is often difficult, particularly when it relies on computer-based forensic evidence.

With regards to security incidents that involve the unauthorized disclosure of personally sensitive information, many U.S. states, as well as other countries, now require organizations to report such disclosures to affected citizens and/or law enforcement authorities. Further, regulations in some industries require that organizations disclose security incidents. Often, organizations no longer have a choice but are required to report security incidents to involved citizens, law enforcement, or industry regulators.

It is recommended that information security professionals establish relationships with local and national law enforcement authorities in order to become acquainted with the procedures for reporting crimes as well as guidance for preventing them.

Forensic Techniques and Procedures

According to Merriam-Webster, the definition of **forensics** is "the application of scientific knowledge to legal problems, especially the scientific analysis of physical evidence as from a crime scene." In the context of computers and networks, forensics is the body of procedures used to examine a computer system and its contents for evidence that may be used in an anticipated legal action.

The primary activities in computer forensics are:

- Identify and gather evidence
- Preserve evidence
- Establish a chain of custody
- Present findings

The U.S. National Institute for Standards and Technology (NIST) has published several documents on computer forensics including:

- Special Publication 800-72, Guidelines on PDA Forensics.
- Special Publication 800-86, Guide to Integrating Forensic Techniques into Incident Response.
- Special Publication 800-101, Guidelines on Cell Phone Forensics.
- Bulletin 11-01, Computer Forensics Guidance.

Identifying and Gathering Evidence

Computers and other devices store a tremendous volume of information. As storage media continues to drop in price, the amount of storage capacity on newer systems is increasing at substantial rates. This provides a challenge to forensics professionals who are sometimes overwhelmed by the sheer volume of data present on systems.

Generally a computer forensics professional will be given some initial indications on the nature of an investigation. Some of the likely possibilities are:

- **E-mail**. The user may be suspected of sending inappropriate messages, or leaking company secrets via e-mail.
- **Web access**. A user may be under suspicion of visiting specific web sites, or categories of web sites that are deemed to be inappropriate.
- **Storing data**. A user may be suspected of storing information inappropriately, such as company secrets on a laptop computer in violation of policy against such a practice.
- **Inappropriate access**. An employee may be using a computer to inappropriately access other computers in the organization in violation with stated policies.

These leads provide a starting point for the forensic specialist. Rather than being given a "we think the employee is doing something wrong," suspected activities such as those listed above provide direction for a forensic investigation.

Prior to the start of a forensics investigation, the computer forensics professional must carefully consider independence and objectivity: does the forensics professional have any interest (or appearance of interest) in the outcome of the matter being investigated? If so, the forensics investigator should consult with management and consider recusing herself from the matter.

Evidence Collection Techniques

The nature of a forensics investigation helps to define the approach taken by the investigator. Some of the activities that may be performed include:

- **Examination of surroundings**. The forensic specialist will usually wish to examine the undisturbed surroundings, where he may see and possibly want to also take any removable media, documents, notes, and so on. The investigator will probably want to take several photographs of the computer and its surroundings for later analysis.
- **Live system forensics**. The nature of the investigation may prompt the investigator to examine the running system. He may record open applications and documents, running processes, and may even wish to examine the memory space of some running processes.
- **Physical examination**. The investigator may wish to carefully examine the computer's case and fasteners, and in some situations examine the interior of the system using fiber optic technology, if he suspects the computer's owner/operator may have implemented forensics countermeasures that could obliterate evidence (or the investigator) should he open the case prematurely.
- **Examination of storage**. The examiner will almost certainly wish to examine the contents of the computer's storage. In most cases this is a hard drive but sometimes a computer's main storage is semiconductor-based, particularly in the case of mobile devices and very small laptop computers.

Examination of a computer's main storage usually necessitates the use of a tool used to make an exact copy of the hard drive or other storage. Sometimes an investigator will make more than one copy, in cases where the investigator wishes to boot a computer with one copy (which will change the contents of the copied media) to see how it behaves.

As the investigator combs through programs, files, and directories, his search will be focused on those parts of main storage that are associated with the activity that is under suspicion. For instance, if the user is suspected of visiting unauthorized web sites, the investigator will examine certain files that provide evidence of the specific pages on web sites that have been visited. Again, because the amount of data stored on a system's main storage can be so vast, the investigator needs to stay focused on specific areas.

Preserving Evidence

When the forensic investigator identifies the evidence he is looking for, he must take care to preserve it properly. Some aspects of evidence preservation are straightforward, such as copying hard drives, but others are more difficult, such as capturing the contents of memory on a running system or the main storage on a mobile device such as a smartphone.

The forensic investigator must follow several principles of evidence preservation including:

- **Recordkeeping**. The investigator must record every step taken during the forensic investigation, starting with his visit to the room where the computer is kept, and including every step taken. The records themselves will become a part of the body of evidence.
- **Use of reliable tools**. The investigator must use tools that are known to be reliable and produce consistent results. The investigator must also record the versions of tools that are used.
- **Evidence safekeeping**. All evidence that is gathered and created must be kept safe from tampering by others. Evidence should be kept in locked cabinets in a locked room except when the investigator is physically present and working on the case.
- **Work in isolation**. The examiner's workstation(s) that are used to examine the evidence should not be connected to any network. Doing so may give an opposing attorney or examiner the opportunity to put into question the integrity of the investigator's work by presenting the possibility that being connected to the Internet can introduce external forces, such as malware, that can alter the evidence.
- **Chain of custody**. Whenever evidence is created, moved, stored, or transferred to another custodian, thorough records must be kept and evidence safeguarded to ensure its integrity. This is discussed in more detail in the next section.

Chain of Custody

Chain of custody is *the document or paper trail showing the seizure, custody, control, transfer, analysis, and disposition of physical and electronic evidence*. As evidence is examined and created (in the case of the investigator's notes and records), it is vitally important that the investigator follow consistent procedures and record all activities in order to support the chain of custody.

If the chain of custody is broken, then it will be possible for a legal opponent to successfully challenge the integrity of the evidence by suggesting that it has been tampered. This could result in the evidence so painstakingly collected being entirely disregarded, which could affect the outcome of the legal proceeding.

Presentation of Findings

When the investigator has completed his investigation of the computer or mobile device, he will then write a formal report that states what evidence was found and his professional opinion on the meaning of the evidence. A good forensics report will contain only the facts and well-supported conclusions and not include any speculation or statements regarding the motive of the person whose system is being examined.

Ethical Issues

The subject of ethics involves the behavior of professionals in a variety of business situations, particularly when challenged with choices that involve the potential for political favor, personal gain, escaping responsibility, or unfair advantage over others. In order to deter such activity, many organizations have developed a formal Code of Conduct statement that defines the types of activities that are permitted and which are discouraged. The Internet Activities Board (IAB) published an ethics statement entitled *Ethics and the Internet* in 1989, and $(ISC)^2$, the governing corporation for the CISSP certification, has developed its own **code of ethics**.

Codes of Conduct

Many organizations publish a **code of conduct** in order to define specific activities that are either permitted or forbidden. A typical code of conduct will include the following topics:

- Obey all laws.
- Always dress and act professionally.
- Avoid conflicts of interest.
- Avoid outside employment.
- Engage in good public relations through community activities.
- Avoid activities with customers or suppliers that would raise suspicion of favoritism or activities that result in personal gain.
- Use organizational resources and funds for business purposes only.
- Always maintain accuracy in all books, records, and communications.
- Separate personal activities from business activities.
- Maintain privacy and confidentiality of all business related information.

In most cultures these activities define an overall manner of professional integrity in line with moral and natural laws, as well as established laws and regulations that the organization is required to conform to.

RFC 1087: Ethics and the Internet

In 1989 the Internet Activities Board (IAB) developed a policy statement entitled Ethics and the Internet, regarding the proper use of Internet resources. The policy reads,

The Internet is a national facility whose utility is largely a consequence of its wide availability and accessibility. Irresponsible use of this critical resource poses an enormous threat to its continued availability to the technical community.

The U.S. Government sponsors of this system have a fiduciary responsibility to the public to allocate government resources wisely and effectively. Justification for the support of this system suffers when highly disruptive abuses occur. Access to and use of the Internet is a privilege and should be treated as such by all users of this system.

The IAB strongly endorses the view of the Division Advisory Panel of the National Science Foundation Division of Network, Communications Research and Infrastructure which, in paraphrase, characterized as unethical and unacceptable any activity which purposely:

(a) seeks to gain unauthorized access to the resources of the Internet,

(b) disrupts the intended use of the Internet,

(c) wastes resources (people, capacity, computer) through such actions,

(d) destroys the integrity of computer-based information,

and/or

(e) compromises the privacy of users.

The Internet exists in the general research milieu. Portions of it continue to be used to support research and experimentation on networking. Because experimentation on the Internet has the potential to affect all of its components and users, researchers have the responsibility to exercise great caution in the conduct of their work. Negligence in the conduct of Internet-wide experiments is both irresponsible and unacceptable.

The IAB plans to take whatever actions it can, in concert with Federal agencies and other interested parties, to identify and to set up technical and procedural mechanisms to make the Internet more resistant to disruption. Such security, however, may be extremely expensive and may be counterproductive if it inhibits the free flow of information which makes the Internet so valuable. In the final analysis, the health and well-being of the Internet is the responsibility of its users who must, uniformly, guard against abuses which disrupt the system and threaten its long-term viability. (Internet Engineering Task Force, http://www.rfc-editor.org/rfc/rfc1087.txt)

RFC 1087 was published prior to the passage of many of the laws that define many of the unacceptable uses as illegal. But, laws or not, we are obligated to protect the Internet and uphold its nearly-universal utility to the countries and citizens of the world, and to discourage and oppose all acts and persons who seek to bring ill favor or harm to it.

The (ISC)^2 Code of Ethics

A **code of ethics** is a formal written statement—a code of responsibility used in an organization to define permitted and forbidden activities. Places of employment and professional organizations often develop a code of ethics (sometimes called a code of conduct). (ISC)^2, the organization that manages the CISSP certification, has a code of conduct. The canons of the (ISC)^2 code of ethics read:

- Protect society, the commonwealth, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals.
- Advance and protect the profession.

The entire $(ISC)^2$ Code of Ethics appears in Appendix B of this book.

All CISSP and SSCP certification holders are required to uphold the $(ISC)^2$ code of ethics. Failure to do so can result in the loss of one's certification. But what does it mean to apply this code of ethics in the security profession? I will expand upon the meaning of each of the code of ethics canons:

- **Protect society, the commonwealth, and the infrastructure**. We must uphold personal and corporate liberties, and act to protect the ongoing viability of peoples, governments, and the means used to communicate with one another. We must help others to better understand how to protect themselves and their ability to communicate with others. More specifically, we are duty bound to help others better understand how to protect their computers and their networks.
- **Act honorably, honestly, justly, responsibly, and legally**. We are to contribute to the good name of our profession, information, and business security. We are to always be truthful, but beyond that, to defend the truth. We cannot show favoritism, bias, or partiality. We must always uphold the law and encourage others to do so.
- **Provide diligent and competent service to principals**. We must value and perform excellent work for our employers. We should work with our heads to discover better ways to do our jobs, and to contribute to the good of our employers.
- **Advance and protect the profession**. We must promote the arts and sciences of business and data security, doing so in ways that bring respect and favor to our profession. We need to encourage others to join our profession, mentoring and guiding them, ultimately making them new guides to lead still others into our vocation.

By upholding these canons we must bring honor to ourselves and our profession. In the eyes of others we must act like model citizens. After we retire, or die, we should each be remembered for our honor and service to others.

Guidance on Ethical Behavior

The following principles provide additional guidance on ethical behavior in the workplace.

- **Behave transparently**. Say what you mean and mean what you say.
- **Make decisions openly**. Give no illusions of a person who makes "back room deals."
- **Shun politics**. Do not give in to a pervasive political culture.
- **Show no favoritism or self-interest**. Treat everyone fairly. Do not give or accept favors or appear that you are doing so.
- **Respect the privacy and dignity of others**. Keep private matters private and continue to earn and keep the respect of others.
- **Keep your commitments**. Be a man or woman of your word.
- **Promote accountability and responsibility**. Every person must be responsible for their behavior and for the consequences of their decisions. Act in this regard and expect others to do the same.
- **Document your actions**. Keep a logbook of conversations, decisions, and actions, to aid the memory and to provide a record of matters considered.

Here are some examples of situations that an information security manager may face:

- Someone reports seeing another manager in the organization encouraging employees to make illegal copies of a registered ISO standards document.
- An executive is discovered to be viewing child pornography on business premises using business resources. When confronted, the executive makes threatening statements to his accuser about "career limiting decisions."
- An IT manager encourages the use of free versions of anti-virus and file compression programs, even though their terms of use prohibit commercial use.

In these types of situations, the information security manager consider his or her professional integrity, accountability on his and his colleagues' part, and legal obligations.

Chapter Summary

- Computers play a variety of roles in computer crimes: they are the target of crimes, an instrument of crimes, and they support crimes.
- The categories of computer crimes are military and intelligence attacks, financial attacks, business attacks, grudge attacks, "fun" attacks, and terrorist attacks.
- The categories of U.S. law are criminal, civil, and administrative. Criminal laws address matters of public order; civil laws address grievances between parties; and administrative law governs the actions of federal agencies.
- The categories of U.S. law that protect information and computers are intellectual property laws, privacy laws, and computer crime laws.
- The types of intellectual property protections are copyrights, trademarks, and patents.
- Most countries have passed laws that protect the privacy of personally-sensitive information. Many U.S. states have passed laws that require the disclosure of unauthorized disclosures of personally-sensitive information, most notably California's SB-1386.
- Security incident response consists of several steps including incident declaration, triage, investigation, analysis, containment, recovery, and debriefing.
- Staff members should be trained in security incident response procedures so that they will act more effectively during a real incident.
- Forensic procedures should be followed when investigating a security incident, because of the possibility that the incident may become a part of a future legal action.
- The primary activities in a forensic investigation are: identify and gather evidence, preserve evidence, establish a chain of custody, and present findings.
- Strict procedures must be followed when performing a forensic examination, so that the original evidence is not altered and that information identified and gathered are never altered or compromised.
- In a forensic examination, the chain of custody is the paper trail that shows the seizure, custody, control, transfer, analysis, and disposition of physical and electronic evidence.

- Many organizations will develop a *code of conduct* to define the activities that are acceptable and unacceptable.
- The $(ISC)^2$ code of ethics defines the desired and undesired behavior that it expects of its CISSP and SSCP certification holders. The $(ISC)^2$ will consider stripping the certification from anyone who violates the code of conduct.
- The Internet Activities Board (IAB) published RFC 1087: Ethics and the Internet, a statement of ethics concerning the acceptable use of the Internet.
- Security professionals should always conduct themselves so as not to ever give even the appearance of violating an organization's security policy or the $(ISC)^2$ Code of Ethics.

Key Terms

Administrative law The branch of law in the United States that defines the rules and regulations that govern activities in executive departments and agencies in the U.S. government.

Blackmail *See* Extortion.

Botnet A collection of software robots (or "bots") under centralized control that run autonomously and automatically.

Business attack An attack that targets a computer or network owned by a business for the purpose of gaining intelligence, financial gain, or Denial of Service.

Chain of custody The procedures and paper trails that track forensic evidence in a legal investigation.

Civil law The branch of law that deals with disputes between individuals and/or organizations.

Code of conduct A policy statement published by an organization that defines permitted and forbidden activities.

Code of ethics A code-of-responsibility statement that is used in an organization to define specific permitted and forbidden activities.

C.F.R. *See* U.S. Code of Federal Regulations.

Competitive intelligence Activities regarding the acquisition of information and secrets about a competing organization's products, services, financials, and other business activities.

COBIT (Control Objectives for Information and related Technology) A controls framework for the management of information technology and security.

Copyright The legal right to exclusive use that is given to the creator of an original work of writing, music, pictures, and films.

COSO (Committee of Sponsoring Organizations of the Treadway Commission) A controls framework for the management of information systems and corporate financial reporting.

Criminal law The branch of law that enforces public order against crimes such as assault, arson, theft, burglary, deception, obstruction of justice, bribery, and perjury.

Cyberterrorism Acts of violence against civilians and governments that are carried out in cyberspace.

Denial of Service attack An attack against a computer or network that is designed to incapacitate the target.

Debriefing A meeting or conference during which the details of an incident are discussed, in order to learn from the incident and the organization's response to it.

Embezzlement The act of dishonestly or illegally appropriating wealth from another party, often an employer or service provider.

Espionage The process of obtaining secret or confidential information without the permission of the holder of the information.

Extortion The act of obtaining money or other valuables from a person or organization through coercion, intimidation, or threat.

Financial attack An attack against a computer or network that is intended to provide financial gain for the attacker.

Forensics The application of scientific knowledge to solve legal problems, especially the analysis of evidence from a crime scene.

Fun attack An attack against a computer or network that is usually performed for the thrill alone.

Fraud An act of deception made for personal gain.

Grudge attack An attack against a computer or network that is carried out as an act of revenge against its owner.

Identity theft A crime that involves the illegal use of some other person's identity.

Incident An unexpected event that results in an interruption of normal operations. See also *Security incident*.

Information warfare The use of information or information systems in the pursuit of an advantage over an opponent.

Intellectual property (IP) A product of creation such as information, architecture, invention, music, image, and design.

Intellectual property law The branch of law that protects created works and includes such safeguards as copyrights, trademarks, service marks, and patents.

Military attack (in the context of information security) An attack against a computer or network used by a military organization.

Patent A means of legal protection for exclusive rights to an invention or process.

Recovery The process of restoring a system to its pre-incident condition.

Script kiddie An individual with relatively low skills who breaks into computer systems using tools written by others.

Security incident An event in which some aspect of an organization's security policy has been violated.

Security incident response The procedures followed in the event of a security incident.

Terrorist attack See *cyberterrorism*.

Trade secret A formula, design, process, or method used by an organization to gain competitive advantage over others.

Trademark A means of legal protection for exclusive rights to a name or symbol.

United States Code (U.S.C.) The body of published criminal laws in the United States.

U.S. Code of Federal Regulations (C.F.R.) The code of administrative law in the United States.

Review Questions

1. The categories of U.S. laws are:
   a. Executive, judicial, and legislative
   b. Criminal, civil, and administrative
   c. Laws and regulations
   d. Criminal and civil
2. Where are U.S. laws published:
   a. Criminal and civil laws are published in the United States Code (U.S.C.), and administrative laws are published in the U.S. Code of Federal Regulations (C.F.R.)
   b. Criminal and civil laws are published in the U.S. Code of Federal Regulations (C.F.R.), and administrative laws are published in the United States Code (U.S.C.)
   c. Executive and judicial laws are published in the United States Code (U.S.C.), and legislative laws are published in the U.S. Code of Federal Regulations (C.F.R.)
   d. Regulations are published in the United States Code (U.S.C.), and laws are published in the U.S. Code of Federal Regulations (C.F.R.)
3. The most appropriate intellectual property protection for the design of a system is:
   a. Trade secret
   b. Copyright
   c. Trademark
   d. Patent
4. An organization has invented a new type of semiconductor for use in computers, and wishes to protect its intellectual property rights in a manner where no other company can know how the semiconductor was designed or constructed. The best course of action is:
   a. Obtain a patent for the design
   b. Obtain a trademark for the design
   c. Keep the design a trade secret
   d. Obtain a copyright for the design
5. The first U.S. law to define computer trespass is:
   a. Federal Information Security Management Act
   b. Sarbanes-Oxley Act

c. Computer Fraud and Abuse Act
d. Computer Misuse Act

6. The purpose of debriefing after a security incident includes all of the following EXCEPT:
   a. Discussion of changes in processes and procedures
   b. Discussion of changes in incident response
   c. Discussion of sanctions against contributing personnel
   d. Discussion of changes in technical controls
7. An organization has discovered that an employee has been harvesting credit card information from its databases and selling them to a criminal organization. The organization should:
   a. Notify law enforcement
   b. Quietly terminate the employee
   c. Install a key logger and continue to monitor the employee's actions
   d. Notify the owners of the compromised credit card numbers
8. A computer forensics expert has been asked to collect evidence from an individual's workstation. The collection techniques used by the computer forensics expert should include all of the following EXCEPT:
   a. Examination of the running system
   b. Physical examination
   c. Examination of surroundings
   d. Collection of fingerprints
9. What factor will motivate a computer forensics specialist to examine a running system instead of waiting to take an image of the system's hard drive:
   a. Full disk encryption
   b. BIOS boot password
   c. Data present in the paging file
   d. Live Internet connection
10. A computer forensics examiner is about to conduct a forensics examination of a computer's hard drive, and anticipates that he will be cross-examined in a deposition. What should the examiner do to ensure that the image he takes of the computer's hard drive is an exact copy of the hard drive?
    a. Reconcile the numbers of files and directories on the original and copied image
    b. Perform SHA-1 and MD5 checksums of the original drive and the copied image
    c. Use a write blocker when making a copy of the original drive
    d. Make a copy of the hard drive and perform forensics on the original

11. The process of safekeeping and recordkeeping of computer forensics evidence is known as:
    a. Chain of custody
    b. Chain of evidence
    c. Burden of proof
    d. Best evidence rule
12. The 1987 statement that defines principles of behavior for Internet usage is:
    a. Computer Fraud and Abuse Act
    b. $(ISC)^2$ Code of Ethics
    c. RFC 1087: Ethics and the Internet
    d. Computer Misuse Act
13. The statements, "Protect society, the commonwealth, and the infrastructure," "Act honorably, honestly, justly, responsibly, and legally," "Provide diligent and competent service to principals," and "Advance and protect the profession" are contained in:
    a. Internet Activities Board (IAB) Guiding Principles
    b. $(ISC)^2$ Code of Ethics
    c. RFC 1087: Ethics and the Internet
    d. Computer Fraud and Abuse Act
14. A security manager in a government post needs to hire an outside consultant to perform risk analysis. A relative of the security manager is qualified to perform the work. The security manager should:
    a. Document why the relative is the best choice
    b. Consider alternative consultants instead
    c. Recuse himself from the decision-making process
    d. Hire the relative
15. The U.S. law that permits a law enforcement agency to conduct a search warrant without a subpoena is:
    a. PATRIOT Act
    b. Communications Assistance for Law Enforcement Act
    c. Personal Information Protection and Electronic Documents Act
    d. Executive Order 13402

Hands-On Projects

Project 6-1: Compare Forensic Analysis Tools

In this project you will compare the features of some forensic analysis tools to be used in a small company's IT department.

Find one or more web sites that discuss and review forensic analysis tools that would be suitable for use in a smaller organization. The tools to be considered should possess ability to:

1. Copy the contents of a computer's hard drive.
2. Find and recover files that have been deleted on a computer's hard drive.
3. Determine a history of web sites that have been recently visited.
4. Search the computer's hard drive for files containing key words.
5. Compare the contents of files on a computer's hard drive.
6. Copy the contents of other storage devices such as USB drives.
7. Log the activities performed with the tool.

The company may want to consider one or more of the following tools that are available, including:

- AccessData FTK Imager
- AccessData Forensic Toolkit
- EnCase
- ProDiscover
- Safeback

Project 6-2: Conduct a Security Incident Simulation

In this project you will create a procedure for a walkthrough of a security incident simulation.

Develop a plan for security incident simulation. The plan should include the following:

1. A description of possible scenarios that will be the subject of the walkthrough.
2. A list of participants by function (network engineer, helpdesk tech, IT manager, and so on).
3. A choreographed set of "events" or "issues" that will unfold throughout the incident (examples of these events will be incoming news of observations seen by various staff members or of incoming communications).
4. A log of discussions and responses by participants.
5. Time allocated to debrief and discuss what was learned in the simulation.

How many participants have you chosen to participate in the simulation? What possible scenarios are you considering? How much total time are you allocating for the simulation?

Project 6-3: Analysis of the Internet Code of Ethics

In this project you will download and analyze the Internet Code of Ethics.

Retrieve a copy of RFC 1087: Ethics and the Internet and answer the following questions:

- Is the document still relevant today? Explain why or why not.
- Is the document written in a form that can be understood by today's Internet users? Explain why or why not.
- If you were asked to update the document, what changes would you make?

Case Projects

Case Project 6-1: Development of Information Security Incident Response Plan

As a consultant with the Risk Analysis Consulting Co., you have been asked to develop the information security incident response plan for the Raising Dough Baking Company, a statewide business that employs over three hundred employees. Raising Dough collects online orders from homes and small businesses and delivers their products with a company owned fleet of trucks.

The company does not currently have a security incident response plan. How will you approach the task of creating one? What information will you need to obtain from the company before you begin?

Will you develop a plan from scratch or will you use a model or template?

Case Project 6-2: Protection of Intellectual Property

As a consultant with the Data Protection Consulting Co., you have been assigned to help a client determine how to protect its intellectual property. The client is a software company that has developed several types of intellectual property including:

- Computer software that helps programmers test their own programs more easily.
- A new technique for analyzing software source code for defects.
- Brand names for programs that it offers for sale to customers.
- Business processes that it uses to process new orders more efficiently.

The client company does not know what kinds of safeguards should be used for each of these pieces of intellectual property. You need to determine whether the client should pursue a trademark, patent, or copyright for each. You also

need to advise the client on the advantages and disadvantages of keeping one or more of these pieces a trade secret.

Case Project 6-3: Develop a Code of Conduct

As a consultant with the Risk Advisors Co., you have been asked to take a consulting assignment with a client, the Rancid Fish Sauce Company, which needs help with the development of its new Code of Conduct.

Rancid Fish Sauce had problems with employee misconduct in the past, which has led company management to commission the development of a code of conduct.

You need to develop an outline for the code of conduct. Describe how you will approach this assignment, and where you will go for information.

Case Project 6-4: An Ethical Challenge

You are a security consultant with the Security Advisors Co. and have been asked to help investigate a recent security incident that took place at the law firm of Dewey, Cheatham, and Howe. In your assignment you have been assigned to work with the vice president of IT.

The security incident that you are investigating appears to be a case of an intruder who broke into a company computer to remove and destroy information on an upcoming legal case. A forensic examination revealed that the incident was actually an inside job that was perpetrated by one of the new programmers, who is a relative of the VP of IT.

When you wrote your findings and presented them to your client, the VP of IT has asked you to change the findings in your report to show that the perpetrator could not be found. The VP has promised future work for your company and a good recommendation for your work if you comply.

What will you do next?

chapter 7

Operations Security

Topics in this Chapter:

- Applying Security Concepts to Computer and Business Operations
- Records Management Security Controls
- Backups
- Anti-virus Software and Other Anti-malware Controls
- Remote Access
- Administrative Management and Control of Information Security
- Resource Protection
- Incident Management
- High Availability Architectures
- Vulnerability Management
- Change Management and Configuration Management
- Operations Attacks and Countermeasures

The (ISC)^2 *Common Body of Knowledge* (CBK) defines the key areas of knowledge for Operations Security in this way:

Operations Security is used to identify the controls over hardware, media, and the operators with access privileges to any of these resources. Audit and monitoring are the mechanisms, tools, and facilities that permit the identification of security events and subsequent actions to identify the key elements and report the pertinent information to the appropriate individual, group, or process.

The candidate will be expected to know the resources that must be protected, the privileges that must be restricted, the control mechanisms available, the potential for abuse of access, the appropriate controls, and the principles of good practice.

Key areas of knowledge:

- *Apply the following security concepts to activities:*
  - *Need-to-know/least privilege*
  - *Separation of duties and responsibilities*
  - *Monitor special privileges (e.g., operators, administrators)*
  - *Job rotation*
  - *Marking, handling, storing, and destroying of sensitive information and media*
  - *Record retention*
  - *Backup critical information*
  - *Anti-virus management*
  - *Remote working*
  - *Malware management*
- *Employ resource protection*
- *Handle violations, incidents, and breaches and report when necessary*
- *Support high availability (e.g., fault tolerance, Denial of Service prevention)*
- *Implement and support patch and vulnerability management*
- *Ensure administrative management and control*
- *Understand configuration management concepts (e.g., hardware/software)*
- *Respond to attacks and other vulnerabilities (e.g., spam, virus, spyware, phishing)*

Most of this chapter contains information on how to put into operation the concepts discussed in much of this entire book.

Applying Security Operations Concepts

Other chapters in this book define some of the basic concepts and tenets of control and good practice in information and business security. This section takes those concepts

and describes how they are put into practice in an organization. The concepts discussed in this section are:

- Need-to-know
- Least privilege
- Separation of duties
- Job rotation
- Monitoring of special privileges
- Records management controls
- Backups
- Anti-virus and anti-malware
- Remote access

Whenever an organization is about to undertake the process of putting a security concept into practice, it must first consult its security policy to see what must be done. As discussed in Chapter 1, "Information Security and Risk Management," the flow of control is Policy, Guidelines, Processes, Procedures, and Recordkeeping. This section describes the steps that can be taken to transform these concepts from idea to practice.

Need-to-Know

The concept of **need-to-know** states that individual personnel should have access to only the information that they require in order to perform their stated duties. Even if any specific individual has the necessary clearance to access specific information, access should still be granted *only* if the individual actually requires access to that information in order to perform her duties.

Here is an example. Managers in the marketing department of a company have access to a directory on a file server that contains a wide variety of marketing documents, including some that pertain to future expansion plans for the company. Of the ten managers, two are responsible for working on future expansion plans. Under the principle of need-to-know, only these two managers should have access to the documents related to future expansion.

In this example, only the persons who need to have access to sensitive future expansion information actually have that access.

The advantage of need-to-know-based access control is reduced risk. When fewer people have access to a given set of information, then the risk of unauthorized disclosure and compromise due to actions performed by employees is reduced proportionally. If the number of persons with access to a data set is reduced from ten to two, then the risk of disclosure through user access is reduced by 80 percent.

Carried to its logical conclusion, applying the concept of need-to-know can impose much additional administrative overhead on the management of access rights on a system. Organizations need to decide if, and where, to implement this level of access control. An organization going in this direction should first develop a policy statement that specifies where and under what circumstances need-to-know access controls will be implemented. Processes and procedures should specify *how* they will be implemented.

Least Privilege

The concept of least privilege states that users should have the fewest or lowest number of privileges required to accomplish their duties. In an environment where privileges are assigned to persons, those persons should be assigned the fewest, or lowest level, of privileges they require to accomplish their assigned duties.

For example, an organization purchases a financial management system that has many pre-defined roles and capabilities. When assigning individual users to the pre-defined roles, management should assign roles such that each user will have the fewest privileges possible while being able to perform their required duties.

The advantage of least privilege is the reduced risk. When users' unnecessary privileges are eliminated, then any risks associated with those prevented actions are reduced or removed.

The concepts of need-to-know and least privilege are very similar and mostly reflect different points of view. Where need-to-know is focused on access to specific information, least privilege is concerned with access levels.

Separation of Duties

The literal definition of **separation of duties** is to take a duty or task and separate it so that two or more persons must be present in order to complete it. In popular culture, tasks that require separation of duties include:

- **Deployment of a nuclear weapon**. Two or more staff members are required to insert a key or type a password.
- **Opening a bank vault**. Two vault tellers each possess one-half of the combination to the vault.
- **Issuing an arrest warrant**. Law enforcement documents a probable cause to arrest an individual, which is signed by a judge.

The objective of separation of duties is to place the completion of a task into the hands of two or more separate individuals. This requires that the two (or more) cooperate in order to perform the task. Employing separation of duties reduces the likelihood that an improper task will be performed:

- **Inappropriate**. When completion of a task requires two or more persons, chances are better that one of the participants will call a halt to the task if there is some reason that the task should not be performed.
- **Fraud**. When completion of a task requires two or more persons, the risk of fraud against the organization is reduced. Where an employee working on his or her own may follow through on committing fraud or embezzlement against his employer, when two or more persons are involved the chances of them cooperating a carrying it out are reduced.

Examples of separation of duties in the realm of business and information security include:

- **Payments to third parties**. In an accounting department (and on the software application that is used to carry out its transactions), the process of making payments to third parties such as suppliers should be controlled by two or more individuals: one person should make a payment request, another should approve the request, and still another should print the check, and still another should sign the check. If there is any

reason that the payment should not be made, there are four people who will have an opportunity scrutinize the payment and ask questions about it.

- **Add a user account**. The creation of a user's computer account should not be done by a sole individual. Instead, the end-to-end process should consist of an HR (human resources or personnel department) person creating a record of a new worker in the organization; another person (perhaps the worker's manager) should request the creation of the user account for the worker, and a third person should create the user account.
- **Add an administrator account**. The creation of a computer or network account that includes administrative privileges should go through at least one additional layer of approval than an ordinary user account. This additional approval could be the approval of a senior manager or executive.
- **Change a firewall rule**. Any change in a firewall rule (which controls network access between networks) should be controlled by two or more persons. This can not only reduce mistakes but also decrease the chances that a network administrator will act inappropriately.
- **Create an encryption key**. The creation of an encryption key should require two or more persons. The concept of **split custody** is a special case of separation of duties where two persons each possess one half of a password to an encryption key, which requires these two individuals' involvement in any activities related to the key.
- **Respond to a security alert**. A system that monitors computers and networks for performance and security purposes should send all of its security alerts to at least two individuals. This would reduce the likelihood that the single individual who monitors security alerts would carry out some inappropriate action that would create such an alert. A person working on his own could cover up the action or claim that it was a false alarm, but when two or more people receive such alerts, someone intent on performing an inappropriate action might be dissuaded from carrying it out.

An organization probably has many more activities that should be designed so that they require two or more individuals to carry them out.

Job Rotation

The practice of moving individual workers through a range of assignments over time is known as job rotation. This practice adds value to the organization by exposing employees to a wider variety of activities, providing additional opportunities for excellence and reducing monotony and boredom.

Job rotation also reduces risk by moving people out of specific tasks. An employee who is performing inappropriate or illegal actions would be less likely to do so if she knew that she would be rotated out of that task and be caught, especially if these changes are made with little or no notice.

Monitoring of Special Privileges

In most environments, administrative-level privileges give the administrator the ability to perform many powerful functions. In some cases, these functions permit the administrator to directly alter business information instead of altering it through the software application that other personnel must use. Also, because administrators' capabilities are greater than most

other users, a mistake can be far more costly, resulting in a partial or complete loss or corruption of data, or more subtle errors that may not be immediately obvious.

For this reason it is especially important for an organization to implement controls to monitor actions carried out by administrators. These controls need to record the activities of the following functions:

- **Network Administrator**. Changes to routers, firewalls, intrusion detection systems, spam filters, switches, and VLANs.
- **System Administrator**. Changes to OS configuration, performance, and security settings; installation of upgrades, software patches, device drivers; changes to user accounts, and authentication rules.
- **Database Administrator**. Changes to DBMS configuration and security settings, changes to application data, triggers, and stored procedures.
- **Application Administrator**. Changes to application configuration, security settings, roles, user role changes, application data.

The reasons for monitoring these functions include:

- **Accountability**. Administrators must be held accountable for their actions; they should have nothing to hide nor have any objection to the practice of logging their actions.
- **Audit logging**. Laws and regulations require that the types of changes made by administrators be logged, to support the management integrity of a supporting environment.
- **Troubleshooting**. If an outage or other problem occurs, administrators can review recent actions, changes, and activities that could provide valuable clues during the troubleshooting effort.

Records Management Controls

Business records are the information that is produced in support of business operations. Business records will consist of many types of information including:

- Management records
  - Policy documents
  - Memos
- Legal records
  - Contracts
- Personnel records
  - Applications
  - Performance reviews
- Operational records
  - Process and procedures
  - Transactions

Admittedly I'm just scratching the surface with the above list. Organizations create an enormous amount of information in these categories, and then some. Most of the data that exists

on information systems is never printed, so the vastness of this information may not be readily apparent, and the true extent will be known by few.

In the context of information security, several activities are vital for records management including:

- **Data classification**. Establishing sensitivity levels and handling procedures.
- **Access management**. Choosing who may access information.
- **Records retention**. How long information must be kept.
- **Backups**. Making sure information is not lost due to a failure or malfunction.
- **Data destruction**. How information must be safely discarded when no longer needed.

Data Classification Organizations will have many different sets of information that will vary widely in their sensitivity. The different levels of sensitivity will call for different procedures for protecting, storing, transmitting, storing, and discarding information.

While an information security department can prescribe safeguards on a case-by-case basis, it is far more effective to establish a schedule of three to five (or more) predefined levels of sensitivity, each with specific procedures for creation, storage, transmitting, destruction, and so forth. A typical schedule would be a chart of columns of sensitivity and rows of procedures.

Chapter 1, "Information Security and Risk Management," explores data classification in more detail.

Access Management Access management refers to the policies, procedures, and controls that determine how information is accessed and by whom. All business information should be housed in a location (physical or logical) that provides a level of access control that is commensurate with its sensitivity (as discussed in the previous section).

An organization that wishes to implement access controls must first develop an access control policy that consists of several components including:

- **User account provisioning**. Policy needs to specify the person or group that provisions user accounts, as well as the process used to assign computer accounts to users.
- **Privilege management**. Policy needs to define which persons may be given privileged (administrative) access, and how the request and approval process should work.
- **Password management**. Policy needs to define how passwords are stored (encrypted, hopefully!) as well as rules about assignment, complexity, expiration, and so on.
- **Review of access rights**. Policy needs to define who and how often user access rights will be reviewed, and the steps followed if exceptions are found.
- **Secure log on**. Policy needs to define whether (and how) a computer log-on needs to be secured (hopefully by encryption so that eavesdroppers cannot harvest credentials).

The above-mentioned policies then need to be operationalized, meaning that processes and procedures need to also be developed that describe step-by-step how the policies are to be carried out.

The policies and procedures described here need to be applied not only to computers and networks that contain business records, but also in the physical sense, since an organization

also has paper records that must be protected. The sensitivity of paper records may also require formal access controls in the form of locked rooms, locking cabinets, safes, or vaults.

Record Retention Organizations collect and maintain business records on paper and electronically. Organizations need to develop policies that specify how long different types of records must be retained. A typical way to implement this is to develop a high level policy that states that business records must be kept for certain periods of time, according to a schedule that lists different types of records and their minimum and maximum retention periods.

The types of records that may be included in a records retention schedule are:

- Payroll records
- Personnel records
- Financial records
- Legal contracts
- E-mail
- Audit reports
- Audit logs from applications

The above listed categories are very general; chances are an organization's retention schedule will be more granular. For instance, in a Human Resources department, employee files might be kept for one period of time, while resumes from applicants might be kept for a shorter interval.

Organizations are establishing records retention policies and schedules in order to manage risks including:

- **Risk of compromise of sensitive information**. The longer an organization keeps credit card transactions, for instance, the greater the impact if that set of data is compromised. Statistically speaking, if a company changes the retention of credit card transactions from eight years to two years, then it has reduced the impact of exposure by 75 percent.
- **Risk of loss of important information**. The flip-side of the risk of compromise is the risk associated with situations where needed information is no longer available. Without clear direction on the minimum period of time that certain information needs to be retained, well meaning employees might discard information too soon, which could deprive the organization of the value that the discarded information would otherwise have provided.
- **E-Discovery**. If an organization keeps information longer than is really necessary, then a discovery or e-discovery process can take longer, increasing costs and potentially revealing additional information.
- **Regulation**. Various laws and regulations require that certain business records be kept for minimum—or maximum—periods of time.

Another important reason for establishing a retention policy is to reduce the cost of maintaining data for periods of time that exceed the true need. If a given set of paper records needs to be kept for only five years, for example, then the organization would be unnecessarily consuming resources such as floor space to keep those records for ten years.

The organization needs to ensure that its records retention schedule is in compliance with applicable laws or regulations.

Backups Information that is worth acquiring and maintaining on a system is generally worth retaining. Information equipment can be prone to failure, resulting in the irretrievable loss of valuable information. For this reason (and others), it is important to make frequent backup copies of information, in the event an accidental loss occurs. **Backup** is the process of copying important information from a computer or storage system to another device for recovery or archival purposes. The causes for information loss include:

- **Equipment malfunctions**. Data storage devices rely on electronic, optical, and/or mechanical technologies that are prone to breakdown, and they just wear out.
- **Software bugs**. Mistakes in coding and configuration can result in accidental changes in, or erasure of, information.
- **Human error**. A wide range of man-caused errors can result in damaged or destroyed information.
- **Disasters**. Fires, floods, hurricanes, and many other types of natural and man-made disasters can damage or destroy computer equipment and stored information.

Data Restoration Backup copies of valuable information should be maintained in case any of these events occur. When data is lost or damaged, backup copies of the data can be copied from the backup media back into the system. This is called a **restore** operation.

It is recommended that a computer operations group periodically test the ability to restore data from backup media. This is really the only way to prove that good backups are being performed in the first place.

Protection of Backup Media Backup media that contain copies of business information need to be given the same level of physical and logical protection that the original data receives. This includes physical controls such as locked doors, surveillance cameras, and visitor logs. Accurate records also need to be kept on backup media so that personnel can restore business information: if a particular file or database needs to be recovered, operators must know which volumes contain the specific information. Records will indicate the location of each volume.

Generally, backup media should be kept in locked cabinets in or near the systems containing the original information so that data can be quickly restored when needed. Only those personnel with a specific need to access media should have access to those cabinets.

Offsite Storage of Backup Media Copying important information to backup media is a necessary safeguard that protects the organization against losses due to equipment failures and human errors. However, since backup media is usually located close to the equipment that stores the original information, that backup media (as well as the original equipment) is at risk of destruction in the event of a disaster. For this reason, it is necessary to locate backup media far away from the original location.

This practice is known as **off-site storage**. Because of the sensitivity of business information on backup media, the backup media needs to be protected, during transit as well as during storage. Factors to consider when searching for a suitable offsite storage facility include:

- **Distance from business location**. The offsite storage facility should not be so close to the main business location that both become involved in a regional disaster such as a

flood. However, it should not be located so far away that the time required to retrieve media would be unacceptably long.

- **Security of transportation**. The mode and security of transportation between the organization and the offsite storage facility should be proportional to the value of the data in transit.
- **Security of storage center**. The facility should also have good records management controls so that it handles stored information properly.
- **Resilience against disasters**. The offsite storage facility should have robust physical controls to ensure the safety of the facility and stored records from events such as earthquakes, fires, and floods.

Data Destruction A **records retention** policy specifies how long business records need to be kept in an organization. When it's time to discard information, a data destruction policy should be in place to instruct employees how to properly discard the information.

The primary purpose of a data destruction policy is to ensure that discarded information is truly destroyed and not salvageable by either employees or outsiders. Information being discarded is of varying levels of sensitivity, according to a data classification or data sensitivity policy. Once information has reached the end of its need, its destruction needs to be carried out in a manner that is proportional to its sensitivity.

Examples of methods available to destroy information include:

- **Degaussing**. Applies to magnetic-based media such as hard drives and backup tapes. **Degaussing** is a process of erasing the data on magnetic media by exerting a strong magnetic field that effectively erases any stored data.
- **Shredding**. Applies to paper records as well as some electronic media such as CD/DVD-ROM, floppy disc, and backup tape.
- **Wiping**. Applies to files on magnetic-based media such as hard drives.

Often, evidence of data destruction needs to be produced, to provide a record of the details of the destruction, including who performed it, when it was performed, and what methods or equipment were used.

Anti-Virus and Anti-Malware

Every organization needs to assess the risk of exposure to and infection by malicious code (also known as malware) such as viruses, worms, Trojan horses, and spyware, and then respond to the risk by implementing anti-virus and anti-spyware controls. Anti-virus software is used to detect and remove malicious code including computer viruses. Similarly, anti-spyware detects and removes spyware.

Malware has the capacity to disrupt the operation of user workstations as well as servers, which could result in:

- Loss of business information
- Disclosure or compromise of business information
- Corruption of business information
- Disruption of business information processing

- Inability to access business information
- Loss of productivity

Applying Defense-In-Depth Malware Protection The problem of malware is so pervasive that nearly every organization that uses computers uses anti-virus software to protect them against the effects of malware. But more than that, many organizations apply a defense-in-depth malware protection strategy that could include one or more of the following controls:

- Anti-malware software on user workstations
- Firewall software on user workstations
- Anti-malware software on e-mail servers
- Anti-malware software on file servers
- Anti-malware appliances
- Anti-malware Web proxy servers
- Firewalls on network boundaries
- Spam filter appliances
- Spam filters in e-mail servers

Central Anti-Malware Management In all but the very smallest organizations, anti-malware software is usually controlled or managed through a central console. An enterprise edition of anti-malware usually includes console management that permits the following capabilities:

- Centralized configuration control
- Centralized control over workstation anti-malware activities such as immediate scans or updates, or workstation firewall configuration changes
- Centralized reporting of malware infections
- Centralized view of which systems have working anti-malware software

Remote Access

Remote access is the broad term that signifies the connectivity to a network or system from a location away from the network or system, usually from a location apart from the organization's premises. Such access usually requires the use of a public network—either a dial-up over voice or ISDN service, or a connection over the public Internet.

Remote access often provides a remote employee with connectivity to most or all internal network resources *as though* he were physically on the internal network. Because internal networks often employ private (non-routable) addresses, a tunneling technology will be used. Often, because of the sensitivity of business information being accessed, the connection will be encrypted to prevent disclosure of business information to anyone who may be eavesdropping on the connection. The technology commonly used to satisfy these requirements is known as **Virtual Private Network**, or **VPN**. In fact, VPN is in such wide use for remote access that VPN is often the term used to describe remote access.

Risks and Remote Access While the technology behind VPN is fairly straightforward and commonplace, several risks associated with the management and operation of VPNs require sound processes and controls including:

- **Remote client security**. Because a client workstation that connects to an organization's network via VPN is functionally a node on the enterprise network, several measures need to be taken to ensure that the remote workstation does not increase risk. Some of the measures include:
  - **Anti-virus software**. Because the remote client workstation will be connected to the Internet without the protection of other organization anti-virus controls, it is especially important that anti-virus software on remote client workstations be active and functioning properly.
  - **Anti-spyware software**. The remote client workstation should have anti-spyware software in order to prevent spyware and other even riskier software such as key loggers.
  - **Firewall software**. Because the remote client workstation will often be connected to the Internet without the protection of the corporate firewall, remote client workstations should have their own firewall software installed and operating. Firewall software will reduce the risk of network-borne attacks from penetrating and infecting remote client workstations.
  - **Split tunneling**. Some VPN software can be configured to permit a "split tunnel," whereby all access to the organization's network passes through the VPN, while all other Internet access bypasses the VPN tunnel. The main disadvantage of a split tunnel is that the remote workstation is not protected by enterprise network safeguards such as firewalls and anti-malware. Organizations that need to rely on enterprise network safeguards to protect remote workstations should forbid split tunnels. Figure 7-1 shows split tunneling.
- **Remote client policy**. The risks associated with remote client security compel many organizations to permit only its own managed client workstations to connect via VPN

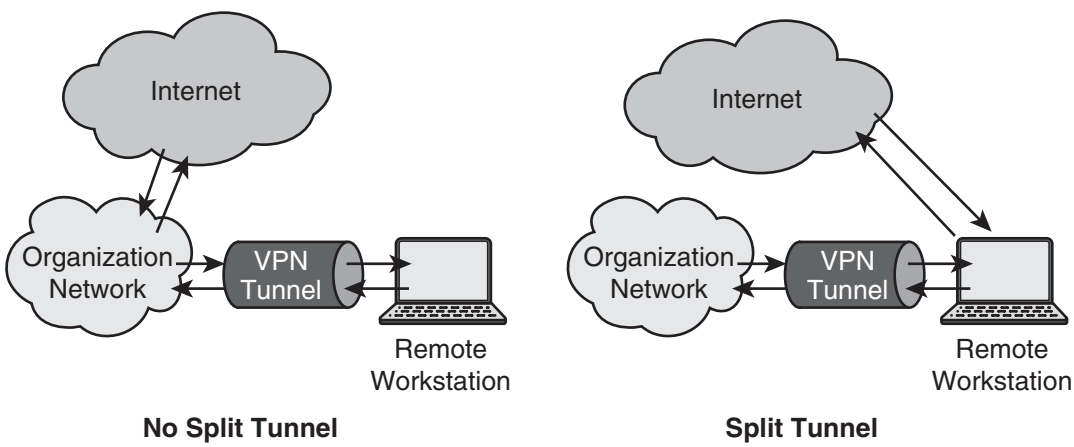


Figure 7-1 Remote access split tunneling

Source: Course Technology/Cengage Learning

to the organization's network. While this may seem an imposition, the alternatives are even more challenging:

- Managing firewall, anti-virus, and anti-spyware on non-company-owned systems will be exceedingly more difficult and labor intensive.
- Permitting non-company owned systems to connect to the network via VPN and also store company documents causes the organization to give up a measure of control over its intellectual property and blurs the lines of control and ownership.

These factors often result in organizations permitting only its own systems to connect to the network via VPN, forbidding *non*-company owned systems from connecting.

Administrative Management and Control

All of the activities that are related to the protection of assets must be controlled by company management in a formal manner that facilitates true management control and oversight.

A model that is gaining wide international acceptance for top-down security management is ISO 27001, which prescribes the establishment of an Information Security Management System (ISMS). The cornerstone to an effective security program is management oversight through the following activities:

- **Define the scope and boundaries of security management.** Management decides what portions of the business are subject to security policy and controls. All exclusions must be documented.
- **Establish and approve a security policy.** This is the top-level document that defines acceptable and unacceptable behaviors and characteristics in the organization.
- **Define the approach for risk assessment.** This is the process and procedures for identifying and documenting risks.
- **Identify, evaluate, and address risks.** When risks are identified, a consistent approach to evaluation and mitigation is needed. In a broad sense, addressing risk could mean mitigation, transfer, or acceptance of risk.
- **Establish control objectives and control activities.** The primary control objectives make broad statements about how security policy will be implemented. Control activities go into greater detail and specify how control objectives are to be carried out.
- **Establish a security training and awareness program.** All personnel need to be aware of risks, controls, and safeguards and develop good judgment, which is all established through security awareness training.
- **Allocate resources.** Once control objectives, risk assessments, and security awareness programs are established, management allocates resources so that these activities can be regularly carried out.
- **Perform internal audits.** Regular verification of proper performance of controls and adherence to policies must be performed.
- **Monitor and review the security program.** Key performance indicators must be established so that management can measure how security is performing in the organization over time. Events and issues are regularly reviewed by senior management.

- **Enact continual improvement.** Whenever deficiencies are identified, improvements must be identified and implemented, in order to gradually improve the risk position of the organization.

Types and Categories of Controls

Earlier in this section I discussed the need to establish control objectives and control activities. A **control** is a designated process (or a part of a process) that is key to the objectives of an organization. Control activities are often called controls; there are three types of controls and six categories of controls.

The types of controls are:

- Technical
- Physical
- Administrative

The categories of controls are:

- Detective
- Deterrent
- Preventive
- Corrective
- Recovery
- Compensating

The typing and categorization of controls is used to better understand a control framework and how controls support policy and mitigate risk. The types and categories of controls are discussed in detail in Chapter 2, "Access Controls."

Employing Resource Protection

Business resources are used to support daily business operations, enabling the business to produce the goods and/or services that it delivers to its customers. These resources consist of:

- Facilities
- Hardware
- Software
- Documentation
- Records (covered in the earlier section, "Records management controls")

Resource protection is the set of activities enacted to protect these business resources.

Facilities

Facilities are the buildings and other structures that house the space where people work and the equipment that they use. Besides the structure itself, a facility has several systems that are integral to its operation including:

- Water and sewage.
- **Electricity.** If sensitive equipment such as computers or networks is in use, then electricity needs to be conditioned and protected against spikes, brownouts, and

complete failures with power conditioners, uninterruptible power supplies (UPSs), and electric generators.

- **Fire alarms and suppression**. This will consist of smoke, heat, and fire detectors, pull stations, fire extinguishers, sprinkler systems, alarms, and possibly communications to a fire department.
- **Environmental controls**. This includes heating, ventilation, and air conditioning (HVAC).
- **Communications**. Phone and data connections that support voice and data communications needs.
- **Security controls**. This will include locking doors and may also include fencing, gates, keycard systems, and video surveillance.

Each of these requires some schedule of maintenance and inspection—some by outside authorities.

Hardware

Hardware is the inclusive term to signify many types of computing and ancillary equipment that support information processing and storage. The types of hardware that protect—and also require protection—include:

- **Workstations**. Known also as end-user workstations, PCs, or personal computers, workstations are located in offices and other workspaces. In many settings they must be protected from theft, restrained usually be locking cables or brackets.
- **Servers**. These are the beefier computers that store and process information for the organization. They are usually located in special higher-security rooms equipped with special environmental controls to control heat and humidity. Servers need to be protected from theft but more importantly from unauthorized access, and this is usually accomplished through locking doors, keycard controls, and video surveillance.
- **Consoles**. Usually found in server rooms, consoles resemble workstations (and sometimes they *are* workstations). Like servers, they need to be protected from unauthorized access as well as theft.
- **Network devices**. These are the **routers**, **hubs**, **switches**, VPN servers, security appliances, intrusion detection systems, and other devices that permit and control the flow of information within the organization, and between the organization and entities in the outside world. Like servers, they need to be protected from unauthorized access and are usually located in server rooms that have specially designed environmental and security controls. Network devices also protect the organization's information and systems in a variety of ways:
  - **Firewalls** protect the network from unwanted traffic from the Internet and from other external organizations. Firewalls are configured with "rules" that specify exactly what types of traffic are permitted to enter (and leave) the organization's network, as well as which devices and systems the traffic is permitted to travel to and from.

  - **Routers** connect different networks together and can also control network traffic similar to a firewall's traffic-limiting capability.
  - **Switches** transmit network traffic among different devices (which includes workstations, printer, and servers) in a network, as well as to and from routers in the case of traffic to and from other networks.
  - **VPN servers** provide safe remote access for off-site employees who need to access resources within the network. VPN servers authenticate users and then encrypt all traffic to prevent any eavesdroppers from viewing company secrets.
  - **Security appliances** perform a variety of tasks including filtering web site content (protecting employees from malware, and also blocking access to non-business-related sites) and spam.
- **Wireless networks**. These let an employee roam around the office with a laptop and stay connected to network resources without having to find a cable to plug into. Wireless networks use radio waves, which can leak outside of the building, permitting people outside the physical perimeter to also eavesdrop on the company's network. Wireless networks can be protected with encryption using **WEP** (**Wired Equivalent Privacy**) or **WPA** (**Wi-Fi Protected Access**), which both employ secret keys and can also require a user to provide a userid and password. The WEP encryption protocol is no longer considered secure, and organizations are urged to use WPA instead.
- **Printers and copiers**. Printers are often connected directly to the corporate network, which allows employees to print to most any printer from anyplace. Because some printed information is sensitive, users are urged to pick up their printouts as soon as possible. Copiers are increasingly being connected to the network, which permits users to print multiple copies of reports and also perform tasks like collating and stapling.
- **Cabling**. Network cabling carries the communications throughout the organization's network, and also between the organization and outside entities such as partners and suppliers and the global Internet. Cabling needs to be protected from physical access to prevent tampering, damage, and eavesdropping through "vampire taps" and other techniques that can be used to try and listen to network communications. Vampire taps are discussed in Chapter 10, "Telecommunications and Network Security."

Software

Every organization that uses computers has **software** that it has purchased, and possibly software that it has developed. The Windows and UNIX operating systems are software, as are relational databases (like Oracle or Microsoft SQL Server), web servers (Apache, Web Logic or Microsoft IIS) and applications.

An organization needs to control and manage its software in many respects, including:

- **Licensing**. Organizations need to track how many copies of software they have installed and are using; many software companies collect license fees based upon the number of computers that are running the software, and also (sometimes) on the size of the computers (number of CPUs or amount of memory) that licensed software is running on.
- **Access control**. In order to remain in compliance with any licensing agreements (and to protect the intellectual property aspect of software from disclosure to unauthorized

parties), access to software must be controlled. Often this is accomplished by using the same controls that are used to control access to data.

- **Source code**. For the software that the organization develops and maintains on its own, source code needs to be protected from unauthorized disclosure. There are a number of reasons for this including:
  - **Intellectual property**. Source code may be an organization's intellectual property that it wishes to keep closely guarded.
  - **Security**. Sometimes the security of a program is compromised if someone is able to read its source code and discover how the software is used to protect information.
- **Source Code Control**. As part of its **software development life cycle** (**SDLC**), an organization needs to keep strict controls over the software that it develops, integrates, and maintains. Source code control is used to control which developers are able to access what parts of software, and also keep track of changes and versions of software. The software development life cycle is discussed in detail in Chapter 3, "Application Security."

Documentation

Processes, procedures, instructions, diagrams, charts, and tables are all **documentation** that describes how an organization is organized, how it was built, and how it is operated and maintained. Documentation is an organization's "owner's manual" and blueprints that its employees refer to in order to better understand how to do their tasks properly.

An organization's documentation must be properly managed, in order to preserve the integrity of each document as well as "look-and-feel" consistency among documents that makes them more easily understood. Each document should have a "home" where its official "source" is kept. Ideally it will reside on a server that is regularly backed up, to preserve documents even when a disaster occurs.

Documentation must also be protected from disclosure to unauthorized parties. While most documentation needs to be protected from disclosure to outside parties, some documentation is sensitive enough that access to it must be restricted to just the few people who really need it.

Documentation is just one aspect of an organization's records. A more detailed discussion on the management of records is found earlier in this chapter in the section, "Records management controls."

Incident Management

Strictly speaking, an incident is an unexpected event that results in an interruption of normal operations. In ITIL (IT Infrastructure Library) terms, an incident is *an event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service*.

In the context of security, a **security incident** is an event in which some aspect of an organization's security policy has been violated. But another way to view a security incident is to

describe it as an unauthorized access to a system or information, or an event that prevents legitimate access to a system or information.

A security incident nearly always has a human root cause. This is true if the security incident is the result of malware (which is written by humans) or a targeted breakin by an intruder. Regardless, the response to a security incident should be organized and systematic and generally consists of the following steps:

- Incident declaration
- Triage
- Investigation
- Analysis
- Containment
- Recovery
- Debriefing

These steps should be documented in the form of written procedures, which should be reviewed from time to time to ensure their continued accuracy and relevance. Personnel who will be expected to respond in the event of a security incident should be trained, in order to better prepare them for response.

Security incident response is discussed in greater detail in Chapter 6, "Legal, Regulations, Compliance, and Investigations."

High Availability Architectures

Information systems and applications are vital to organizations and their customers, so much so that in many cases extra steps need to be taken to ensure their continuous availability.

Well organized computer operations departments can develop quite a good record of application uptime, but in order to keep systems running smoothly, period maintenance is required for the installation of patches, software updates, hardware upgrades, and so on. And, unexpected failures do sometimes occur, seemingly at the most inopportune times. These predictable and unpredictable occurrences often drive an organization to develop a more resilient architecture than is achievable with standalone servers and other equipment. Options available include:

- Fault tolerance
- Clusters
- Failover
- Replication

These aspects can give an application architecture the resilience it needs to achieve the high availability that the organization and its customers require. Usually, a resilient architecture seeks to avoid a **single point of failure**, a characteristic of an environment where a single component failure will cause an entire system or application to fail. Often, a component in a system that has no backup or alternative path is considered a single point of failure—even if it is

unlikely that the component will actually fail. Figure 1-2 in Chapter 1, "Information Security and Risk Management," illustrates the concept of a single point of failure.

Fault Tolerance

Fault tolerance refers to the design of a device whereby is failure-prone components are duplicated, so that the failure of one component will not result in the failure of the entire device. Some examples of fault tolerant devices include:

- **Multiple power supplies**. A server or device that has two or more removable power supplies may be considered fault tolerant, especially if a faulty power supply will not cause failure of the device and that the faulty power supply can be replaced while the system continues to operate.
- **Multiple network interfaces**. Servers and network devices may have multiple network interfaces in the event that one of them fails. While the system or device may not permit the replacement of the network interface while the system is operating, it still could be considered fault tolerant if the system can continue operating with one less network interface until the next regularly scheduled maintenance window.
- **Multiple processor units**. Some servers and network devices are designed to house multiple processor units, and may even permit a "hot replacement" of a faulty unit while the system continues to operate.
- **RAID** (**Redundant Array of Inexpensive Disks**, but sometimes referred to as Redundant Array of Independent Disks). Servers and disk storage systems often use RAID-5, RAID-6, or RAID-10 architectures, which are the most common types of multiple-disk architecture in a storage system or server. RAID permits a storage system to continue operating—without data loss or interruption—in the event that a single disk drive in the system fails. RAID systems further usually permit the "hot replacement" of a faulty drive while the system continues to operate.

Fault tolerance can also refer to an architecture that utilizes redundant components that permits the whole system to continue operating should one of the systems or devices in the system fails. Figure 1-2 in Chapter 1, "Information Security and Risk Management," shows an architecture where most of its components have counterparts that permit the entire system to keep functioning even if one of the components fails.

Clusters

A cluster refers to a group of two or more servers that operate functionally as a single logical server, and will continue operating in the event that one of the servers fails.

Clusters generally operate in one of two modes: active-active or active-passive. In **active-active** mode, both servers (or all three or four if the cluster is that large) actively operate and service incoming requests. In **active-passive** mode, one (or more) server actively services requests, and one (or more) servers remains in a standby state but is ready at a moment's notice to switch to active mode should one of the active servers in the cluster fail. In active-passive mode, servers change state automatically through a process called a failover.

Systems in a cluster need not be located near each other. Instead, they can be next to each other or halfway around the world from each other in what is called a **geographical cluster** or *geo-cluster*.

Failover

A **failover** is an event in a server cluster running in active-passive mode, where an active server has failed and a passive server is switching to active mode. This permits requests for service to be continuously serviced, with little or no interruption from the point of view of the systems requesting service.

A failover can be likened to a highway toll plaza, where one toll booth will close but another one will immediately open, which permits the continuous servicing of cars paying tolls.

Replication

Replication is an operation concerning the data on a storage system, where additions and changes to the data are transmitted to a counterpart storage system where the same additions and changes take place. It is said that changes to the data on one storage system are *replicated* to a counterpart storage system.

Replication often takes place under the control of the operating system, database management system, or the hardware storage system. This means that an application will require little or no changes in order to establish replication, making replication far easier to implement.

Replication is usually set up in conjunction with clustering. Clustering will manage the states of each of its member servers, controlling whether each is in active or passive mode. Alongside, replication will make sure that the most up-to-date data is available across all storage systems, so that any server that becomes an active server in a cluster will have access to current data. This is illustrated in Figure 7-2. Server 1 is the active server in a cluster, and its data is replicated from its Storage System 1 to its counterpart, Storage System 2. If a failure occurs anywhere in Server 1 or Storage System 1, then Server 2 can become the new active

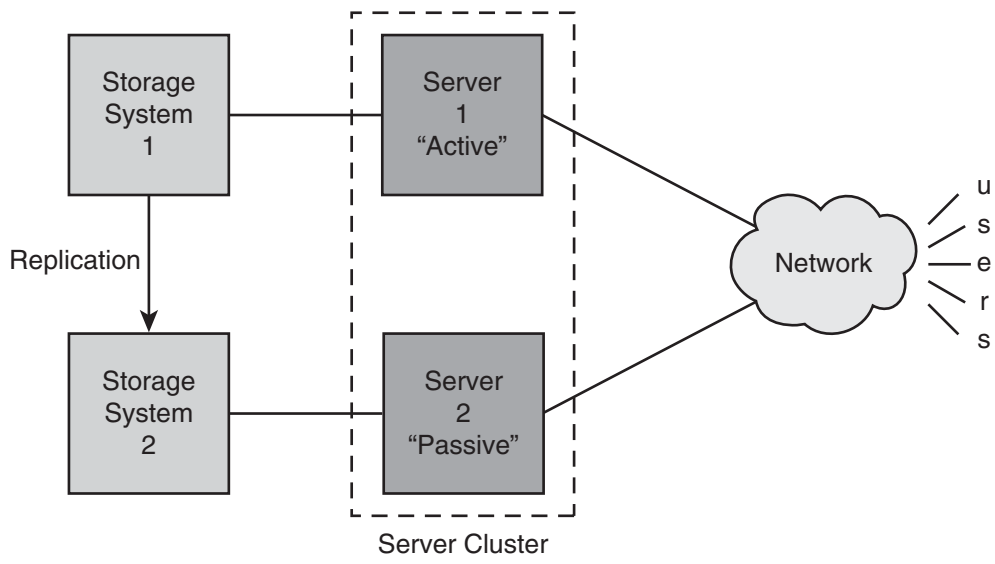


Figure 7-2 Clustering and replication working together to form a highly available architecture

Source: Course Technology/Cengage Learning

server (through a failover), and Server 2 will have up to date data because of the replication that was taking place from Storage System 1 to Storage System 2.

High-availability architectures are usually implemented in conjunction with, and as a result of, a risk analysis that is performed in a business continuity effort.

Business Continuity Management

A **business continuity plan** is the result of a management activity where analysis is performed to better understand the risks associated with potential disaster scenarios and the steps that can be taken to reduce the impact of a disaster should one occur. A common outcome of a business continuity project is the implementation of a high-resilience architecture that will permit critical business functions to continue operating even when a disaster strikes. Highly resilient architectures are discussed in the previous section, "High Availability Architectures," in this chapter.

Business continuity planning and disaster recovery planning are discussed in much detail in Chapter 4, "Business Continuity and Disaster Recovery Planning."

Vulnerability Management

The process of identifying vulnerabilities in a system and then acting to mitigate those vulnerabilities is known as **vulnerability management**.

Vulnerabilities result when a software program contains a weakness that, if exploited, could lead to the malfunction of the system or, worse yet, unauthorized disclosure of information contained in the system.

Vulnerabilities can be discovered in one of two basic ways: through passive means or through active means. Passive means includes receiving alerts of vulnerabilities from sources such as the components manufacturer or independent sources such as US-CERT of Secunia. Active means includes performing penetration testing scans or application vulnerability scans in an active effort to find vulnerabilities.

Penetration Testing

Penetration testing is a technique used that mimics the actions of a hacker who scans a system or network for active, exploitable ports and services. A tool can be used to probe an individual system or an entire network of systems, to look for open ports. When an open port is found, the penetration testing tool can send more probes in order to learn more about the open port, including whether it has any exploitable weaknesses that a hacker could exploit to gain unlawful entry to the system.

Better penetration testing tools will not only include details about the vulnerable port that it found, but also will include a severity ranking and information about how the vulnerability can be fixed—whether through the application of a security patch or a change in configuration. The severity ranking can be used to decide how urgently a patch or other fix should be applied.

A proper vulnerability management process will also include detailed recordkeeping on the scans performed, vulnerabilities identified, and also details on how the vulnerability was fixed and by whom. These records can be used to measure the amount of effort that is being expended over time to keep systems at an acceptably safe level.

Application Scanning

Application scanning is the process of performing security tests on an application (usually, but not always, a web-based application) in order to find vulnerabilities in the application code itself. Application scanning is like penetration testing in that a tool or technique is used to discover vulnerabilities in a system. But where application scanning and penetration testing differ is the target of the testing: penetration testing examines the operating system and other major components such as database server or web server, whereas application scanning concentrates its testing only on an application.

The tools used to perform penetration scanning and application scanning are usually different. While a single tool could perform both kinds of tests, generally these tools are written to do just one type of testing and not the other. The audience is usually different, too. The results of penetration tests will be system administrators who will make configuration changes or apply operating system security patches, whereas the results of application scans will be of interest to application developers who will make changes in the source code of the target application.

Application scanning tools most often are used to assess the security of web-based applications, to ensure that the application's developers have written the application to be robust enough to avoid any of the common pitfalls including:

- Cross-site scripting
- Cross-site request forgery
- SQL injection
- Script injection
- Parameter tampering
- Buffer overflow
- Boundary checking
- Defective or unsecure session management
- Defective or unsecure logon
- Malicious file execution

Patch Management

Patch management is a process—usually assisted with a management tool—to manage the installation of patches on target systems. Generally, a patch management tool will have the ability to scan systems (for instance, the servers or end user workstations) to determine the existence of operating system and software patches. Generally the same tool has the ability to also remotely install selected patches on target systems.

Patch management tools are generally considered to be time savers by making a labor-intensive task (installing patches on hundreds or thousands of systems) far more automated. However, it is considered unwise to simply "spray and pray" by installing all possible patches on all systems, because the indiscriminate installation of patches can introduce subtle performance or stability problems, not to mention consuming resources (the "undo" information for each patch) and incurring more downtime. Rather, it is recommended that skilled analysts perform a risk analysis on each applicable patch and make an informed risk-based decision on whether each available patch should be installed (and, if so, after how much testing). Many respected voices in the security industry (including the author of this book) urge organizations to *not* install patches by default but instead install each patch only as specifically needed.

Change Management

Change management is the name of a management process whereby each proposed change in an environment is formally planned and reviewed by peers and stakeholders, prior to the change being made.

The object of change management is the improvement in stability and the reduction of unscheduled downtime in an environment. When stakeholders are given the time to review a proposed change, they have an opportunity to identify issues that could adversely impact the environment. For instance, a system administrator wishes to make changes to certain security settings on database servers. But a database administrator, when she reviews the proposed change, identifies a problem that could result in a malfunction in the database. As a result, the system administrator takes another approach and proposes an alternative change that will not affect the database.

The steps in a simple change management process are:

1. **Prepare the change**. The proposed change should include: a) the procedure for making the change; b) the time the change will be made; c) how the change will be verified; d) how the change will be backed out if it fails; e) whether there will be downtime associated with the change; and f) test plans and results.
2. **Circulate and review the change**. The proposed change is circulated to a set of stakeholders and subject matter experts who will review the change.
3. **Discuss and agree to the change**. All of the stakeholders, usually in a formal meeting, will meet to discuss the proposed change. Concerned parties can ask questions of the person proposing the change. The team can agree to permit the change to be made, or request that the change be altered and re-presented at a later time.
4. **Perform the change**. Those personnel who are designated to make the change do so according to the procedure in the proposed change. After verifying that the change is complete and correct, they can close the change. If the change encountered any problems, it can be re-attempted or backed out.

The primary principle of change management is: only approved changes are made to an environment. No unapproved changes are made.

In the event of an emergency, the organization can establish a procedure for making emergency changes (usually through an incident management process), and then review the emergency change at the next regular change management meeting.

Configuration Management

Configuration management is the process of recording configuration changes that are made in an environment. In all but the simplest environments, configuration management is enabled through the use of a configuration management tool that is used to record, manage, and capture changes automatically and store them in a **configuration management database (CMDB)**. Without such a tool, it can be exceedingly difficult to keep the configurations of supposedly-identical systems in sync.

Configuration management is often used in conjunction with change management, as the means of implementing and recording approved changes to systems. Configuration management tools that are able to detect changes in a system can also be used to detect changes that were not authorized through the change management process.

Operations Attacks and Countermeasures

An attack on operations is primarily an attack on processes and controls. The targets of attacks may be personnel, records, or information systems. This section discusses some of these attacks and the countermeasures that reduce their likelihood or impact.

Social Engineering

Social engineering is a person-to-person attack where an individual is attempting to cause a staff member to do something improper, such as provide sensitive information to an untrusted third party or allow a stranger to enter a secure facility.

The primary countermeasure to social engineering is education and training, so that personnel are better prepared to recognize a social engineering attack and respond appropriately to it.

Social engineering is discussed in detail in Chapter 2, "Access Controls."

Sabotage

An insider or outsider may attack an organization's security operations by attempting to alter or destroy an information system that supports operations. Such an attack, for instance, may be an attempt to destroy records that provide evidence of unauthorized action, or the deliberate destruction of backup tapes. "Accidental errors" on the part of disgruntled employees can fall into this category as well.

Effective countermeasures include controls to protect systems and records from unauthorized access and alteration. These controls will typically consist of access controls (discussed in Chapter 2, "Access Controls."), cryptography (discussed in Chapter 5, "Cryptography"), and physical controls (see Chapter 8, "Physical and Environmental Security").

Theft and Disappearance

Stealing equipment and media is a certain and effective attack on operations. Employees schlep laptops and portable media such as thumb drives everywhere, and thousands are lost and stolen every month in the United States alone. Equipment is stolen from work locations with alarming regularity. There have even been some equipment heists from so-called "fortress" commercial data centers.

Several countermeasures are needed to curb theft and disappearance, including:

- Awareness training and safeguards such as cable locks for laptop users
- Video surveillance
- Restricted access to areas containing valuable equipment and media

Extortion

An individual might threaten to cause harm to information or information systems and coerce an organization to make payments of money or services in order to avoid the threatened harm. Recent examples in the context of information technology include:

- Perpetrator threatens to implant victim's computer with porn and other illegal content unless the victim makes a payment.
- Perpetrator encrypts victim's data files and will decrypt it for a fee.
- Perpetrator threatens to launch a Distributed Denial of Service (DDoS) attack unless victim organization makes a payment. Similarly, perpetrator launches the attack and requires payments in order to stop the attack.

Extortion countermeasures consist of controls that would thwart or repel the threatened attacks and actions.

Bypass

An individual may attempt to **bypass** security operations controls in order to be able to access or alter information, or to access a facility without authorization. This is known as a **bypass attack**.

Effective countermeasures consist of:

- Tests of operations controls to ensure that they are effective and that they are operating properly
- Enact a *defense-in-depth* control environment, so that the failure of one control is compensated by the existence of one or more other controls

Bypass is discussed in more detail in Chapter 2, "Access Controls."

Denial of Service

Denial of Service (DoS) attack is any type of attack that is designed to incapacitate its target, either through a sheer volume of stimulus (e.g., a flood of network traffic) or a specially crafted attack that causes the target's malfunction.

Generally a Denial of Service attack is a technical attack that is launched over a network, but a Denial of Service attack can also be an attack on people. Examples include a high volume of incoming phone calls, or a false fire alarm that results in building evacuation.

For technical systems, countermeasures against a Denial of Service attack include security patches to eliminate vulnerabilities, and increased capacity or other means for absorbing or shunting a network flooding attack. For personnel, countermeasures should include emergency procedures and training, and controls to ensure the continued protection of critical assets even during emergencies.

Chapter Summary

- The concept of *need-to-know* states that individual personnel should have access to only the information that they require in order to perform their stated duties.
- The concept of *least privilege* states that users should have the fewest or lowest numbers of privileges required to accomplish their duties.
- The concept of *separation of duties* states that high-value or high-risk tasks should be designed to require two or more individuals to complete it.
- The concept of *job rotation* moves individual workers through a range of assignments over time.
- The actions of individuals with special privileges should be monitored, to detect potential problems as well as to deter individual wrongdoing.
- Controls must be established that will manage the creation and use of business records.
- *Data classification* is the practice of assigning security levels and handling procedures to documents and databases.
- *Access management* is used to control who and what can access specific business records.
- *Records retention* governs the minimum and maximum periods of time that specific business records must be retained.
- *Backups* ensure the survival of business records even if malfunctions, errors, or disasters destroy original records.
- Backup media must itself be protected, to guard against unauthorized disclosure of records and to protect it from damage or loss.
- Data *destruction* is the process of securely discarding data when it is no longer needed.
- Malware has the capacity to disrupt the operation of user workstations as well as servers, which could result in loss or compromise of business information and the inability to access or process business information.
- Anti-*virus, anti-spyware*, and other anti-malware controls are used to prevent malware from entering the organization. Often a *defense in depth* strategy is used to ensure that malware cannot gain a foothold.

- Remote *access* equipment enables workers not on physical premises to access network-based resources such as file servers, applications, and internal web sites. Technology such as *VPN* encrypts remote access communications to prevent business information from compromise or disclosure.
- The activities that are related to the protection of assets must be controlled by company management, in a formal top-down manner that facilitates true management control and oversight.
- Management should establish security policies, control objectives, a risk assessment methodology, a security awareness program, direct internal audits, and strive for continuous improvement.
- The *types of controls* are technical, physical, and administrative.
- The *categories of controls* are detective, deterrent, preventive, corrective, recovery, and compensating.
- *Resource protection* ensures that the buildings, equipment, and systems used to operate the business are protected from harm, damage, or loss.
- *Facilities* protective measures include electric power conditioning, storage, and generation equipment to ensure the continuous supply of clean power; fire detection and prevention equipment; environmental controls to control temperature and humidity, and security controls to restrict access to sensitive areas.
- Hardware assets that need protection include workstations, servers, consoles, network devices, wireless networks, printers & copiers, and communications cabling.
- Organizations must protect their software to ensure compliance with license agreements and to control access to source code.
- Access to documentation must be restricted, and documentation needs to be protected from damage or loss.
- A *security incident* is an event in which some aspect of an organization's security policy has been violated.
- A *security incident response plan* is a process or procedure that is followed when a security incident occurs. The plan will usually include these steps: incident declaration, triage, investigation, analysis, containment, recovery, and debriefing.
- A *high availability architecture* is a system or application architecture that includes one or more of the following characteristics: fault tolerance, clusters, failover, and replication.
- *Fault tolerant* devices typically are equipped with redundant components that can be changed while the device continues operating.
- A *cluster* is a group of servers that logically functions as a single server, which will continue operating even if one of the servers in the cluster fails or is shut down for maintenance or repairs.
- A *failover* is an event that occurs in a cluster where the role of an *active* server is transitioned to another server in the cluster.
- *Business continuity planning* is an activity that is concerned with the continuation of critical business operations during and after a disaster.

- *Vulnerability management* is a collection of activities all concerned with the identification and remediation of vulnerabilities in an environment.
- *Penetration testing* is a vulnerability management activity that is used to identify active and exploitable ports and services on servers and network devices.
- *Application scanning* is a vulnerability management activity that is used to identify vulnerabilities in an application.
- *Patch management* is a vulnerability management activity that is used to identify important software patches and the systems and devices where they should be installed.
- *Change management* is an operations process where all changes in an environment are analyzed in a peer review process prior to implementation.
- Configuration management is an operations process where all changes to systems and components are recorded or controlled by a configuration management tool and recorded in a configuration management database (CMDB).

Key Terms

Access management The policies, procedures, and controls that determine how information is accessed and by whom.

Active-Active An operating mode in a cluster where all of the servers in the cluster actively operate and process incoming requests.

Active-Passive An operating mode in a cluster where one or more servers actively operate and process incoming requests and one or more servers remain in a standby mode.

Application scanning The task of identifying security vulnerabilities in an application.

Backup The process of copying important information from a computer or storage system to another device for recovery or archival purposes.

Business continuity plan A contingency plan that governs the business response to a disaster in order to keep critical business functions operating.

Bypass An attack that attempts to bypass security controls to access or alter information.

Change management The management process where proposed changes in an environment are formally planned and reviewed prior to implementing them.

Configuration management database (CMDB) A database containing the configuration settings of a system or environment.

Data destruction The process of discarding information that is no longer needed, in a manner that will render it irretrievable.

Degaussing The process of bulk-erasing magnetic-based storage media by imposing a strong magnetic field onto the media.

Documentation Processes, procedures, and even records, whether in paper or electronic form.

Facilities The buildings and other structures that house the space where people work and the equipment that they use.

Fault tolerance The design of a device or system where failure-prone components are duplicated, so that the failure of one component will not result in the failure of the entire device or system.

Geographical cluster A cluster whose members are dispersed over a wide geographic area.

Hardware computers and ancillary equipment that support information processing and storage.

Hub A device used to connect multiple computers together to form a network. A hub sends all packets on the network to all nodes. See also *switch*.

Need-to-know The access control concept where individual personnel should have access to only the information that they require in order to perform their stated duties.

Off-site storage The storage of storage media or paper documents at an off-site storage facility, to prevent against irrecoverable loss of information in the event of a disaster.

Records retention The determination of the minimum and/or maximum period of time that specific business records must be retained.

Redundant Array of Independent Discs (RAID) A disc storage technology that allows for greater reliability and performance in a disc-based storage system.

Remote access Any means used to connect to a target network from a remote location.

Resource protection Controls and procedures enacted to protect business resources including facilities, hardware, software, documentation, and records.

Restore The process of copying data from backup media to a system.

Router A network device that connects two or more networks together logically, and can also control the flow of traffic between networks according to a set of rules known as an Access Control List (ACL).

Segregation of duties *See separation of duties*.

Shredding The process of cutting paper, magnetic, or optical media into small pieces for the purpose of secure destruction.

Software Computer instructions that fulfill a stated purpose.

Split custody A control safeguard in which an important secret (such as a password) is broken into two or more parts, each of which is kept by different individuals.

Switch A network device used to connect multiple computers to form a network. A switch sends packets only to destination nodes. See also *hub*.

Vulnerability management The process of identifying vulnerabilities in a system and then acting to mitigate those vulnerabilities.

Wiping The process of destroying data stored on magnetic media by overwriting the media several times.

Wi-Fi Protected Access (WPA) A wireless network encryption protocol.

Review Questions

1. The concept of "need-to-know" states:
   a. Paths to data containing sensitive information should not be published
   b. Documents should be marked as "confidential" and distribution kept to a minimum
   c. Individual personnel should have access to only the information they require to perform their jobs
   d. Documents should be marked as "restricted" and distribution kept to a minimum

2. The process of periodically changing workers' assigned tasks is known as:
   a. Job rotation
   b. Cross-training
   c. Privilege rotation
   d. Separation of duties

3. The purpose of data classification is:
   a. Notify users that documents are subject to special handling procedures
   b. Notify users that they may be required to ask permission of a document's owner before sending it to another person
   c. Notify users that documents may be subject to restrictions when sending them via e-mail
   d. All of the above

4. Data retention standards specify:
   a. The minimum and maximum periods of time that specific types of data should be retained
   b. Procedures for retention of backup media
   c. Procedures for destruction of backup media
   d. Standards for archiving data that resides in databases

5. Data backups are performed:
   a. To protect critical data in the event of a disaster
   b. To protect critical data in the event of a hardware failure
   c. To protect critical data in the event of a disaster, hardware failure, or data corruption
   d. To protect critical data in the event of data corruption

6. Data destruction procedures:
   a. Ensure that expired backup media are destroyed
   b. Ensure that discarded paper documents are shredded

c. Ensure complete and irrecoverable destruction of data

d. Act as a safeguard in the event a user forgets to delete data

7. An organization is considering adding anti-virus software to its email servers and file servers. This reflects:

   a. A defense in depth strategy

   b. The fact that anti-virus on workstations is unreliable

   c. The need to protect systems that lack anti-virus software

   d. The need to protect the organization from malicious code contained in spam

8. A device whose design employs duplication of failure-prone components so as to ensure the greatest possible availability is known as:

   a. Optimized

   b. Redundant

   c. Highly available

   d. Fault tolerant

9. A collection of four servers that act in coordination to give the appearance of a single logical server is known as:

   a. Grid

   b. Virtual

   c. Fault tolerant

   d. Cluster

10. A systems engineer is managing a server cluster. A memory fault has occurred in one of the active servers; the cluster software has caused another server in the cluster to become active. The system engineer has witnessed a:

    a. Pairing

    b. Failover

    c. Load balance

    d. Synchronization

11. The recovery point objective (RPO) for a critical application is set to two hours for a 4TB database; the recovery time objective (RTO) is set to twenty four hours. An IT architect needs to design a solution where a server in a remote data center can assume production duties within the RPO and RTO specifications. Which method for data transfer to the alternate data center should the IT architect use?

    a. Replication to a warm server

    b. Replication to a cold server

    c. Recovery from backup tape

    d. Recovery from an electronic vault

12. A security manager needs to find a professional services firm to identify vulnerabilities in a running web application. The security manager should find a professional services firm that can perform:
    a. Code reviews
    b. Penetration testing
    c. Application scanning
    d. Ethical hacking
13. A security engineer is testing a Web application for vulnerabilities, and has inserted the following characters into a form field: "`script OR name LIKE %user%;.`" The security engineer is performing:
    a. Buffer overflow
    b. Cross-site scripting
    c. SQL injection
    d. Script injection
14. The purpose of a change management process is to:
    a. Test the changes made to a system
    b. Record the changes made to a system
    c. Plan and review the changes made to a system
    d. Reduce downtime
15. The best approach for applying security patches is to:
    a. Apply only the security patches that are applicable
    b. Apply all available security patches as soon as possible
    c. Apply no security patches
    d. Apply all available security patches as soon as possible

Hands-On Projects

Project 7-1: Security Evaluation for Remote Access

In this project you will compare the security features of VPN remote access products.

Research and compare features from "thick client" VPN software from companies like Cisco and Nortel. Also research the "clientless" SSL VPN clients that are available.

What products can you find that are suitable for smaller organizations? You may wish to examine "all in one" network-based products that combine a router, firewall, and VPN server in a single appliance.

Some of the features to consider are:

- Thick client vs. SSL-clientless
- Authentication types supported (userid/password, token, smart card)
- Security including 802.1X

Project 7-2: Centrally Managed Anti-Virus

In this project you will research workstation- and server-based anti-virus software that can be managed from a central management console.

Collect information from four or more companies that have enterprise-class anti-virus software for servers and workstations. Identify the features that these products have in common, and also identify any unique features.

Opine on the following:

- What is the business value of the feature(s) that are in common among the different products?
- What is the business value of the unique features you found?
- What features are unnecessary? Why?

Project 7-3: Physical Security Survey

In this project you will perform a survey of the physical security at your school or workplace.

Identify vulnerabilities in the design and use of the following aspects of the facility:

- Use of locking doors at main entrances
- Access to sensitive areas
- Cabling, communications, or computing equipment readily accessible
- Video surveillance
- Personnel badges
- Loading area
- Fire suppression

Make a list of issues you found. Include a categorization of risk, and a suggested remedy to reduce the risk.

Do not enter any "employee only" areas during this exercise unless you have obtained permission in advance or are escorted by authorized personnel.

Case Projects

Case Project 7-1: Data Replication Products Survey

As a consultant with the Risk Analysis Consulting Co., you have been asked to research data replication products for a manufacturing company, XYZ Plastics.

XYZ Plastics has decided to build its backup application servers in a distant city. In its headquarters and in the other location, the servers run Solaris (operating system) and Oracle (database), and the database resides on a SAN system. XYZ Plastics would like transactions on its headquarters servers to be transmitted over a wide-area connection to the SAN in the other city.

Find some reviews and information on data replication products. Some possible sources of information include:

- Searchstorage.techtarget.com
- Computerworld.com
- Sun.com
- Oracle.com

Make a comparison of some of the replication products you have identified. Discuss the differences and similarities among the products and discuss their business value.

Case Project 7-2: Administrative Access Process

As a consultant with the Data Protection Consulting Co., you have been assigned to the Thick Slice Bread Co. You are to develop a process developed for assigning administrative access. Requirements for this process include:

- Subject (the person for whom administrative access is being requested) must hold a job description that is eligible for administrative access.
- Subject's manager must make the request.
- Request must specify the system(s) for which administrative access is being requested.
- VP of IT must approve all requests.
- VP of Security must approve all requests.
- Security token must be issued to the subject if he/she does not have one already.
- Subject must verify access within 24 hours of notification.

Note whether these requirements are sufficient for the development of the process. Identify any issues or ambiguities that need to be addressed.

Case Project 7-3: Quarterly Review of Access Rights

As a consultant with the Security Advisors Co., you have been asked to develop a process for a quarterly review of privileged access rights for a company with two thousand employees. Requirements for this process include:

- Access review for physical, network, VPN, system, database, and application must be performed.
- Access reviewers must have access to a list of employees terminated in the past
  90 days, as well as a list of active employees.
- Access reviews must include the creation of evidence that the review was performed, so that auditors may confirm this activity later in the year.

Develop the procedure(s) needed to support this process.

Are there any additional requirements that should have been included?

Are there any ambiguities or issues?

This page intentionally left blank

chapter 8

Physical and Environmental Security

Topics in this Chapter:

- Site access controls including key card access systems, biometrics, video surveillance, fences and walls, notices, and exterior lighting
- Secure siting: identifying and avoiding threats and risks associated with a building site
- Equipment protection from fire, theft, and damage
- Environmental controls including HVAC and backup power

The (ISC)^2 *Common Body of Knowledge* (CBK) defines the key areas of knowledge for Physical and Environmental Security in this way:

The Physical (Environmental) Security domain addresses the threats, vulnerabilities, and countermeasures that can be utilized to physically protect an enterprise's resources and sensitive information. These resources include people, the facility in which they work, and the data, equipment, support systems, media, and supplies they utilize.

The candidate will be expected to know the elements involved in choosing a secure site, its design and configuration, and the methods for securing the facility against unauthorized access, theft of equipment and information, and the environmental and safety measures needed to protect people, the facility, and its resources.

Key areas of knowledge:

- *Participate in site and facility design considerations*
- *Support the implementation and operation of perimeter security*
- *Support the implementation and operation of interior security*
- *Support the implementation and operation of operations/facility security*
- *Participate in the protection and securing of equipment*

Physical security is concerned with the protection of business premises and assets through the use of physical controls that restrict and manage the movement of people and equipment. The main categories of physical security are:

- Access security
- Secure siting
- Equipment protection
- Environmental controls

Site Access Security

The purpose of a site's access security is the protection of the site and its occupants and assets from intruders. This is achieved through access control systems, notices, and sound site selection.

Site Access Control Strategy

Other chapters in this book discuss the concept of **defense in depth** (particularly Chapter 2, "Access Controls"), which is the general technique of using layers of controls to protect valuable assets. Defense in depth is commonly used to protect information systems by protecting them with one or more layers of physical controls, in addition to logical controls discussed elsewhere in this book. The concept of defense in depth is illustrated in Figure 8-1.

Site Access Controls

The purpose of site access controls is to restrict the movement of people, so that only authorized persons are permitted to enter the facility and specific work zones within the facility; and also to record the movements of those personnel.

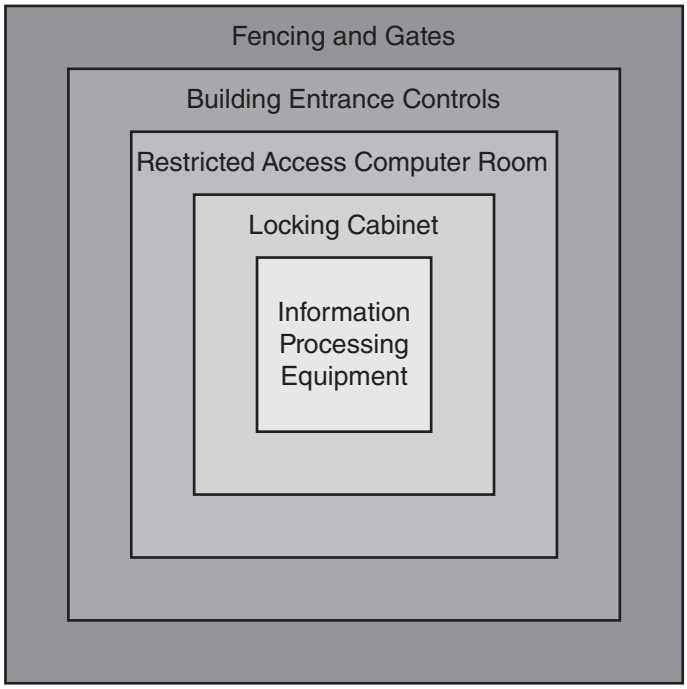


Figure 8-1 Defense in depth protects information resources and other assets

Source: Course Technology/Cengage Learning

The categories of controls are:

- Detective
- Deterrent
- Preventive
- Corrective
- Recovery
- Compensating

These categories of controls apply as much in physical space as in the logical space of computers. In fact, they are probably easier to understand in physical space, since physical controls aren't abstract like logical, computer-based access controls are.

For a detailed explanation on the meaning of these control categories, go read the section in Chapter 2, "Access Controls." Their names should be pretty intuitive, however, so even if you haven't read that section in chapter 2 you'll probably be fine.

Key Cards Key cards are a form of preventive and detective controls that is used to control which persons are permitted to enter a facility as well as specific zones within a facility. A key card is one part of a larger system that includes **card readers** (devices used to read the contents of key cards) and electrically operated door latches that, when activated, unlock the

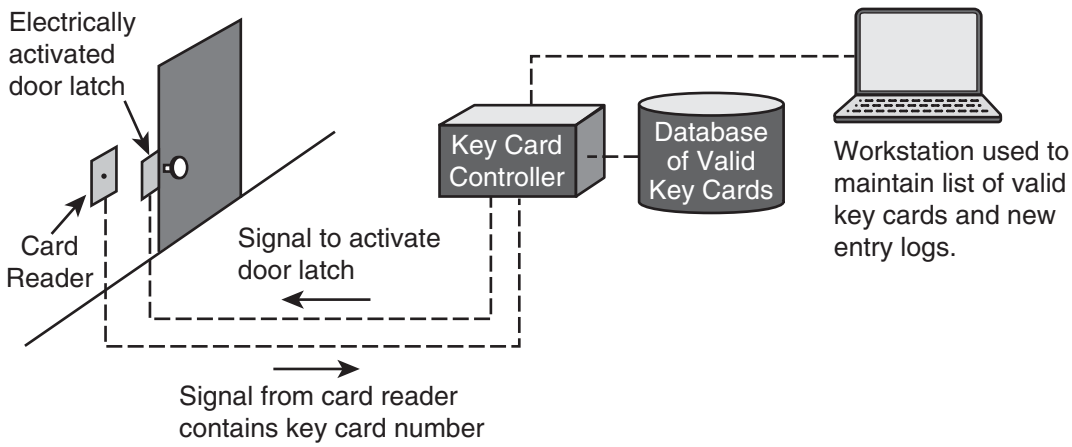


Figure 8-2 Key card system schematic

Source: Course Technology/Cengage Learning

door for a few seconds; and a central computer system that contains a database of all registered key cards and which doors they are permitted to enter. Figure 8-2 shows an entire key card system.

A **key card** is typically the same size as a credit card and is embedded with a RFID chip, Smartcard chip, or magnetic stripe that uniquely identifies the cardholder. A key card is typically issued to each employee who is authorized to enter the facility. Figure 8-3 illustrates a typical key card reader that is used to control access to a secured room.

One weakness of a key card system is that a lost card can be used by a third party to enter the facility. For this reason it is advised that there be no identifying information on the card that would provide any clues to a passer-by who might find a lost card.

Another weakness of a key card system is the tendency for some personnel to "tailgate" those who use their key cards to open a secured door. This can be remedied in one of several ways:

- Enforcing a "one card, one person" policy that includes consequences for breaking the policy
- RFID-equipped cards that can be detected as a person passes through (or near) a secured door, even if the person does not pass her card through the card reader
- Mantraps that enforce one-at-a-time entrance or exit of personnel
- Security guards who observe and intervene when necessary

Another control that mitigates the problem of a lost key card is the use of a PIN pad at some or all entrances. A **PIN pad** is a numeric keypad that is typically used in connection with an access control system. Someone who wishes to enter the facility must have not only the key card in their possession but must also know a PIN before the doorway will be activated. A combination card reader and PIN pad is shown in Figure 8-4.

Figure 8-3 Key card reader used to control physical access

Photo by Rebecca Steele

The events that permit an employee with a key card to enter a protected entrance are:

Key card is issued to employee as a part of a process that documents the request, approval, and issuance of the card.

Security personnel specify which doorways or zones the employee is permitted to enter.

1. Employee approaches a doorway and causes the card reader to read the key card. If the card reader has a PIN pad, then the employee keys the PIN at this time.
2. Card reader sends a signal to the central key card controller, which looks up the key card number in its database and, further, determines if the key card is authorized at the particular doorway.
3. Central controller logs the attempted entrance, including the date and time, key card number, door number, and whether the entrance was permitted.
4. Central controller activates the doorway's electric latch if the key card is permitted at that doorway.
5. Employee pushes or pulls the door open to access the facility or room.

Figure 8-4 Card reader and PIN pad protects sensitive facilities

Photo by Rebecca Steele

The controller that controls the system's card readers and door latches should be located in a locked cabinet or room and be accessible by only the smallest number of security personnel who manage physical access control for the organization.

The controller will usually have a backup power supply, so that personnel can still enter the facility even during a power failure. However, in the event of a malfunction of the key card system, usually an organization will issue hard keys to a limited number of highly trusted personnel who can enter the facility using hard keys.

Biometric Access Controls While key card-based controls are widely used for facility access controls, certain drawbacks—such as the ability for another person to use a lost card—persuade organizations to use a more effective control. PIN pads in combination with key cards, as discussed in the previous section, reduce risks somewhat, but PINs can sometimes be easily guessed. An organization that wants a stronger control can consider biometric-based building access controls. Biometrics is a means for measuring a physiological characteristic of a person as a means for positively identifying him or her.

Figure 8-5 Fingerprint reader

Image copyright, 2009. Used under license from istock.com

Biometric controls rely upon a measurement of a feature of someone's body as a means for establishing positive identification. The most common biometrics in use in facility access controls are:

- **Fingerprint.** A small fingerprint reader scans the fingerprint of someone who wishes to enter a facility or doorway within a facility. The reader sends the scanned fingerprint to a central access controller for comparison. A security panel that incorporates a fingerprint reader is illustrated in Figure 8-5.
- **Hand print.** Another popular biometric measurement is the geometry of a human hand.
- **Iris scan.** Human irises are as unique as fingerprints, and high-resolution digital imaging is able to capture a high quality image from a comfortable distance from the subject. Iris scan-based biometric systems are available and growing in popularity. An image of the human iris is shown in Figure 8-6.

Metal Keys Metal keys are used to unlock doors and other locks. Metal keys are discouraged for use as a primary access control for the following reasons:

- Keys are easily copied
- No record of who entered a room or facility is available

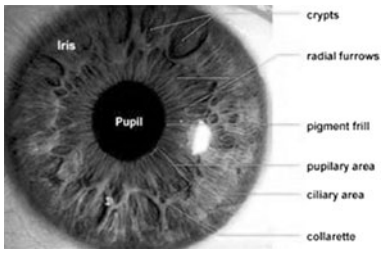


Figure 8-6 The human iris is a reliable and unique biometric subject

Source: Illustration by U.S. Army Research Laboratory

- Many key operated locksets are vulnerable to a specially crafted key called a "bump key" that can be used to open a lock with no sign of forced entry

Metal keys do, however, make a suitable secondary control in limited situations including:

- A backup method for entering a facility, in the event of the failure of the primary method, for example.
- A locking cabinet located in a room protected by a key card or other recording access control.

All metal keys should be issued according to a strict procedure that includes written records. When possible, each key should be serialized (stamped with a unique identifying mark or number), which enables identification of a specific key, should it be found. Employees who are issued metal keys should sign a form that describes their responsibility for safe-keeping of the key.

Mantraps A **mantrap** is a set of interconnected double doors used to control the entrance or exit of personnel. The typical operation of a man trap is:

1. Person approaches first door, and issues access control (such as a key card, PIN pad or biometric) to open it.
2. Person steps in to the mantrap, and the first door closes.
3. When the first door has closed, person is able to open the second door and proceeds through it.

The "mantrap" area is usually small, just large enough to hold a few persons. A functional diagram of a mantrap appears in Figure 8-7.

Some mantraps are manually operated by a guard who is physically isolated from the mantrap itself.

Security Guards **Security guards** are trained personnel who perform a variety of duties in a facility. Some of these duties include:

- Checking employee identification
- Handling visitors

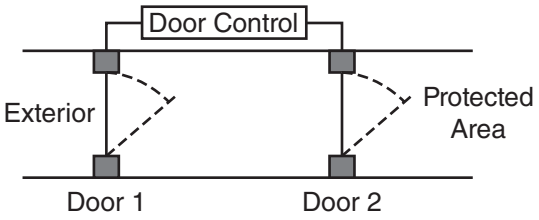


Figure 8-7 A mantrap permits only one door at a time to be opened, thus restricting movement of personnel

Source: Course Technology/Cengage Learning

- Checking parcels and incoming/outgoing equipment
- Manage deliveries
- Apprehend suspicious persons
- Call additional security personnel or law enforcement
- Assist persons as needed

Most of these activities cannot be achieved with automated controls such as key card systems. There are several advantages to security guards including:

- **Human judgment.** A guard can spot a suspicious activity that no automated system can handle.
- **Flexibility.** A guard can perform many other duties such as helping visitors and employees.
- **Roaming.** A guard can walk to another part of a facility to check on a suspicious activity or apprehend an intruder.

Guard Dogs A **guard dog** is a dog that is employed to guard against or detect unwanted or unexpected personnel. Guard dogs are a physical control that can serve as detective, preventive, and deterrent controls. Guard dogs can accompany security personnel and assist in detecting and apprehending intruders, as well as detecting substances including explosives and illegal drugs.

Access Logs Access logs are a detective control, meaning they serve to record events such as the comings and goings of personnel. An **access log** is a record that contains building access attempts. The types of access logs that should be maintained at a work facility include:

- **Personnel entrance and exit**. This can usually be accomplished with a key card system or some other automated means.
- **Visitor log**. This allows the organization to track all visitors who have entered the facility. The log should contain identifying information and the nature of their visit.
- **Vehicles**. If the facility includes a gated parking facility, the entrances and exits of all vehicles should be recorded.
- **Packages**. All incoming and outgoing parcels should be logged, including their contents, origin or destination, and personnel associated with the parcel.

- **Equipment**. Personnel taking equipment into and out of the facility should be logged, including serial numbers where applicable.

Fences and Walls Fences and walls are an effective preventive and deterrent control that is designed to prevent unwanted persons from accessing specific areas such as the grounds of a building. They can also force visitors to approach a facility through a manned control point such as a guard station or entrance gate. Refer to Table 8-1 for various fence and wall heights and their effectiveness.

Fencing can be further protected with motion detection that will trigger alarms when someone may be attempting to climb over a fence. Video surveillance can also be used to observe fence lines and fenced areas.

Video Surveillance In most settings it is not economically feasible to place security guards at all vantage points at a facility. An effective addition to a smaller number of security guards is a video surveillance system that provides comprehensive visual coverage of place of particular interest. A **video surveillance system** is a system consisting of one or more video cameras that are used to observe and/or record activities such as personnel movement. Typical locations for video cameras include:

- Building entrances and exits
- Lobby and reception areas
- Loading docks
- Refuse collection and disposal areas
- Stairwells
- Corridors

Camera Types Surveillance systems obtain their video images from video cameras that are placed in strategic locations at a facility. Surveillance systems can support several types of cameras including:

- **Closed Circuit Television (CCTV) cameras.** The mainstay of surveillance systems, CCTV cameras send standard composite video (and, sometimes, audio) signals through CCTV cabling. CCTV is a technical standard for the transmission of video signals through a cable. A surveillance camera is shown in Figure 8-8, and surveillance monitors that view images from surveillance cameras are shown in Figure 8-9.
- **IP cameras.** Cameras can send their video signals through wired TCP/IP networks to an IP-enabled controller.

Height	Effectiveness
3-4 ft	Deters casual trespassers
6-7 ft	Too difficult to climb easily
8 ft plus 3 strands of barbed/razor wire	Deters all but the most determined trespassers

Table 8-1 Fence and wall heights to control intrusions

Figure 8-8 Video surveillance cameras

Image copyright, 2009. Used under license from istock.com

Figure 8-9 Video surveillance monitors

Image copyright, 2009. Used under license from istock.com

- **IP wireless cameras.** Cameras can transmit their video signals through Wi-Fi, Bluetooth, or other wireless networks.
- **Night vision cameras.** Cameras can be equipped with infrared LEDs that artificially light the area being viewed. This enables surveillance of an area even in complete darkness. Night vision cameras can transmit their signals in any of the formats listed here.
- **Fixed cameras.** Video cameras that are permanently aimed in one direction.
- **Pan/tilt/zoom cameras.** Video cameras that can be remotely controlled by an operator for a closer look at some activity or person of interest.
- **Hidden cameras.** Surveillance cameras can be placed secretly out-of-sight to record activities that might not take place if cameras were visible. Hidden surveillance cameras that are disguised as common objects like clocks, smoke detectors, books, radios, and other objects are available.

Recording Capabilities Video systems can provide real-time-only viewing, recording of video information, or both. The range of recording and viewing capabilities includes:

- **Real time viewing only.** Events taking place will be viewable only when they happen.
- **Motion-activated recording.** Surveillance system can record video only when there is motion to record, such as a person walking or a vehicle driving through the camera's field of view.
- **Periodic still images.** A surveillance system can record still images from each camera every few seconds, whether something is going on or not.
- **Continuous video recording.** A surveillance system can continuously record video whether there is motion or not.

Surveillance systems can record data onto videotape, hard drive, or DVR media. Systems can be configured to retain images for a day, a month, several months, or longer, depending upon the storage capacity of the system.

Intrusion, Motion, and Alarm Systems

Intrusion- and motion-based alarm systems are a supplement or substitute for video surveillance systems. An **alarm system** is an apparatus that consists of a central controller called an alarm panel, plus several sensors of different kinds including:

- Door and window sensors that detect when the door or window is opened
- Motion sensors
- Glass-break sensors that detect the sound of a broken window

Alarm systems also have some means for alerting building owners, occupants, or security staff that an intrusion has occurred. Typical alarm methods include:

- Audible siren or bell
- Strobe light to guide security personnel or law enforcement to the location of the intrusion
- Alert on an in-building monitoring center

- Alert via a phone line to a remote monitoring center
- Alert via a cellular call to a remote monitoring center
- An alarm system is configured and operated via the alarm panel. Typically the alarm is activated when employees vacate the premises by entering a security code or password. Then, when employees return, the alarm system is similarly deactivated by entering a security code or password and then the instructions for deactivating the alarm. This prevents an intruder from being able to deactivate an alarm system.
- Organizations considering an alarm system should consider one where each employee who has responsibility for operating the alarm will get his or her own separate alarm code. This will enable the organization to track which persons activate and deactivate the alarm. Further, the alarm system should record the days and times that the alarm system is activated and deactivated. This will deter a dishonest employee with the alarm code from returning to the premises after hours to steal company property, since the alarm system will have recorded their entries and exits.

Visible Notices

Physical security controls usually include deterrent controls that are designed to discourage would-be intruders from considering entering or damaging a facility or asset. These deterrent controls include visible notices such as:

- No Trespassing signs.
- Surveillance notices.
- Surveillance monitors.

Laws or regulations in some areas require an employer to post visible notices if video surveillance is present at a facility. The visible notice shown in Figure 8-10 is an example of such a notice.

Exterior Lighting

Lighting is primarily a deterrent control that is designed to discourage intruders during nighttime hours. Lighting is intended to illuminate an intruder's actions so that others may see them and call appropriate authorities.

- Lighting should not betray the locations of other security controls such as surveillance cameras, motion detectors, or guard posts. The purpose of lighting is not to illuminate security controls.
- NIST (National Institute for Standards and Technology) standards require that critical areas be illuminated with at least two foot-candles of power at a height of 8 feet. When a facility is illuminated by lights on poles, the poles should be spaced so that there are no dark areas between the lights; for example, if lights illuminate a diameter of 50 feet, then they should be placed no more than 50 feet apart.

Figure 8-10 Visible notices inform intruders of physical security controls

Photo by Rebecca Steele

Other Physical Controls There are other physical controls that organizations may consider using that provide additional protection against intrusions.

- **Bollards.** These heavy upright posts restrict vehicle traffic while permitting pedestrians to walk through. The primary purpose of bollards is to prevent vehicles-as-weapons from getting too close to buildings. Some bollards are retractable or removable, to allow access for maintenance vehicles, for instance. Figure 8-11 shows bollards that block vehicles from the entrance to an office building.
- **Crash gates.** A movable device that can be used to prevent the entry or exit of a vehicle. Crash gates are so-named because an attempt to drive a vehicle through one would result in a crash, as shown in Figure 8-12.

Secure Siting

The concept of **secure siting** is, simply, locating a business at a site that is reasonably free from hazards that could threaten its ongoing operation.

Figure 8-11 Bollards restrict vehicle traffic

Photo by Rebecca Steele

Figure 8-12 Crash gates prevent unwanted vehicles from entering (or leaving) a facility

Illustration by Delta Scientific

No location is free of all threats. And, threats are not the only factor that is considered in business site selection. A business operation also needs a facility that is reasonably close to customers, suppliers, transportation, and workers. But when threats are also considered and weighed in the decision making process, company management can make an informed decision.

The presence of a threat does not automatically mean that a business should not locate its operation at a particular site. Some threats can be mitigated, reduced, or transferred. Some are simply accepted. For instance, locating an operation close to an airport or railroad may increase the threat from a transportation accident (plane crash or train derailment), but those threats might be considered to be highly improbable and transferred in part by insurance. This topic of risk analysis and risk management is covered fully in Chapter 1," Information Security and Risk Management."

An organization needs to take into consideration the threats associated with the site that is selected and incorporate those threats into its business continuity and disaster recovery planning. These topics are discussed in detail in Chapter 4, "Business Continuity and Disaster Recovery Planning."

Threats can directly or indirectly affect a business operation. For instance, a business can be safely located away from areas prone to flooding or landslides, but if the community's only transportation and/or communications are subject to these threats, then an event can disrupt business operations by severing transportation or communications that are required to continue business. For this reason the site selection process needs to consider the bigger picture and not end at the boundary of the premises.

Natural Threats

Several natural phenomena can occur that may disrupt business operations. These factors should be taken into account when making a site selection, so that management is aware of all of the factors related to the selection decision.

These natural threats include:

- **Floods.** Overflowing streams, rivers, and lakes may threaten a business directly or indirectly. A local hydrologist should be consulted in order to determine the risk of any particular location that may be near a body of water.
- **Landslides and Avalanches.** These events can damage buildings, transportation, utilities, and communications.
- **Earthquakes.** A seismologist can be consulted to help determine the risk of a seismic event at or near the site.
- **Volcanoes.** These violent events can produce many effects including falling rocks and ash, pyroclastic flows, landslides, and flooding that damage buildings, transportation, utilities, and communications infrastructure. A pyroclastic flow that is racing down the side of an erupting volcano is shown in Figure 8-13.
- **Tsunamis, waves, and high tides.** These events can damage buildings and infrastructure such as transportation, utilities, and communications.

Figure 8-13 Pyroclastic flow from a volcano

Courtesy United States Geological Survey

- **Severe Weather.** Hurricanes, tornadoes, heavy rain, blizzards, ice storms, and wind storms can damage buildings and equipment as well as supporting infrastructure such as transportation and public utilities. While most of these threats are regional in nature, knowledge of these threats may help the organization to choose the type of building it occupies.

Man-Made Threats

Several types of man-caused events can potentially disrupt business operations and should be considered in the site selection process.

- **Chemicals spills.** A business located near a refinery, chemical factory or business that uses hazardous substances could be disrupted by an event such as a spill, leak, or explosion.
- **Transportation.** A business wants to be close enough to transportation corridors to be able to send and receive materials and facilitate workers and visitors. However, if a business is too close to an airport, railroad, or highway, then the hazards of accidents can pose a threat to nearby businesses.
- **Utilities.** Site selection needs to consider the proximity to overhead and buried power transmission lines, natural gas pipelines, LPG (liquefied petroleum gas) pipelines and storage facilities, gasoline pipelines, and so on, and consider the types of events that could require evacuation or could damage business premises.

- **Military base.** A business located near a military base might consider the hazard of being located near a location that may be high on an enemy state's list of targets.
- **Social unrest.** Being located near areas prone to demonstrations and other mass gatherings could prove to be disruptive at inopportune times. These areas include major downtown thoroughfares, public squares, schools, and universities.

Other Siting Factors

In addition to natural and man-made threats, other security-related factors should influence site selection, including

- **Building construction and materials.** The composition and quality of construction of a building has a direct bearing on the protection of its occupants and business equipment.
- **Building marking.** While many businesses are proud to erect a large sign that proclaims the presence of a business location, oftentimes doing so is like hoisting a giant target that says, "Hit me here." Sometimes it's enough to simply display the address without advertising the name of the organization that is located there.
- **Loading and unloading areas.** Areas where freight and deliveries take place require additional safeguards such as video surveillance, auto-closing doors, and double sets of doors so that a delivery agent cannot access the premises while loading or unloading goods.
- **Shared tenant facilities.** Many office buildings called shared-tenant facilities house more than one business. This makes physical access control far more complicated, since they cannot be erected at the whim of one of the tenants without affecting others. Further, the businesses that occupy shared tenant buildings typically do not own the building, which means that any physical changes to improve physical security must be approved by the facility's owner. Some controls, such as access to the building's main entrances may be held in common by all of the businesses that occupy the building; this makes implementation of controls such as key card systems more complicated.

Protection of Equipment

Business equipment needs to be protected from theft and damage, so that business operations that depend upon equipment can continue functioning. This section discusses the protection of business equipment located in a business facility. Topics covered here include theft protection, damage protection, fire prevention and response, and cabling security. The protection and security of communications cabling is also discussed.

Theft Protection

Business equipment must be protected from theft. While part of the risk can be transferred through insurance, in many cases stolen equipment cannot be *immediately* replaced, resulting in business disruption and fines or possible loss of revenue. However, if the stolen equipment also contains business information, then the loss and business disruption may be more

significant and difficult to quantify, and the results could be more widespread. For example, a stolen backup tape or laptop computer containing sensitive business or personal information could result in negative publicity, embarrassment, fines, and customer distrust.

Several measures can be taken to reduce the threat and probability of theft including

- **Protection of laptop computers.** Employees who are issued laptop computers need to understand their responsibilities and be held accountable for their actions. This will probably include
  - Use of cable locks to prevent or discourage theft.
  - Use of defensive software such as firewalls, anti-virus, anti-spyware, location tracking, and self-destruct-if-stolen controls.
  - Use of two-factor authentication such as fingerprint or smart card.
  - Use of encryption to protect sensitive information from disclosure.
  - Training to make personnel aware that they must not leave laptop computers unattended.
- **Protection of servers and backup media.** Place servers in locked rooms that few personnel can access. Attach servers to racks or cabinets with locking fasteners. Clearly mark equipment with difficult-to-remove asset tags or labels. Place backup media in locking cabinets. Use a reliable off-site storage vendor that utilizes secure transportation and transfer. Use keycard systems to restrict personnel entry into computer and server rooms. Use video surveillance to record entry and exit from sensitive areas.
- **Protection of sensitive documents.** Place sensitive documents in locking, fire-resistant cabinets. Institute a "clean-desk" policy that requires sensitive documents to be locked away when not in use. Discarded documents containing sensitive information should be shredded.
- **Protection of valuables.** Items such as currency, blank checks, precious metals or gems, should be placed in a safe.
- **Institute equipment check-in/check-out.** All equipment that enters or leaves a facility should be tracked. A log that is similar to a visitor sign-in/sign-out sheet should be instituted that records the worker's name, equipment description, and serial number. Laptop computers issued to employees can be exempted from this since they can be considered to be permanently checked out to an employee. Some organizations require that any laptop computer leaving the premises be scrubbed, to remove sensitive data in order to eliminate the risk of a security incident if the laptop computer is lost or stolen while out of the physical control of the organization.

Damage Protection

Business equipment needs to be protected from damage that can be caused by a variety of events such as fires, floods, earthquakes, and so on. Some of the safeguards that can be instituted include

- **Earthquake bracing.** Shelves and racks used to store equipment and supplies (as well as running equipment) can be braced, to minimize the possibility that they will fall

over in an earthquake or other event. Equipment can be fastened to racks and shelves so that they will not slide off and fall, resulting in damage and injury.

- **Water detection and drainage.** Ground floor rooms of buildings with business equipment and machinery should have water detectors connected to alarms, to alert personnel that water is present in the facility. This is especially true in computer rooms with raised floors where the incursion of water may not be noticed until it has begun to cause damage. Floor drains and/or sump pumps may also be needed to help channel water away from equipment to prevent damage.

There are probably other means for equipment protection available, and perhaps even necessary in some circumstances and locales.

Fire Protection

Fire prevention capabilities are required in virtually locale in the world. Required systems in business locations include one or more of the following:

- Fire extinguishers
- Smoke detectors
- Automatic sprinkler systems
- Fire alarm systems

Fire Extinguishers

Fire extinguishers are portable devices that an individual can use to extinguish small fires. There are four types of fire extinguishers that are used to extinguish different types of fires:

- **Class A**. Ordinary combustibles: wood, paper, and so on.
- **Class B**. Flammable liquids and gases: gasoline, propane, etc.
- **Class C**. Energized electrical equipment.
- **Class D**. Combustible metals: magnesium, etc.
- **Class K**. Cooking oils.

Fire extinguishers come in single-type and combination type models. A common type of combination fire extinguisher is Class ABC, which can be used to fight fires of those types.

Smoke Detectors

Smoke detectors are automatic devices that sense the presence of fire in its incipient stages, at the very beginning of combustion. Detectors are either equipped with annunciators or wired into a central fire alarm system. There are 2 types of smoke detectors:

- **Optical**. These types of detectors utilize an infra-red LED and a photo detector, and function by detecting minute changes in the refraction of light caused by smoke.
- **Ionization**. These detectors detect smoke before it is visible by measuring slight changes in current between electrodes in the vicinity of a small amount of radioactive Americium-234.

Smoke detectors are powered by small batteries, external electric current, or both. Smoke detectors in commercial buildings are usually powered by external electric current and do not rely solely on internal batteries.

Fire Alarm Systems

Fire alarms function by alerting personnel of smoke or fire in a facility. Alarms can also be wired to a fire department or centrally monitored public safety center in order to alert a fire department. Alarms can be triggered in several ways, including:

- **Pull stations.** These are manually operated switches, activated by personnel who observe smoke or fire. A pull station is shown in Figure 8-14.
- **Smoke detectors.** Devices that detect smoke, described earlier in this section.
- **Sprinkler system flow detectors.** Devices built-in to sprinkler systems that detect their flow.

Fire alarms typically have annunciators located throughout a building that audibly and visibly notify personnel of the fire in the building. A typical fire alarm is shown in Figure 8-15.

Automatic Sprinkler Systems

Sprinkler systems are systems consisting of water supply pipes and sprinkler heads that are used to douse a fire with water, or a combination of water and fire extinguishing foam. There are several types of sprinkler systems including:

- **Wet pipe systems.** The simplest and most common type of sprinkler system, wet pipe systems are filled with pressurized water, which is released when a sprinkler valve's fusible link is melted by heat from a nearby fire.

Figure 8-14 Fire alarm manual pull station

Photo by Rebecca Steele

Figure 8-15 Fire alarm annunciator

Photo by Rebecca Steele

- **Dry pipe systems.** A more complex type of sprinkler system where water is not present in the pipes until the system is activated.
- **Deluge systems.** A system where all sprinklers are open. When the system is activated, water is discharged from all sprinklers.
- **Pre-Action Systems.** A dry pipe that is converted to a wet pipe system when a smoke, fire, or heat alarm is activated. This type of system is often used in computing facilities, where the consequence of an accidental discharge is high.
- **Foam water sprinkler systems.** A variation of any of the water-based sprinkler system where the liquid discharged is a combination of water and fire-retardant foam.

Figure 8-16 shows a close-up view of a fire sprinkler head.

Gaseous Fire Suppression An alternative to water- and foam-based fire suppression, **gaseous fire suppression** systems consist of inert gas in storage tanks, delivered via piping and nozzles. Gaseous fire suppression systems are used in areas with valuable electrical equipment such as computer systems. They work by displacing oxygen from the room(s) where the fire is located. In the heat-oxygen-fuel fire triangle, gaseous fire suppression works by removing oxygen from the fire by interfering with chemical combustion.

Figure 8-16 Fire sprinkler head

Photo by Rebecca Steele

Gaseous fire suppression lowers the amount of oxygen in a facility; thus, these fire suppression systems have additional alarms and signage to alert personnel of the hazard. Still, a discharge is not lethal to humans.

Cabling Security

Voice and data communications cabling must be protected from accidental or deliberate damage and tapping that can result in eavesdropping or man-in-the-middle attacks. Because organizations are connected to one another over private and common carrier networks, not all cabling is in the direct control of the organization, so there's only so much that an organization can do directly on its own.

Some of the threats and remedies for cabling risks are:

- **Exposure of organization's own cabling on its premises**. Place cabling in conduits or re-route away from exposed areas
- **Exposure of common carrier's cabling to threats outside of business's control**. The common carrier must protect its cabling on behalf of its business customers. But there are remedies that businesses can take to mitigate possible threats, including:

  Select a different common carrier that does a better job of protecting its cable plant.

Utilize **diverse network routing**, a strategy of utilizing physically separate communications circuits so that damage or malfunction in one circuit will not result in the loss of communications.

Utilize encryption on common carrier networks to thwart eavesdropping.

Environmental Controls

Environmental controls are the various electric and mechanical systems that support the heating, cooling, humidity, and electric power needs for a facility. Environmental controls provide a comfortable environment for workers, as well as the heating, cooling, humidity, and energy required to support business equipment and information systems in the building.

Heating and Air Conditioning

Heating, ventilation, and air conditioning (**HVAC**) systems ensure a steady temperature within a range that is comfortable for workers and beneficial to business equipment and information systems.

Information systems can produce a great deal of heat that must be continuously removed with air conditioning systems. Overheating for even short periods can greatly reduce the life of systems, making them far more likely to fail.

Because computer systems have so little tolerance for HVAC failures, redundant HVAC systems are often used. HVACs are electro-mechanical systems that require periodic shutdown and maintenance, another reason why redundant systems are often used. It is important to note that a facility should be able to operate indefinitely when one of its HVAC systems is offline.

The cooling capacity of HVAC systems are rated in one of two ways:

- BTU/hour
- Tons

Engineers will calculate the required capacity of a building's HVAC system by measuring the building's size as well as obtaining an estimate of the amount of heat output from computer equipment.

Ventilation should be a concern. Building designers need to be aware of external conditions in areas where ventilation air is drawn into a building, in order to avoid the introduction of harmful gases into the building. Areas in a building that require contaminant-free air may need to utilize additional filtering as well as positive pressure flow so that opened doorways do not permit contaminated air to enter areas that require cleaner air.

HVAC systems also have controls for the regulation of humidity, which is described next.

Humidity The amount of water vapor in the air is a measure of the **humidity**. **Relative humidity** is the amount of water vapor in a sample of air compared to the maximum amount of water vapor the air can hold. Relative humidity is expressed as a percentage, from 1% to 100%.

The relative humidity in a facility with workers and computing equipment should range from 30% to 50%. Levels below 30% will result in discomfort and excessive thirst for staff, cause electronic equipment to become more brittle, and permit more static electricity.

Levels above 50% will permit dust mites to survive, and higher levels may result in condensation, where moisture causes corrosion. Moisture condensing on equipment will cause short circuits.

Electric Power

Information processing equipment requires clean power, lots of it, and is intolerant of the wide variety of electric power problems that can occur. Electric power is similar to piped water in that events like leaks or sudden shut-ons and shut-offs will create changes in pressure and even shockwaves that will travel up and down the pipeline that affect other users. Some of the electric power anomalies include:

- **Blackout.** A total loss of power.
- **Brownout.** A prolonged reduction in voltage below the normal minimum specification.
- **Dropout.** A total loss of power for a very short period of time (milliseconds to a few seconds).
- **Inrush.** The instantaneous draw of current by a device when it is first switched on.
- **Noise.** Random bursts of small changes in voltage.
- **Sag.** A short drop in voltage.
- **Surge.** A prolonged increase in voltage.
- **Transient.** A brief oscillation in voltage.

Several different types of equipment are available to improve the quality of electric power. The remainder of this section discusses these:

- Line conditioner
- Uninterruptible power supply
- Electric generator

Line Conditioner

A **line conditioner** (sometimes called a power conditioner) is a device that filters or removes some of the undesirable anomalies in a power feed, "smoothing out" incoming power to make it cleaner for sensitive equipment. Line conditioners smooth out the smaller rises and dips in incoming voltage by using an isolation transformer that filters incoming electric power.

Line conditioners aren't usually seen as standalone devices but instead are found in UPS systems, discussed next.

Uninterruptible Power Supply (UPS)

An uninterruptible power supply (UPS) is a device that produces a continuous supply of electric power. A UPS can be thought of as a line conditioner with a battery or bank of batteries connected to it, so that it functions both as a line conditioner but also as a temporary supply of electric power.

UPS systems do require maintenance on its batteries, which must be checked from time and replaced every few years. Also, it is common to load-test a UPS by actually shutting off the power feed to the UPS to see whether it will actually support the equipment that it supplies power to.

The period of time that a UPS can serve as a source of electricity depends entirely upon the storage capacity of its batteries and on the electric load of the equipment it supplies power to. The shortest period of time commonly used ranges from a low of 10–15 minutes, which is enough time to either shut down the equipment or start an electric generator (discussed in the next section), to as long as several hours. Regardless, a UPS system is considered a short to medium time interval substitute for utility-supplied electric power.

Electric Generator An electric generator is a device that consists of an internal combustion engine (usually diesel-powered, but also natural gas or gasoline) that is connected to a generator—the engine-generator combination is simply called a generator. They vary greatly in size from a few hundred watts to thousands of kilowatts.

A generator will usually be switched off and idle except when utility power fails, at which time the generator is started. It can take as long as a few minutes for a generator to be started and be ready to assume the full electric load. Because of this, a facility that utilizes vital computing equipment will have both a UPS system plus an electric generator. When utility power fails, the UPS system will supply a continuous supply of electricity to computer equipment. If utility power is not restored within a minute's time, the electric generator will be started, and within a few more minute the generator will supply electricity to the facility. After utility power is restored, the generator will run a few minutes longer (to make sure utility power will remain) and then shut down.

A generator can be run almost continually for long periods of time during extended power outages. But at facilities such as Tier IV Internet data centers, two or more generators will be used, permitting on-site power generation for even several weeks if necessary, provided a sufficient fuel supply. An electric generator that provides electricity for a work site is shown in Figure 8-17.

Redundant Controls

Some facilities will have a demand for higher than the typical availability and reliability from its environmental control equipment. These facilities include:

- Larger buildings
- Buildings containing a large quantity of information systems
- Buildings containing business-critical information systems

Redundant control systems enable the facility to continue operating even if one of the components fails. All of the control systems can be duplicated, although the duplication may be expensive in some cases. A facility can have:

- Dual electric power feeds
- Redundant generators
- Redundant UPS systems
- Redundant HVAC systems

A term often used to describe this redundancy is "N+1." This means that if a building has a need for "N" control systems, then having N+1 systems means there is some redundancy that will enable the facility to continue operating even if one of the control systems fails completely.

Figure 8-17 Electric generator produces electric power when utility power is unavailable

Photo by Rebecca Steele

Chapter Summary

- A site access control strategy should consider a defense-in-depth approach.
- Key cards are a preferred method for personnel access control because they can be deactivated at any time and because all accesses are logged.
- A PIN pad in conjunction with a key card can provide a stronger access control for sensitive areas.
- Biometrics are a stronger access control method that utilizes some unique measurement of a person's body such as a fingerprint, hand print, or iris scan.
- Metal keys can also be used for personnel access control, but should only be used by the fewest possible number of personnel and only as an emergency means for accessing a building in the event the primary access system fails.
- A mantrap is an access control that consists of a set of two doors, one after the other, where only one door can be open at a time.
- Guards are trained personnel who protect a facility and manage the entry and exit of personnel and visitors. The advantage of guards is their judgment and versatility.

- Guard dogs improve site security through their ability to deter and apprehend intruders.
- Access logs are the records that show all successful and unsuccessful entrances by personnel and visitors.
- Fences and walls can be used to keep intruders away from a facility. A height of 3–4 feet keeps casual trespassers away, while a height of 6–7 feet is too high to climb easily. A fence or wall that is at least eight feet in height and contains three strands of barbed wire or razor wire is sufficient to deter even the most determined intruders.
- Video surveillance is used to observe site perimeters, entrances and exits, and control points.
  Video signals from cameras can be viewed in real-time and/or recorded for later use.
- Intrusion and motion alarm systems utilize sensors that detect entry through doors and windows and motion in a room or corridor, and send an alarm signal if intrusion or motion is detected.
- Visible notices such as "No Trespassing" signs deter persons from entering a facility.
- Exterior lighting reduces the ability for an intruder to work under cover of darkness. Critical areas should be illuminated with at least 2 foot-candles of power at a height of 8 feet.
- Bollards and crash gates restrict the movement of vehicles.
- A business should be located in an area that is reasonably free of hazards and threats.
- Natural threats include floods, landslides, avalanches, earthquakes, volcanoes, tsunamis, and severe weather.
- Man made threats include chemical spills, transportation corridors, utilities, social unrest, and nearby military bases.
- Other siting issues include building construction techniques and materials, building marking, loading and unloading areas, and shared-tenancy.
- Business equipment should be physically secured to prevent theft.
- Laptop computers should be issued with cable locks. Personnel should be trained on safe and unsafe use of laptop computers.
- Sensitive documents should be locked away and safely and securely discarded.
- Organizations should institute a "clean desk" policy so that personnel do not leave sensitive documents where others can find them.
- Records of equipment leaving and entering a facility should be maintained.
- Equipment should be protected from damage by water with water sensors, drains, and sump pumps. Racks and free standing shelving should be braced to protect them from topping over.
- Fire prevention equipment is a necessary part of disaster recovery. Organizations need to have smoke detectors, fire extinguishers, fire alarms, and fire suppression systems such as sprinklers and gaseous discharge systems. These are required by law in most locations.
- Cabling should be protected from unauthorized access. Because an organization cannot protect cabling that is a part of a common carrier's network, other means such

as route diversity and encryption should be used to protect sensitive transmissions over common carrier networks.

- Heating, Ventilation, and Air Conditioning (HVAC) systems control the temperature and humidity of air in buildings.
- Line conditioners remove the undesirable anomalies from incoming electric power such as spikes, surges, and noise.
- Uninterruptible Power Supplies (UPSs) provide a continuous supply of electric power, even when utility power has failed.
- On-site electric generators can produce electric power for extended periods of time in the event utility power has failed for even as long as several days.
- Facilities that cannot tolerate downtime due to the failure of HVAC, UPS, or generators should consider redundant, or "N+1," environmental controls.

Key Terms

Access log A record that contains building or computer access attempts.

Alarm system A system of sensors and a control unit that is designed to detect intrusions into a building or room and send an alarm signal if an intrusion is detected.

Bollard A heavy upright post used to restrict vehicle traffic.

Card reader A device used to read the contents of a key card.

Closed Circuit Television (CCTV) A standard for the transmission of video signals over a cable, often used in video surveillance systems. See also *IP camera*.

Crash gate A movable device that can be used to restrict the entry or exit of a vehicle.

Diverse network routing A network design strategy where two or more separate circuits to a given location will be located in different areas. If a mishap severs one of the circuits, communication will continue via the other circuit(s).

Fire alarm An alarm system that warns human occupants of the presence of a nearby fire.

Fire extinguisher A portable fire suppression device that sprays liquid or foam onto a fire.

Gaseous fire suppression An installed system of pipes and nozzles that sprays a fire-retardant gaseous substance into a room.

Guard See *security guard*.

Guard dog A dog that is employed to guard against or detect unwanted or unexpected personnel.

Heating, ventilation, and air conditioning (HVAC) A system that is used to control the temperature and humidity in a building or a part of a building.

Humidity A measurement of the amount of water vapor in the air.

IP Camera A video surveillance camera that sends its video signal over a TCP/IP data network.

Key card A credit card-sized plastic card with a magnetic stripe or embedded electronic circuit encoded with data that uniquely identifies the cardholder, and generally used to access restricted areas in a facility.

Line conditioner A device that filters or removes some of the undesirable anomalies in an incoming power feed.

Mantrap A set of interconnected double doors used to control the entrance or exit of personnel.

PIN pad A numeric keypad that is typically used in connection with an access control system.

Pull station A manually operated device that is used to trigger a building fire alarm.

Relative humidity The amount of water vapor in a sample of air compared to the maximum amount of water vapor that the air can hold.

Secure siting Locating a business at a site that is reasonably free from hazards.

Security guard A trained person who is responsible for protecting building assets and controlling access to the building.

Smoke detector A device that detects the presence of combustion-related smoke and contains or is connected to an audible warning alarm.

Sprinkler system An installed system of piping and nozzles used to spray water or foam onto a fire.

Video surveillance system A system that consists of monitors and/or recording equipment plus one or more video cameras, which together are used to observe and/or record activities such as personnel movement.

Review Questions

1. An organization has issued metal keys to its employees and has recently suffered some after hours employee thefts. The organization should consider acquiring:
   a. PIN pads
   b. Guards
   c. A key card entry system
   d. Mantraps
2. An organization that is setting up a key card entry control system should:
   a. Establish different zones and determine which personnel should be able to access each zone
   b. Establish one zone and assign all personnel to the zone
   c. Determine, for each employee, whether they should be able to access each controlled door
   d. Permit employees to access all general-entrance doors and issue metal keys to more sensitive areas

3. An organization needs to keep determined intruders away from its facility. The organization should install:
   a. Fencing that is six to seven feet high
   b. Fencing that is six to seven feet high with three strands of barbed wire
   c. Fencing that is six to seven feet high with three strands of razor wire
   d. Fencing at least eight feet high with three strands of razor wire
4. A video surveillance system that does not have the ability to record:
   a. Is adequate as a detective control
   b. Is adequate as a deterrent control
   c. Must be continuously attended and monitored by security personnel
   d. Is adequate as a preventive control
5. An organization that wishes to implement additional deterrent controls should consider:
   a. An intrusion alarm system
   b. A key card entry control system
   c. "No Trespassing" signs
   d. Fencing
6. A business is considering relocating to another city. The selection criteria for a new site should include:
   a. The proximity to possible social unrest events
   b. Proximity to man made threats
   c. All of these
   d. Proximity to natural threats
7. In a facility with workers and computing equipment, the appropriate range for humidity should be:
   a. Between 30% and 50%
   b. Between 50% and 70%
   c. Between 20% and 40%
   d. Less than 20%
8. An organization has a computer facility that is powered by utility power and a generator. When utility power fails:
   a. Personnel will have to start the generator to restore power
   b. Power to computing equipment will dip slightly and then be restored
   c. Power to computing equipment will be down for 1-2 minutes, then restored
   d. Power to computing equipment will not be interrupted

9. An organization experiences many transients, surges, and dropouts in its utility power. In order to prevent damage to its computer equipment, the organization should install:
   a. Line conditioner
   b. Uninterruptible power supply (UPS)
   c. Electric generator
   d. Power distribution unit (PDU)
10. A commercial Internet hosting facility advertises that it has "N+2" HVAC systems. This means that:
   a. One more HVAC unit than is needed to provide cooling to the entire facility
   b. Two more HVAC units than are needed to provide cooling to the entire facility
   c. Spare parts on-hand for two HVAC units
   d. Twice the HVAC capacity than is needed to provide cooling to the entire facility
11. The primary purpose for earthquake bracing is:
   a. Protection of human life
   b. Protection of computing equipment
   c. Protection of network infrastructure
   d. Protection from excessive lateral movement
12. The hazard from natural threats:
   a. Damage to supporting infrastructure
   b. Direct damage to facilities and equipment plus damage to supporting infrastructure
   c. Direct damage to facilities and equipment
   d. Damage to communications facilities
13. The NIST standard for outdoor lighting requires:
   a. At least 2 lumens of power to a height of 8 feet
   b. Lights no more than 50 feet apart
   c. At least 6 foot candles of power to a height of 8 feet
   d. At least 2 foot candles of power to a height of 8 feet
14. Video surveillance is generally appropriate in all of the following areas except:
   a. Employee cubicles and offices
   b. Loading docks and storage areas
   c. Computer rooms and data closets
   d. Power control rooms

15. A corporation is considering leasing office space in a shared tenant building. The security manager has expressed a concern regarding building access control. The most likely cause of the concern is:
    a. Shared management of a building access management system
    b. Common access to corridors and stairwells
    c. Common access to video surveillance data
    d. Common access to workspaces

Hands-On Projects

Project 8-1: Site Review of Video Surveillance System

In this project you will perform a survey of the video surveillance system at your school, place of work, or other business location.

In order to avoid drawing suspicion, you should first ask for permission to perform this survey beforehand. You should not enter any restricted areas unless you are escorted or have explicit permission.

1. Visit your school, place of work, or other business.
2. Observe grounds and building entrances and note any video cameras that may be present. If possible determine whether each is a fixed camera or if it is the pan/tilt/zoom type.
3. Note the interior and exterior areas that appear to be lacking video surveillance.
4. Prepare a short written report with your findings and recommendations.

Project 8-2: Site Review of Building Access System

In this project you will perform a survey of the access management system at your school, place of work, or other business location.

In order to avoid drawing suspicion, you should first ask for permission to perform this survey beforehand. You should not enter any restricted areas unless you are escorted or have explicit permission.

1. Visit your school, place of work, or other business.
2. Observe building entrances and interior doors and note any key card readers or other controls that may be present.
3. Note any areas that appear to be lacking access controls.
4. Prepare a short written report with your findings and recommendations.

Project 8-3: Perform a Building Site Threat Analysis

In this project you will perform a survey of the access management system at your school, place of work, or other business location.

In order to avoid drawing suspicion, you should first ask for permission to perform this survey beforehand. You should not enter any restricted areas unless you are escorted or have explicit permission.

1. Visit your school, place of work, or other business.
2. Observe the building grounds and surrounding areas, as far as one quarter mile from the building.
3. Note any hazards that could pose a threat to the premises.
4. Prepare a short written report with your findings and recommendations.

Project 8-4: Perform a Dumpster Diving Analysis

In this project you will perform a survey of one or more centralized waste collection receptacles ("dumpsters") at your school, place of work, or other business location.

In order to avoid drawing suspicion, you should first ask for permission to perform this survey beforehand. You should not enter any restricted areas unless you are escorted or have explicit permission.

In some places of business, looking through waste materials may expose you to potentially hazardous materials that may cause injury, sickness, or death. You should seek the guidance of qualified and experienced personnel before putting yourself at risk.

1. Visit your school, place of work, or other business.
2. Locate one of the trash receptacles ("dumpsters") on the premises. While paying careful attention to personal safety, observe whether you can see any discarded documents or other materials that could contain potentially sensitive business information.
3. Prepare a short written report with your findings and recommendations.

Case Projects

Case Project 8-1: Research Biometric Access Controls

As a consultant with the Risk Analysis Consulting Co., you have been asked to research biometric access controls for a chemical company, Colorful Plastics.

A number of security incidents in the past year has prompted Colorful Plastics to consider using biometrics for its building access control system. Using online research, identify several biometric access control products that could be used. Consider systems that are based on fingerprint, iris scan, and hand print.

Recommend two finalists that Colorful Plastics should consider testing on-site.

Case Project 8-2: Research Document Shredding Options

As a consultant with the Information Protection Consulting Co., you have been assigned to Smokey Fire Insurance Company. Three hundred employees in this company handle paper documents with sensitive information that must be shredded when discarded. Company management has considered three options:

- Personal shredders at each desk
- Shredders near each printer
- Secure shred bins near each printer (once a week, an on-site shredding service empties these bins and shreds documents in the presence of a security guard)

Using online research, find pricing for each of these options. Create a written report that includes recommendations, noting what factors besides cost were considered.

Case Project 8-3: Video Surveillance Upgrade

As a consultant with the Seeing Eye Security Advisors Co., you have been asked to develop a plan for upgrading the video surveillance system for your client, a small high-tech manufacturing company. Recent thefts of high-value materials have prompted the client to upgrade its video surveillance system in order to be able to identify and apprehend the person(s) who are stealing materials.

Today, your client's video system includes fixed cameras in the building's main lobby and in the computer room. The video surveillance controller can accept video signal inputs from a maximum of four cameras. No surveillance capability exists for any of the other building entrances, the grounds, the shipping and receiving area, or the high-value materials storage areas.

Using online research, identify candidate video surveillance systems with recording and real-time viewing capabilities that can take inputs from several cameras. Create a written report that includes candidate systems and your recommendations.

chapter 9

Security Architecture and Design

Topics in this Chapter:

- Security models including Biba, Bell LaPadula, Access Matrix, Take-Grant, Clark-Wilson, Multi-Level, Mandatory Access Control, and Discretionary Access Control
- Information systems evaluation models including Common Criteria, TCSEC, ITSEC
- Computer hardware architecture
- Computer software: operating systems, applications, and tools
- Security threats and countermeasures

The (ISC)^2 *Common Body of Knowledge* (CBK) defines the key areas of knowledge for Security Architecture and Design in this way:

The Security Architecture and Design domain contains the concepts, principles, structures, and standards used to design, implement, monitor, and secure, operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity, and availability.

The candidate should understand security models in terms of confidentiality, integrity, information flow; system models in terms of the Common Criteria; technical platforms in terms of hardware, firmware, and software; and system security techniques in terms of preventative, detective, and corrective controls.

Key areas of knowledge:

- *Understand the theoretical concepts of security models*
- *Understand the components of information systems evaluation models*
- Understand security capabilities of computer systems
- *Understand how the security architecture is affected by*

  Covert channels

  States attacks (e.g., time of check/time of use)

  Emanations

  Maintenance hooks and privileged programs

  Countermeasures

  Assurance, trust, and confidence

  Trusted computer base (TCB), reference monitors and kernels

The title of this chapter is "Security Architecture and Design," the name for Domain 9 of the CISSP Common Body of Knowledge (CBK). However, the subject matter in this chapter is a good deal bigger than that. This domain contains the loosely related topics of:

- Abstract security models
- Information system evaluation criteria
- Computer system architecture
- Software

Security Models

In the context of this chapter, a *model* is a simplified representation used to explain a real-world system. In the natural sciences, models are used as a means for understanding some phenomenon in nature. In data security it's the other way around: models are used as the basis for the design of a security mechanism that can be used to protect secrets.

Several security models are discussed in this section, roughly in the chronological order of their development. They are:

- Bell LaPadula
- Biba
- Clark-Wilson
- Access matrix
- Multi-Level
- Mandatory access control (MAC)
- Discretionary access control (DAC)
- Role-based access control (RBAC)
- Non-interference
- Information flow

When designing a new information system (or the access model for a new or existing system), a system developer may wish to use a security model in order to build or choose an access model that will fulfill the system's security access requirements. Similarly, an analyst or developer who is studying an existing security system might wish to compare the system to security models in order to better understand the system.

Bell-LaPadula

Published in 1973, the **Bell-LaPadula** model is a *state machine* model that addresses the *confidentiality* of information. This **data confidentiality model** was developed to formalize and explain the DoD multilevel security policy.

In the Bell-LaPadula model, a subject can read all documents at or below his level of security, but he cannot read any documents above his level of security. This is called *no read-up*, or *NRU*. This prevents a subject from learning secrets at a higher level than his own. For example, a diplomat can read documents intended for common citizens but cannot read documents intended for the President.

In the model, a subject can write (create/modify) documents at or above his level of security, but he cannot write documents below his level. This is called *no write-down*, or *NWD*. This prevents a subject from accidentally leaking secrets at his level into a document at a lower level. For example, a diplomat can write documents intended for the President but cannot write documents for common citizens, out of the concern that the diplomat may accidentally leak sensitive information to the common citizens.

Bell-LaPadula had one shortcoming that is addressed by the Biba model.

Biba

The **Biba** model was published in 1977, a few years after the Bell-LaPadula model, and after a lot of people in the security community had opportunities to discuss it and put it into practice. Biba is often considered the first formal integrity model because it prevents modifications to data by unauthorized persons. For that reason Biba is called a **data integrity model**.

Biba addresses a shortcoming in the Bell-LaPadula model whereby a subject at a lower security level is able to overwrite and potentially destroy secret information at a higher level.

In the Biba model, a subject cannot read documents below his level. This is called *no read-down*, or *NRD*. For example, a diplomat can read documents written by the President but cannot read documents read by common citizens.

Further, a subject cannot write documents above his level. This is called *no write-up*, or *NWU*. For example, a diplomat can write procedures to be written by common citizens but cannot write procedures to be read by the President.

Neither the Bell-LaPadula nor the Biba are perfect security models; each has its shortcomings and advantages. Principles from each can be used to construct other security models and mechanisms.

Clark-Wilson

Clark-Wilson is a **data integrity model** that was published in 1987 as a rebuttal to the Bell-LaPadula and Biba models, which Clark and Wilson argued were more suited for confidentiality than integrity. The Clark-Wilson model consists of two principals: authenticated users, programs (called *transformation procedures*, or TPs); which operate on two types of data items: *unconstrained data items* (UDIs), and *constrained data items* (CDIs). One type of TP, called an *integrity verification procedure* (IVP), is used to transform UDIs into CDIs.

In the model there are two sets of rules: *certification* (C) rules and *enforcement* (E) rules:

- C1—an IVP must ensure that CDIs are valid.
- C2—for a given CDI, a TP must transform the CDI from one valid state to another valid state.
- C3—*allowed relations* (or *triples* that consist of a user, a TP, and one or more CDIs) must enforce separation of duties.
- C4—TPs must create a transaction log that contains all transaction details.
- C5—TPs that accept a UDI as input may perform only valid transactions on the UDI (to convert it to a CDI) or reject the UDI.
- E1—the system must permit only the TPs certified to operate on a CDI to actually do so.
- E2—the system must maintain the associations between users, TPs, and CDIs. The system must prevent operations outside of registered associations.
- E3—every user must be authenticated before they may run a TP.
- E4—only a TP's certifier may modify its associations.

Access Matrix

An **access matrix** security model consists of a two-dimensional matrix that defines which subjects are permitted to access which objects. An example access matrix appears in Table 9-1.

Subject	Directory: Contracts	Directory: Personnel	Process: Expense Reports
Warren	Read	Read	Submit
Wilson	None	None	Approve
Wyland	Read/Write	None	Submit
Yelte	Read/Write	None	None

Table 9-1 Sample access matrix

Multi-level

The **multi-level** security model is one in which a system will have several levels of security and be used by persons of varying levels of security clearances, where the system will control access to objects according to the clearance level of subjects.

For example, a file server contains documents at three different levels of security: Confidential, Secret, and Top Secret. The users of the system are registered as having one of three levels of clearance: Confidential, Secret, and Top Secret. A user with Secret clearance can view documents at Confidential and Secret levels, but not Top Secret. A user with Confidential clearance can only view Confidential documents. A user with Top Secret clearance can view all documents. This is illustrated in Table 9-2.

Mandatory Access Control (MAC)

Mandatory access control (**MAC**) describes a system (such as an operating system) that controls access to resources. When a subject (which could be a program, process, or thread) requests access to an object (which could be a file, device, stream, or port), the system examines the subject's identity and access rights together with the access permissions associated with the object. The system will then permit or deny the requested access.

Discretionary Access Control (DAC)

In the **discretionary access control** (**DAC**) model, the owner of an object controls who and what may access it. DAC is so-named because permission to access an object is made at its owner's discretion.

User Access Level	Authorized to View
Top Secret	Top Secret Secret Confidential
Secret	Secret Confidential
Confidential	Confidential

Table 9-2 Multi-level access

DAC is common in information systems where owners of files, directories, web pages, and other objects can set access permissions on their own, to control which users or groups of users may access her objects.

Role-Based Access Control (RBAC)

Role-based access control (RBAC) is usually used to simplify the task of managing user rights in a complex system that contains many objects and users.

Instead of managing the access rights of individual users, an RBAC-based system relies on the existence of roles, which contain collections of allowed accesses. Each user is then assigned to one of the established roles, and each user then inherits the rights defined by the role to which he is assigned.

For example, a financial accounting application in a corporation will have hundreds or even thousands of access controls. The application will have several pre-defined roles such as *Accounts Payable Clerk*, *Account Payable Manager*, *Accounts Receivable Clerk*, *Accounts Receivable Manager*, *Corporate Controller*, and many others. Each role contains all of the access rights required by a person assigned to the role.

Non-Interference

The **non-interference** model states, in fairly abstract terms, that low inputs and outputs will not be altered by any high inputs or outputs. In other words, a user with low clearance cannot gain any knowledge of any activities performed by high-clearance users. The term *non-interference* means that activities performed by a user with high clearance will not interfere with any activities performed by a user with low clearance.

Information Flow

Information flow models are based upon the flow of information rather than upon access controls. Objects are assigned to a class or level of security, and the flow of these objects is controlled by a security policy that specifies where objects of various levels are permitted to flow.

Information Systems Evaluation Models

It is insufficient for an organization to build a system and simply assert that it is secure. An organization that is concerned about security is not likely to put much credibility in such an assertion. But how can an organization reliably test a system?

Several evaluation models and frameworks have been established for the purpose of objectively evaluating the security (that is, the confidentiality, integrity, and availability) of a system. The frameworks discussed in this section are:

- Common Criteria
- TCSEC
- TNI
- ITSEC

- SEI-CMMI
- SSE-CMM

The general processes of certification and accreditation are also discussed in this section.

Common Criteria

Common Criteria for Information Technology Security Evaluation is usually known as just the **Common Criteria** or *CC*. This is the formal name for the international standard, **ISO 15408**. The Common Criteria is a framework for the specification, implementation, and evaluation of a system against a given set of security requirements.

Common Criteria supersedes TCSEC and ITSEC.

A system called a **Target Of Evaluation** (**TOE**) is evaluated against one of seven **Evaluation Assurance Levels** (**EALs**), which are:

- EAL1: Functionally Tested.
- EAL2: Structurally Tested.
- EAL3: Methodically Tested and Checked.
- EAL4: Methodically Designed, Tested, and Reviewed.
- EAL5: Semiformally Designed and Tested.
- EAL6: Semiformally Verified Design and Tested.
- EAL7: Formally Verified Design and Tested.

Evaluation of a system to CC standards is both expensive and time-consuming. According to the U.S. General Accounting Office (GAO), evaluation at levels EAL2 through EAL4 can take as long as two years and cost as much as US$350,000. See Figure 9-1.

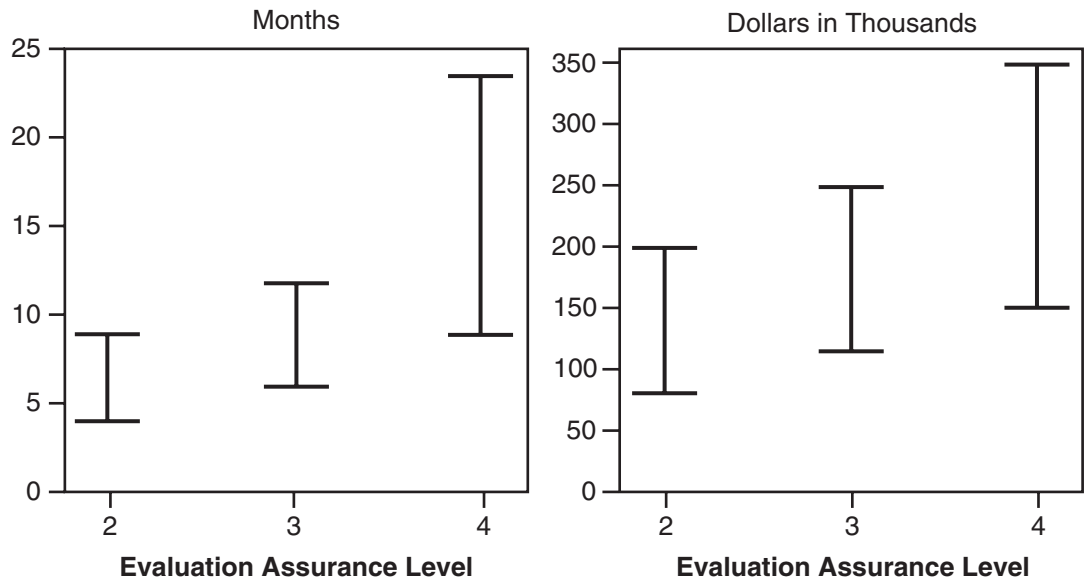


Figure 9-1 Evaluation of a system to various assurance levels of the Common Criteria requires considerable time and cost

Source: Courtesy the United States Government Accounting Office

TCSEC

The **Trusted Computer Security Evaluation Criteria** (**TCSEC**) is the system evaluation criteria that address confidentiality of information. Developed by the U.S. Department of Defense in the 1980s, TCSEC is commonly known as the *Orange Book*, which is a part of the *Rainbow Series*.

TCSEC defines four main levels, plus sub-levels of security protection:

- **A**—Verified Protection
- **B**—Mandatory Protection
- **B3**—Security domains
- **B2**—Structured protection
- **B1**—Labeled security
- **C**—Discretionary protection
- **C2**—Controlled access
- **C1**—Discretionary protection
- **D**—Minimal security

TCSEC has been superseded by the Common Criteria.

Trusted Network Interpretation (TNI)

The **Trusted Network Interpretation** (**TNI**) evaluation criteria is known as the *Red Book* in the Rainbow Series. TNI is used to evaluate confidentiality and integrity in trusted communications networks.

ITSEC

Information Technology Security Evaluation Criteria (**ITSEC**) is the European standard for the security evaluation of systems. Whereas TCSEC addresses only data confidentiality, ITSEC addresses confidentiality as well as integrity and availability.

ITSEC uses two sets of security levels (functionality and evaluation) that map to TCSEC's levels. See Table 9-3 for a side by side comparison of TCSEC and ITSEC levels.

ITSEC has also been superseded by the Common Criteria.

SEI-CMMI

The Software Engineering Institute at Carnegie-Mellon University developed a model to objectively assess the maturity of an organization's systems engineering practices. The model is called the **Software Engineering Institute Capability Maturity Model Integration** (**SEI CMMI**).

The objective of an organization's assessment is to arrive at a rating of maturity levels, which are:

- **Level 0—Incomplete.** Processes are incomplete and many activities are performed ad hoc if at all.
- **Level 1—Performed.** Processes are documented and performed.

ITSEC Functionality Level	ITSEC Evaluation Level	TCSEC Level
NA	E0	D
F-C1	E1	C1
F-C2	E2	C2
F-B1	E3	B1
F-B2	E4	B2
F-B3	E5	B3
F-B3	E6	A1
F-IN	NA	TOEs with high integrity requirements
F-AV	NA	TOEs with high availability requirements
F-DI	NA	TOEs with high integrity requirements during data communication
F-DC	NA	TOEs with high confidentiality requirements during data communication
F-DX	NA	Networks with high confidentiality and integrity requirements

Table 9-3 Comparison of ITSEC and TCSEC security levels

- **Level 2—Managed.** Processes are managed and supported with skilled workers and tools.
- **Level 3—Defined.** Processes are defined according to a standard process framework model.
- **Level 4—Quantitatively Managed.** Processes are measured and managed according to the results of those measurements.
- **Level 5—Optimizing.** Processes are measured and changed over time in order to improve them.

SSE-CMM

The **Systems Security Engineering Capability Maturity Model (SSE CMM)** is a process evaluation reference model that is focused on the requirements for implementing security in a system. Developed by the International Systems Security Engineering Association (ISSEA), SSE-CMM has five levels of performance, which are:

- Capability Level 1—Performed Informally
- Capability Level 2—Planned and Tracked
- Capability Level 3—Well Defined
- Capability Level 4—Quantitatively Controlled
- Capability Level 5—Continuously Improving

Certification and Accreditation

Certification and accreditation, sometimes coined C&A, are the processes used to evaluate and approve a system for use. These activities are not generally seen in average businesses, but instead are found in government and military environments, and also in highly regulated industries such as pharmaceuticals and aeronautics.

C&A is a two-step process:

- **Certification** is the process of evaluation of a system's architecture, design, and controls, according to established evaluation criteria.
- **Accreditation** is the formal management decision to approve the use of a certified system.

Five standards for certification and accreditation are discussed in this section: FISMA, DITSCAP, DIACAP, NIACAP, and DCID 6/3.

FISMA **Federal Information Security Management Act of 2002** (**FISMA**) is a law that requires all U.S. federal information systems to conform to security standards and processes used to evaluate them.

The compliance process required by FISMA includes the following steps:

- **Determine Scope.** In other words, define the components and boundaries of a system and the subsequent assessments that will take place.
- **Determine the Information Types.** It is necessary to know what kinds of information will be present in the system (whether stored in, transmitted through, or both). This includes performing a FIPS-199 Categorization of information.
- **Document the System.** This includes the full collection of documents that describe the system including architecture, design, hardware and software components, connections, and procedures for building, operating, and maintaining.
- **Risk Assessment.** A comprehensive identification of threats, vulnerabilities, impact, and steps available to mitigate threats and vulnerabilities.
- **Implement Security Controls.** Once the architecture, types of information, and risks of a system are known, security controls can be established.
- **Certification.** This is the formal evaluation of the system to confirm that it has been built as intended.
- **Accreditation.** This is the formal decision to allow use of the system.
- **Continuous Monitoring.** Once the system has been placed into operation, it must be continuously monitored to ensure that it is performing adequately and correctly.

DITSCAP **Department of Defense Information Technology Security Certification and Accreditation Process** (**DITSCAP**) is the process used to certify and accredit information systems used by the U.S. military.

The four phases of the DITSCAP process are:

- System Definition
- Verification

- Validation
- Re-Accreditation

In 2006 DITSCAP was superseded by DIACAP, which is discussed next.

DIACAP The **Department of Defense Information Assurance Certification and Accreditation Process (DIACAP)**, is the successor to DITSCAP, and is used to certify and accredit military information systems.

The steps in the DIACAP process are:

- Initiate and plan information assurance (IA) C&A
- Implement and validate information assurance (IA) controls
- Certify and accredit the system
- Maintain authorization to operate system and conduct reviews
- Decommission

NIACAP **National Information Assurance Certification and Accreditation Process (NIACAP)** is the process used to certify and accredit systems that handle U.S. national security information. It is modeled after the DITSCAP that is discussed earlier in this section.

The phases of a NIACAP certification and accreditation are:

- Definition
- Verification
- Validation
- Post accreditation

NIACAP is administered by the U.S. National Security Agency.

DCID 6/3 **Director of Central intelligence Directive 6/3 (DCID 6/3)** is the process for protecting sensitive compartmented information within information systems at the U.S. Central Intelligence Agency (CIA). This directive defines security standards, classification levels, and the C&A process for certifying and accrediting information systems.

DCID 6/3's process for C&A includes these steps:

- Perform Certification Evaluation
- Perform Security Testing
- Identify Shortfalls
- Define Vulnerabilities
- Conduct Risk Analysis
  - Identify and Prioritize Risks
  - Identify additional Counter-measures
  - Make risk assessment recommendations
- Develop Certification Package
- Obtain interim approval to operate, if applicable
- Obtain Accreditation

Computer Hardware Architecture

This section describes the hardware architecture used in contemporary computer systems. While it may, at first, seem irrelevant to security, it is asserted that a security manager must fully understand how every facet of information systems works, including the underlying hardware. The security manager is explicitly responsible for the protection of information and information systems; a working knowledge of every facet and layer of the organization's information systems is necessary in order to be able to protect it.

Computers contain several components including:

- Central processor
- Bus
- Main storage
- Secondary storage
- Communications
- Firmware

Other components and concepts related to computer architecture that are discussed in this section are **Trusted Computing Base** and **Reference Monitor**.

Central Processor

The **central processing unit** (**CPU**) is the portion of a computer where program instructions are executed. Historically, CPUs consisted of discrete components (transistors, resistors, capacitors, diodes, and so on) on circuit boards, but starting in the 1970s, CPUs were constructed from integrated circuits (ICs) and in that form they were often known as *microprocessors*.

Components

CPUs have a number of components including:

- **Arithmetic logic unit** (**ALU**). This is where arithmetic and logic operations are performed.
- **Registers.** These are temporary storage locations that are used to store the results of intermediate calculations. A CPU can access data in its registers far more quickly than main memory.
- **Program counter.** A register that keeps track of which instruction in a program the CPU is currently working on.
- **Memory interface.** This is the circuitry that permits the CPU to access main memory.

Operations

CPUs do a computer's work by performing the instructions in computer programs. They do this by performing a small number of basic operations which are:

- **Fetch.** The CPU fetches (retrieves) an instruction from memory.
- **Decode.** The CPU breaks the instruction into its components: the *opcode* (or *operation code*—literally, the task that the CPU is expected to perform) and zero or more *operands*, or numeric values that are associated with the opcode (for example, if the CPU is to add to numbers together, the opcode will direct an addition, and two opcodes will be the two numbers to add together),

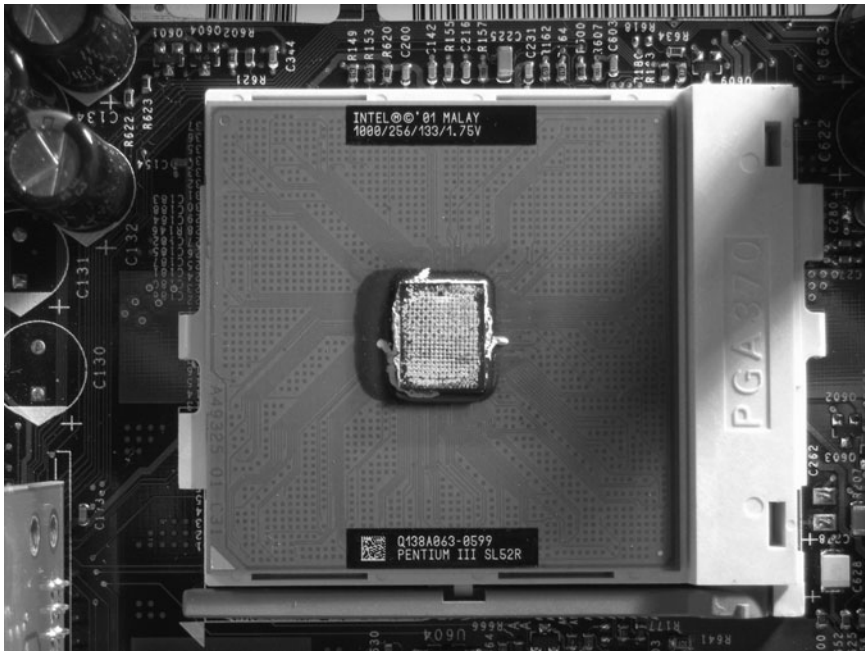


Figure 9-2 Typical CPU

Photo by Rebecca Steele

- **Execute.** This is the actual operation as directed by the opcode.
- **Writeback.** The CPU writes the result of the opcode (for instance, the sum of the two numbers to add together) to some memory location.

Instruction Sets Each type of CPU has an *instruction set*—the set of instructions or opcodes that it can use to run a program. Some of the common instruction set models in use are:

- **CISC (Complex Instruction Set Computer)**—a microprocessor architecture in which each instruction can execute several operations in a single instruction cycle. Earlier microprocessors had larger instruction sets to more closely match the semantics of high-level languages. Examples include VAX, PDP-11, Motorola 68000, and Intel x86.
- **RISC (Reduced Instruction Set Computer)**—a newer microprocessor design where the CPU has a smaller (reduced) instruction set that permits it to be more efficient. Examples include SPARC, Dec Alpha, MIPS, and Power PC.
- **Explicitly Parallel Instruction Computing (EPIC)**—a microprocessor that permits parallel execution in a single CPU. The prime example in use is the Intel Itanium.

Single Core and Multi-Core Designs Microprocessor CPUs began as single core designs; that is, the CPU die consisted of a single processor unit. Newer *dual-core* CPUs have two independent CPUs present on a single die. There are also quad-core and eight-core CPU designs.

Single and Multi Processor Computers While end-user workstations generally have only one CPU (whether single- or dual-core, as discussed earlier), servers can have several, even dozens or hundreds of CPUs. There are two main types of multi processor designs: symmetric and asymmetric.

- **Symmetric multiprocessing (SMP).** This is a computer architecture where two or more CPUs are connected to the computer's main memory. An operating system that supports SMP can easily move tasks among CPUs in order to improve computing efficiency and throughput. Most multiprocessor systems use the SMP model.
- **Asymmetric multiprocessing (ASMP).** This computer architecture employs an asymmetrical design that may be built on the theme of master- and slave-processors, processors of different types, or processors that are dedicated to specific tasks. ASMP has fallen out of favor, so much so that no current operating system supports ASMP.

CPU Security Features CPUs contain security features that offer protection of processes and information and improve the integrity of a running system. Some of these features are:

- **Protected mode.** This is a feature wherein the CPU itself prevents a process from being able to attempt to access the memory space assigned to another running process.
- **Executable space protection.** This refers to any of several mechanisms that prevent the execution of data. A running computer program consists of instructions (the program) and data (stored variables); executable space protection prevents the CPU from executing instructions that reside in data.

Bus

A computer's **bus** is a subsystem used to transfer data among the computer's internal components, including its CPU, storage, network, and peripherals. A bus can also be used to transfer data between computers.

A computer bus is really a high-speed network that facilitates communication among the computer's internal components. This communication may be token-based (like a token ring network), synchronous (like an ATM network), or interrupt-driven.

Contemporary computers often have more than one bus—one or more for communication with high-speed components such as main memory, as well as separate buses for disk I/O and peripherals.

One or more of a computer's buses usually contains connectors that permit the installation of additional components such as additional memory, storage, or peripheral devices.

A selection of internal bus architectures used over the past twenty years includes:

- **Unibus**—used by Digital Equipment Corp. PDP-11 and VAX computers.
- **SBus**—used in SPARC-based computers, including those made by Sun Microsystems.
- **Microchannel**—used by IBM in PS/2 systems as a replacement for the slower *ISA* bus.
- **PCI (Peripheral Component Interconnect)**—used by several brands in modern PCs. PCI connectors on a computer's motherboard are shown in Figure 9-3.

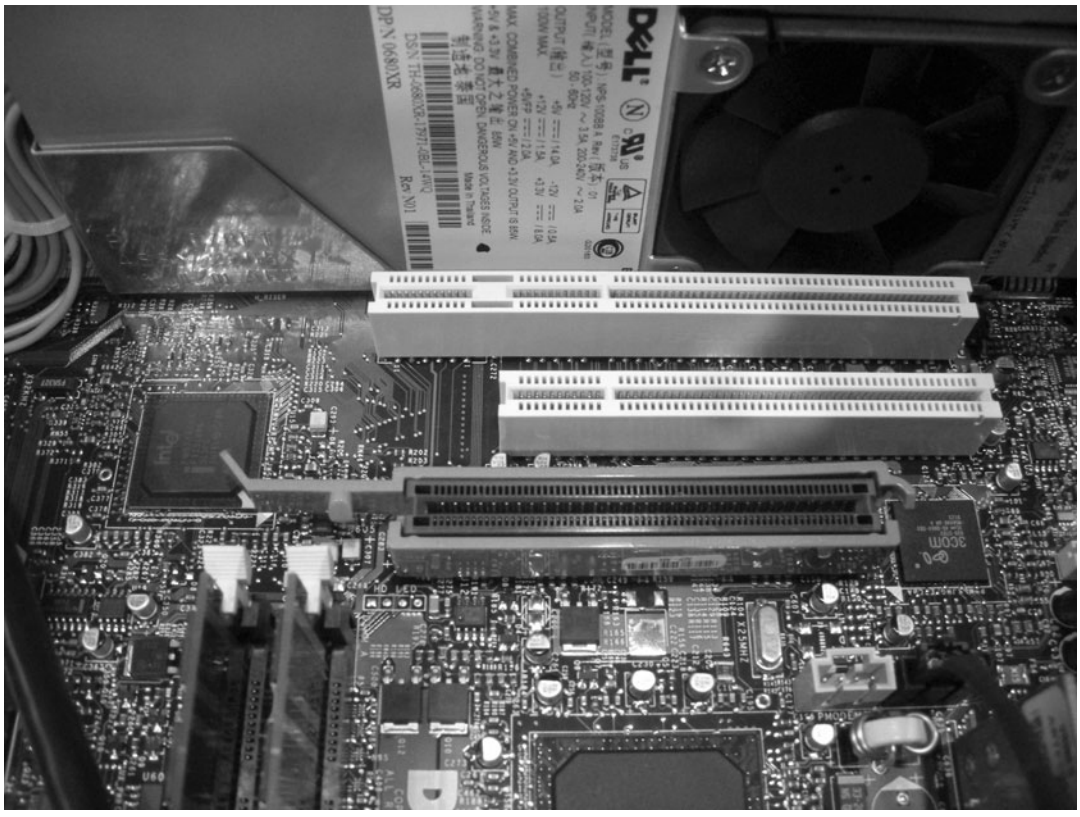


Figure 9-3 PCI bus connectors on a computer motherboard

Photo by Rebecca Steele

Some of the external bus architectures include:

- **SCSI (Small Computer Systems Interface)**—used primarily for the connection of a computer to its disk storage. Within the SCSI framework are many standards including Fast-SCSI, Fast-Wide SCSI, Ultra-SCSI, Ultra2-SCSI, and Ultra640-SCSI.
- **SATA (Serial ATA)**—used primarily for communications with disk storage.
- **IEEE1394**—Also known as **FireWire**, this is a serial bus standard used to connect high-speed external devices such as video cameras.
- **PC card**—Formerly known as PCMCIA, this standard is used for the connection of peripheral devices for laptop computers.
- **Universal Serial Bus (USB)**—This is a serial bus protocol used to connect computer peripherals such as keyboards, mice, storage devices, network adaptors, printers, scanners, and cameras.

The once-clear distinction between bus communications and network communication is blurring. With network traffic being carried over bus architectures such as USB and IEEE 1394, and bus-like traffic being carried over networks, both are forms of high-speed communications between computers.

Storage

A computer uses storage to store programs and data. There are two primary types of storage: **main storage** and **secondary storage**, which are discussed in this section. The concept of **virtual memory** is discussed as well.

Main Storage

Also known as **primary storage** or **memory**, a computer's **main storage** is used to store instructions and data being actively worked on. In contemporary computers this is also known as the computer's **RAM** (*random access memory*—a reference to the way that main storage is used).

A computer's main storage is the fastest storage: the CPU can access data in main storage far more quickly than data in secondary storage.

The purposes for main storage include:

- **Operating system.** As the arbiter of access to memory and peripherals, active parts of the operating system program code, as well as a good deal of information that the OS keeps track of including:
  - Active processes
  - Memory usage
  - I/O buffers
- **Active processes.** Each active process will occupy a portion of main storage for storage of program code and active data in use.

In most contemporary computer architectures, main memory is volatile; this means that the contents of main memory will vanish if power is removed from the computer. Secondary storage is used to store information that needs to be retained if the computer stops running or if power is removed.

Two primary technologies are in use for main storage including:

- **Dynamic Random Access Memory (DRAM)** is RAM that must be "refreshed" many times per second in order to retain the correct values stored. Some of the common packages of DRAM include SIPP (Single In-line Pin Package), SIMM (Single In-line Memory Module), DIMM (Dual In-line Memory Module), and SO-DIMM (Small outline DIMM).
- **Static random access memory (SRAM)** is RAM that needs no refresh as does DRAM. Because it draws more power and is less dense than DRAM, SRAM is usually not used for personal computer main storage, but it is sometimes found in devices such as modems and CD-ROM drives for buffer storage.

Secondary Storage

Secondary storage is the much larger and much slower means of storage used by a computer. Secondary storage is often implemented with hard disks. The reasons for secondary storage include:

- **Persistence.** Secondary storage is usually permanent; data stored in secondary storage will remain intact even if the computer is powered down or disconnected.

- **Capacity.** The available amount of storage in secondary storage is usually far greater than in main storage, by a factor of hundreds to tens of thousands.

Secondary storage is usually organized according to a structure through the use of **partitions** and **file systems**.

Partitions are a means used to divide an entire storage device into logical components that can be used for separate purposes.

A secondary storage device can also contain a **Master Boot Record** (**MBR**), which contains computer instructions that can be read into memory when a computer is powered up or restarted.

One or more of a storage device's partitions can contain a **file system**. Depending upon a few factors such as the type of hardware used and the capabilities of the operating system, a file system may include:

- Files.
- Directories that include files.
- A hierarchy of directories that include files and subdirectories, all of which can include files.

Secondary storage can also be unstructured, or *raw*. UNIX operating systems use the term *raw* for secondary storage that is used to store raw characters or blocks of data, and the term *cooked* for secondary storage that contains one or more file systems that can be accessed by the operating system, its tools, and software applications.

Virtual Memory

Virtual memory is a memory management technique whereby the operating system can permit a process's memory to become fragment and even overflow onto secondary storage without the process being aware. Virtual memory permits inactive parts of a program's memory to occupy secondary storage, which provides memory that can be used by other processes.

Operating systems employ two methods for moving a process's memory between main storage and secondary storage: **swapping** and **paging**.

Swapping

Swapping is a technique where the contents of main storage occupied by a process are written to a location in secondary storage (disk). This permits a scheme where a process that wants to run can be permitted to run, after the OS has swapped out another process.

Some operating systems are able to support a fixed number of running processes. When more processes are started, they are placed in a queue of waiting processes until one or more active processes either terminate or are swapped out. A system will experience *thrashing*, which is the severe performance degradation that occurs when too many active processes are causing excessive swapping.

Swapping was employed by early timesharing operating systems.

Paging

Paging is another approach to the problem of limited resources, where there are more processes that want to occupy main memory than can be accommodated. Instead of swapping out an entire process's memory space, only the unused parts of memory (called

"pages") are written to disk. Using this scheme, a process can be active and executing while unused parts of its memory space are not in main memory at all, but occupying disk space instead.

When an active process is running and it addresses a page of memory that is not presently occupying main memory, a **page fault** occurs. This causes the operating system to fetch the requested page from disk and place it in main memory for the process to use. In an active operating system, page faults can be occurring at a high rate (hundreds or even thousands per second) while the OS is moving requested pages in from secondary storage and moving idle pages from main memory to secondary storage.

In the Windows XP operating system, all of the system's paging data is stored in a single file, `pagefile.sys`.

Communications Computer communications are generally performed by hardware modules that are connected to the computer's bus. Because computers almost universally are equipped with means for communications, there is a separate section on the subject.

These hardware modules are usually called *adaptors, communications adaptors, communications controllers, interface cards*, or **network interface cards** (**NICs**). A typical adaptor is shown in Figure 9-4. A **network interface card** is a computer hardware component that connects the computer's bus to a communication channel or network.

Generally, a computer's bus is many times faster than external communications. Because of this, the hardware module must be able to manage the differences in communications speed as well as the differences in the style of communications between the bus and the communications medium. This is accomplished with *communications buffers*—temporary storage of data being transmitted through the hardware module, as well as the necessary logic to communicate properly on the bus and on the communications medium.

Firmware

Firmware is the term used to describe software that is embedded in persistent memory chips in the computer. Firmware generally is used to store the initial computer instructions required to put the computer into operation after power is applied to it. Instructions in firmware

Figure 9-4 Network interface card connects the bus to a communications medium

Photo by Rebecca Steele

permit the computer to begin running and load further software from secondary storage (usually a hard drive, optical disc, floppy disc, or external storage device) to complete the loading and startup of the operating system.

Firmware is used to store the *BIOS* (Basic Input-Output Subsystem) in an Intel-based PC.

Several technologies are used to store firmware including:

- **PROM (Programmable Read-Only Memory)**
- **EPROM (Erasable Programmable Read-Only Memory)**
- **EEPROM (Electrically Erasable Programmable Read-Only Memory)**
- **Flash Memory**

All of these technologies utilize the capability to store data even after power is removed. The methods used to update the data stored vary by the technology in use.

Trusted Computing Base (TCB)

The DoD Orange Book defines the **trusted computing base (TCB)** as the hardware, firmware, operating system, and software that effectively supports security policy. The Orange Book itself defines the trusted computing base as "*the totality of protection mechanisms within it, including hardware, firmware, and software, the combination of which is responsible for enforcing a computer security policy*."

Reference Monitor

A **reference monitor** is a hardware or software component in a system that mediates access to objects according to their security level or clearance. A reference monitor is an access control mechanism that is auditable: it creates a record of its activities that can be examined at a later time.

Security Hardware

Computer systems sometimes contain hardware that is used to improve the security of the entire system.

Trusted Platform Module **Trusted Platform Module (TPM)** is the implementation of a secure cryptoprocessor, a separate microprocessor in the computer that stores and generates cryptographic keys and generates random numbers for use in cryptographic algorithms. TPM is used for a variety of cryptographic functions such as disk encryption and authentication.

Hardware Authentication Many systems, particularly end-user desktop and laptop systems, have built-in user authentication hardware including:

- **Fingerprint reader.** Provides biometric-based authentication that requires the user permits the scanning of their finger in order to permit use of the system.
- **Facial recognition camera.** A small built-in camera will view the user's face and compare it to a baseline image to decide whether the current user is the same as the registered user.

Mode	Signed NDA	Proper Clearance	Formal Access Approved	Need-to-Know
Dedicated	All data	All data	All data	All data
System High	All data	All data	All data	Some data
Compartmented	All data	All data	Some data	Some data
Multilevel	All data	Some data	Some data	Some data

Table 9-4 Security modes of operation

- **Smart card reader.** A built-in smart card reader will read a user's smart card (a memory card with memory and sometimes active devices) as a part of two-factor authentication.

Security Modes

Security modes of operation is the term used to designate the type of security in place on a MAC- (*mandatory access controls*) based system containing classified information. This term is generally used only in the context of U.S. government and military systems. The modes are:

- **Dedicated security mode.** This is a system with only one level of security level. All users can access all data. All of the information on the system is at the same security level, and all users must be at or above the same level of security and have a valid need-to-know for all of the information on the system.
- **System high security mode.** Similar to dedicated security mode, except that users may access *some* data on the system based upon their *need-to-know*.
- **Compartmented security mode.** Similar to system high security mode, except that users may access *some* data on the system based upon their need-to-know plus formal access approval.
- **Multilevel security mode.** Similar to *compartmented security mode*, except that users may access some data based upon their need-to-know, formal access approval, *and* proper clearance.

These modes are illustrated in Table 9-4.

Software

Software is the overall term referring to sets of computer instructions that are built to fulfill some purpose.

Operating Systems

An *operating system* is the software that facilitates the use of application programs and tools and controls access to the computer's hardware resources. Examples of desktop operating systems are AIX, Linux, Mac OS, Solaris, and Windows.

The primary components of an operating system are:

- **Kernel**. This is the "core" software that runs on the computer to allocate resources and control processes.
- **Device drivers.** These are programs that permit the operating system and other programs to communicate with hardware devices that are a part of the computer or connected to it.
- **Tools.** These are separate programs that are used to build and maintain a system. Tools are used to change system configurations, edit files, create directories, and install other programs.

The primary functions of an operating system are:

- **Process management.** Processes are programs that are running on the computer. The operating system's process management includes the means for starting processes, allocating resources to processes, and terminating processes.
- **Resource management.** The operating system provides access to resources such as primary storage, secondary storage, and devices such as displays and external storage devices.
- **Access management.** The operating system employs authentication as well as access controls to determine whether to grant access to a specific resource such as a file or a device.
- **Event management.** The operating system responds to common events and error conditions in a variety of ways including logging, starting or stopping processes, or communicating with internal processes or external entities.
- **Communications management.** The operating system facilitates communications via the resources and devices present in the computer for that purpose.

Operating systems employ security protection: preventing one process from interfering with other processes, and controlling access to resources. Two common protection models are:

- **Privilege level.** This is a scheme where the operating system implements levels of privilege. The Windows operating system implements this through the Administrative-level privilege, user-level privilege, and guest privilege. UNIX implements this through root and non-root privilege levels.
- **Protection Ring.** This is a scheme of concentric rings, starting with Ring 0 in the center that is the highest security that the kernel uses, plus one or more additional rings where device drivers and user programs run.

These protection models are enforced by the operating system kernel.

Subsystems

A computer's operating system provides the software framework to support the use of the computer. Depending upon the intended use of the computer, some *subsystems* may be required. *Subsystems* are software programs that perform functions that are required by applications and programs. Examples of subsystems include:

- **Database management system (DBMS).** A DBMS is a software component used to manage large organized collections of data, called *databases*. Example DBMS programs include Microsoft SQL Server, IBM DB2, Oracle, and Sybase.

- **Web server.** A *web server* is a software component used to accept and process incoming requests for information that are sent from end users running browsers or other applications via *Web Services*. A web server may fulfill incoming requests by returning static content that is stored on the computer, or pass the request to an application server program running on the same computer or on a different computer.
- **Authentication server.** This is a software component that is used to provide authentication services for other programs running on the same computer, or for other computers on the network.
- **E-mail server.** An e-*mail server* is used to transmit, receive, and store e-mail messages. An e-mail server may be used to relay messages to other servers, or it may be used to store e-mail messages to be read directly by end users.
- **File server.** A *file server* is a software component that is used to store and make available directories and files to users over a network. The Windows and UNIX/Linux operating systems have basic file server capabilities built-in, and there are third-party software components available that provide advanced capabilities.
- **Directory services.** A *directory server* is a software component that provides reference services for other computers or users on the network. Examples of directory services includes:

  Domain Name Service (DNS)

  Network Information Service (NIS)

  Active Directory (AD)

  Lightweight Directory Access Protocol (LDAP)

Programs, Tools, and Applications

Applications, tools, and programs are the broad class of software that runs on computers under the control of an operating system.

- **Program.** A single set of instructions for a computer that usually reside in a single file. A program can refer either to an executable program that contains machine-readable instructions, or to the source code that contains human-readable instructions. Examples of programs that would run on an end user's computer include:

  Firefox—a web browser used to communicate with web servers

  Writer—a program used to create human-readable documents or simple web pages

  Photoshop—a program used to manipulate digital images

  Winamp—a program used to listen to audio recordings or view video recordings or broadcasts

- **Tool.** A tool is also, strictly speaking, a program, but is used for some simpler purpose in support of applications, programs, and subsystems. Example tools include:

  Compilers—programs used to create machine-readable executable programs from human-readable source-code

  Debuggers—programs used to test and debug the operation of a computer program

Defragmenters—programs used to reorganize the files stored in a file system in order to make the file system more efficient

- **Application**. A collection of programs and tools that support a business function. Example applications include:

  Financial management applications that support general ledger (GL), accounts payable (AP), accounts receivable (AR), and so on.

  Customer relationship management

  Incident management applications

  Enterprise resource planning (ERP)

  Material requirements planning (MRP) and manufacturing resource planning (MRP II)

Applications often require the support of subsystems such as database management systems (DBMSs) to manage stored data, authentication servers, directory servers, and web servers to provide users with a user interface.

Software Security Threats

A *threat* is a potential and harmful action that – if realized – can cause some harm to its target. In the realm of computer architecture and security models, there are a number of threats including covert channels, side channel attacks, state attacks, emanations, maintenance hooks and back doors, and privileged programs.

Other types of threats, such as malware, social engineering, and dictionary attacks, are discussed in several other chapters in this book.

Covert Channels

A **covert channel** is an unauthorized, hidden channel of communications that exists within a legitimate communications channel. Because many communication channels include some idle time (or space), it can be quite difficult to detect a covert channel.

There are two types of covert channels: *storage* and *timing*.

A covert storage channel involves a storage location used by a target system. The location may be a memory location, a disk sector, or a file. The unauthorized third party may be able to directly or indirectly read the storage location and gain some level of knowledge about the information stored there.

A covert timing channel uses observable timings seen in an information system to determine what is happening in the system.

Examples of covert channels include:

- **Use of unused fields.** Covert messages can be inserted into the padding or unused fields in TCP/IP packets, packets used by other protocols, or unused fields in stored or transmitted data streams.
- **Steganography.** This is the technique of hiding data within images, sounds, or video files.

Side-Channel Attacks

A **side-channel attack** is an attack on a system where a subject can observe the physical characteristics of a system in order to make inferences on its operation. Generally the term *side-channel attack* is used to describe an attack on a cryptosystem.

Some of the observations that can be used include *timing, power consumption*, and *emanations*, any of which may provide clues to a system's operation that may permit an attacker to compromise it.

State Attacks (TOCTTOU)

A **time of check to time of use** (**tocttou**) bug is a defect in software or hardware that can result in a malfunction or security violation in a system. Also known as a **race condition**, a **tocttou** bug is one where changes in a system occur between the *checking* of a condition and the *use* that results from the check.

Here is an example: two users wish to open a file for exclusive use. The program that each user is running first checks to see if the file is in use; the program for each user reports that the file is not opened by anyone. Because of that, both users' programs open the file, expecting that they each have exclusive use of the file.

Emanations

The term emanations refers to the phenomena where radio frequency (RF) electrical signals—called compromising emanations (CE)—are emitted from computing and network equipment. While this is most often associated with CRT (cathode ray tube) monitors and poorly terminated network wiring, emanations can also be emitted from circuits within computers and other devices themselves.

The U.S. Department of Defense conducted research into the field of emanations in a program that was code-named TEMPEST. The result has been a set of standards for shielding equipment, rooms, and entire buildings from compromising emanations.

Maintenance Hooks and Back Doors

During development, software programmers often place a **maintenance hook** or back door into the program they are working on in order to facilitate easier testing. These hooks and back doors are rarely documented, and sometimes programmers will forget to remove them, which results in a program in production or commercial use having vulnerabilities that can be exploited by the programmer himself or someone else who discovers them.

Occasionally, programmers deliberately place hooks and back doors into programs, and leave them there intentionally, either to ease the support process or for malicious reasons, such as falsifying information or theft.

Privileged Programs

Developers and other persons may accidentally or intentionally place tools or utilities on a system that have privileged levels of operation. The purpose of these tools or utilities permits the tools' user to surreptitiously perform unauthorized functions on the system.

These privileged programs may be an acceptable artifact on a development or testing environment where the developer or tester needs quick, privileged-level access to programs or data in order to facilitate a rapid and efficient development or testing process. But if these programs are installed on the production environment, they may permit unauthorized and inappropriate access, allowing personnel to manipulate the system.

An additional security risk of privileged programs is discovery by an outsider who is seeking ways of gaining unauthorized entry to a system.

Software Security Countermeasures

Countermeasures are actions that can be taken to reduce the potential of a threat by reducing its probability of occurrence or its impact. The countermeasures in this section are those that can be used to reduce the threats discussed in the previous section.

Sniffers and Other Analyzers

Sniffers are devices used to record communications on a network medium, such as Ethernet or Wi-Fi. A sniffer can be used to analyze communications in order to study what communications are taking place. Other types of analyzers include bug detectors, which are devices used to detect covert wireless transmitters).

Source Code Reviews

A **source code review** is an activity where programs analyze a program's source code in order to ensure that recent changes were applied correctly and that the program contains no unwanted code, such as back doors or maintenance hooks. To be effective, source code reviews must be performed by skilled programmers who have not made recent changes to the program being reviewed; if a malicious programmer has placed illicit code in a program, she will deliberately overlook it in order to make sure that it is not detected and removed.

Auditing Tools

Auditing tools includes a wide range of tools that are used to examine a system in order to detected unwanted conditions. Examples of auditing tools are:

- **Filesystem integrity checking.** These tools periodically examine the part of a system's filesystem where the operating system and important programs reside and report any changes that occurred. These changes could be the result of normal maintenance, unauthorized changes, or an intruder. *Tripwire* is a well known filesystem integrity tool.
- **Configuration checking.** These tools periodically examine the configuration of an operating system in order to detect any changes or configurations that would be considered unsafe or unsecure.
- **Log analyzers.** These tools examine system logs and report on any suspicious activity that could be the result of an intrusion or an administrator performing unauthorized activities.

Penetration Testing Tools

Penetration testing is a technique that is used to detect network-based weaknesses in a system that could be exploited by an intruder. A *pen testing* tool works by sending a collection of specially-formed packets over a network to the target system and then examines the results.

A different class of network-based testing tools is used to detect vulnerabilities in web-based applications. These tools operate like intelligent web browsers and send a collection of specially-formed messages to the application to look for signs of weaknesses that could be exploited by intruders and that could result in the compromise of sensitive data. Many noteworthy hacking incidents have occurred because of web application vulnerabilities.

Chapter Summary

- Bell LaPadula and Biba are state machine models that describe access to various levels of information for subjects at various levels of clearance.
- Clark-Wilson is a data integrity model that consists of principals that operate on data items.
- Common Criteria for Information Technology Security Evaluation is a framework for specifying, implementing and evaluating a system against a set of security requirements. Common Criteria supersedes TCSEC and ITSEC, which are older security evaluation methodologies.
- The Capability Maturity Model Integration, or CMMI, is a model used to evaluate the maturity of systems engineering processes. The Systems Security Engineering Capability Maturity Model (SSE-CMM) is a model used to evaluate the maturity of security in an organization.
- Certification is the process of evaluating a system against a set of criteria. Accreditation is the process of formally approving the use of a system. These two terms are often used together and coined *C&A*.
- FISMA is the U.S. federal government mandated framework for certifying and accrediting information systems.
- The *DoD Information Assurance Certification and Accreditation Process*, or DIACAP, is used to certify and accredit military information systems. DIACAP supersedes DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process). The *National Information Assurance Certification and Accreditation Process* (NIACAP) is the process used to certify and accredit systems that handle national security information. DCID 6/3 is the process used to certify and accredit systems used by the U.S. Central Intelligence Agency (CIA).
- A computer's hardware consists of a CPU (central processing unit, which executes the instructions in *programs*), a bus, main storage, secondary storage, firmware, and communications capabilities.
- A CPU contains an arithmetic logic unit (ALU), registers, program counter, and memory interface. The CPU's basic functions are fetch (retrieve an instruction from memory), decode (parse an instruction), execute (perform the instruction), and

writeback (write the results of the instruction to a register or memory location). A CPU chip may have a single core (CPU) or multiple cores (CPUs).

- Most computers with multiple CPUs have a symmetric multiprocessing (SMP) architecture in which all CPUs are connected to main memory. Some older computers employ an asymmetric multiprocessing (ASMP) architecture that employs master and slave CPUs or some other asymmetric scheme.
- A computer's bus is used to connect the computer's main components (CPU, main memory, secondary memory, peripherals) together. Many modern computers have more than one bus.
- A computer's main memory usually consists of electronic random access memory in the form of DRAM (dynamic random access memory) or, less often, SRAM (**static random access memory**). A computer's secondary storage usually consists of one or more hard disk drives, although some compact computers employ flash memory for secondary storage.
- Virtual memory is the means used to accommodate more active processes than can be directly supported by main memory. Swapping (archaic) and paging (contemporary) are used to shuttle process' memory images back and forth between main storage and secondary storage.
- Firmware is software that is permanently (or semi-permanently) stored on memory chips in a computer and usually used to store machine readable instructions for bootstrapping the computer.
- Trusted computing base (TCB) is a DoD *Orange Book* term used to describe the entire set of hardware, firmware, operating system, and programs that support a stated security policy.
- The *security modes of operation* are dedicated, system high, compartmented, and multilevel.
- An operating system (OS) is the software that facilitates the use of application programs and tools and controls access to the computer's hardware resources. The primary functions of an OS are process management, resource management, access management, event management, and communications management. The OS may use the *privilege level* model or the *protection ring* model to enforce security policy.
- A computer system may have one or more software subsystems installed including a database management server (DBMS), web server, authentication server, e-mail server, file server, and directory server.
- A *program* is a set of computer instructions used for some business purpose. A *tool* is a program usually used for some system maintenance purpose. An *application* is a collection of programs and tools that supports a high level business activity, such as financial accounting or manufacturing resource planning.
- Threats to computing architectures include covert channels (unauthorized (and perhaps hidden) communications that occupies a legitimate communications channel); side channel attacks (inference attacks that use observations of timing, power consumption and emanations to discover facts about a system); state attacks (also known as race conditions); emanations (usually-RF radiation from devices such as

CRT monitors and network cabling to eavesdrop on computer activity); and maintenance hooks, back doors, and privileged programs (to gain illicit access to information).

- Countermeasures to these threats include source code reviews (to discover unwanted or illicit program instructions); auditing tools (to detect unauthorized changes or unwanted events); and penetration testing tools (to discover weaknesses in systems and software).

Key Terms

Access Matrix A security model that consists of a two-dimensional matrix of subjects, objects, and the permissions for each subject's access to each object.

Application A collection of programs and tools that fulfill a specific business purpose.

Arithmetic Logic Unit (ALU) The portion of a CPU where arithmetic and logic operations are performed.

Asymmetric multiprocessing (ASMP) A multi-CPU computer architecture consisting of master and slave CPUs or some other asymmetric arrangement.

Bell LaPadula A security model that addresses the confidentiality of information.

Biba A security model that addresses data integrity.

Bus A hardware subsystem used to transfer data among a computer's internal components, including its CPU, storage, network, and peripherals.

Central processing unit (CPU) The portion of a computer where program instructions are executed.

Certification The process of evaluating a system against a specific criteria or specification.

Clark-Wilson A security model that addresses data integrity that is a rebuttal to the Bell LaPadula and Biba models.

Common Criteria The current framework for evaluating the security of a system.

Compartmented security mode One of the security modes of operation where users can access some data based upon their need-to-know and formal access approval.

Complex Instruction Set Computer (CISC) A microprocessor architecture in which each instruction can execute several operations in a single instruction cycle.

Covert channel An unauthorized channel of communications that exists within a legitimate communications channel.

Data confidentiality model A security model whose chief concern is the confidentiality of data.

Data integrity model A security model whose chief concern is data integrity.

Database management system (DBMS) A set of software programs used to manage large organized collections of data called databases.

Dedicated security mode One of the security modes of operation where all users can access all data.

Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) The process used to certify and accredit information systems used by the U.S. military.

Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) The process used to certify and accredit information systems used by the U.S. military; superseded by DIACAP.

Device driver A program that permits the operating system and other programs to communicate with a specific hardware device or type of device.

Director of Central intelligence Directive 6/3 (DCID 6/3) The process for protecting sensitive compartmented information within information systems at the U.S. Central Intelligence Agency (CIA).

Discretionary access control (DAC) An access control model where the owner of an object may grant access rights to subjects based upon the owner's discretion.

Dynamic Random Access Memory (DRAM) A random access memory (RAM) technology used in computer main storage.

Electrically Erasable Programmable Read Only Memory (EEPROM) A form of erasable semiconductor memory used to store firmware.

Erasable Programmable Read Only Memory (EPROM) A form of erasable semiconductor memory used to store firmware.

Evaluation Assurance Level (EAL) The seven levels of evaluation in the Common Criteria.

Explicitly Parallel Instruction Computing (EPIC) A microprocessor design that permits parallel execution in a single CPU.

Federal Information Security Management Act (FISMA) A U.S. law that requires the evaluation of all systems used by the U.S. federal government.

File system A logical collection of files that resides on a storage medium.

FireWire See IEEE1394.

Firmware Computer instructions that are stored on a non-volatile memory device such as a PROM or EPROM.

Flash memory A form of erasable semiconductor memory used to store firmware.

Hook See maintenance hook.

IEEE1394 An external bus architecture used to connect high-speed external devices such as video cameras.

Information flow A security model that describes permitted and forbidden flows of information rather than access controls.

Information Technology Security Evaluation Criteria (ITSEC) The European framework for system security evaluation now superseded by the Common Criteria.

ISO 15408 See Common Criteria.

Kernel The part of an operating system that actively manages processes and access to resources.

Main storage The primary, but usually volatile, high-speed storage used by a computer.

Maintenance hook A feature in a program that permits easy maintenance or access to information that bypasses security controls.

Mandatory access control (MAC) An access control model where subjects are permitted to access objects based upon specific security policies.

Master boot record (MBR) A place on a mass storage device (such as a hard drive) that contains computer instructions that can be read into memory when a computer is powered up or restarted.

Memory See main storage.

Memory interface The portion of a CPU that facilitates access to the computer's main memory.

Microchannel An internal bus architecture used by IBM in PS/2 systems as a replacement for the slower ISA bus.

Multi-Level A security model consisting of several clearance levels for subjects and objects.

Multi-level security mode One of the security modes of operation where users can access data based upon their need-to-know, formal access approval, and security clearance.

National Information Assurance Certification and Accreditation Process (NIACAP) The process used to certify and accredit systems that handle U.S. national security information.

Network interface card (NIC) A computer hardware component that connects the computer's bus to a communication channel or network.

Non-interference An abstract security model that states that subjects with low clearance levels cannot learn anything about information at higher clearance levels on account of activities performed by subjects at higher clearance levels.

Page fault An event where a process attempts to access data in a memory location that has been moved to secondary storage.

Paging The memory management technique of moving inactive memory pages between main storage and secondary storage.

Partition A separate division of storage, usually on a hard disk drive.

PC card An external bus architecture used for the connection of compact peripheral devices to laptop computers.

Peripheral Component Interconnect (PCI) An internal bus architecture used in modern PCs.

Primary storage See main storage.

Privilege level An operating system protection scheme where users are assigned levels of permissions that dictates the resources and data that they are permitted to access.

Program A set of computer instructions that usually resides in a file and is used to perform a specific task.

Program counter A CPU register that tracks the current instruction in a program.

Programmable Read Only Memory (PROM) A form of semiconductor memory used to store firmware.

Protection ring A hierarchical operating system protection scheme used to protect resources based upon levels of privilege.

Race condition See Time of check to time of use (tocttou) bug.

Random Access Memory (RAM) See *main storage*.

Reduced Instruction Set Computer (RISC) A newer microprocessor design where the CPU has a smaller (reduced) instruction set that permits it to be more efficient.

Reference monitor A hardware or software component in a system that mediates access to objects according to their security level or clearance.

Register A storage location within a CPU.

Serial ATA (SATA) An external bus architecture used primarily for communications with disk storage.

SBus An internal bus architecture used in SPARC-based computers including those made by Sun Microsystems.

Small Computer Systems Interface (SCSI) An external bus architecture used to connect a computer to disk storage devices.

Secondary storage The slower, but persistent, form of storage used by a computer.

Security modes of operation The security classifications for systems that determine the types of permissions necessary for users to access data.

Software Engineering Institute Capability Maturity Model Integration (SEI CMMI) A framework for evaluating the maturity of an organization's systems engineering practices.

Side-channel attack An attack on a system where a subject can observe the physical characteristics of a system in order to make inferences on its internal operation.

Sniffer A device or program used to record communications on a network.

Source code review A review of a program's source code in order to ensure that recent changes were applied correctly and that the program contains no unwanted code.

Static random access memory (SRAM) A random access memory (RAM) technology used in computer main memory.

Swapping The memory management technique of moving an entire process's memory contents between main storage and secondary storage.

Symmetric multiprocessing (SMP) A computer architecture where two or more CPUs are connected to the computer's main memory in a symmetrical arrangement.

System high security mode One of the security modes of operation where all users can access some data based upon their need-to-know.

Systems Security Engineering Capability Maturity Model (SSE CMM) A framework for evaluating the maturity of an organization's security implementation practices.

Target of evaluation (TOE) A system being evaluated with the Common Criteria.

Time of check to time of use (tocttou) bug A resource allocation vulnerability where a period of time elapses between the time when a resource's availability is confirmed and the resource is assigned or used.

Tools Separate programs that are included with an Operating System that are used to change system configurations, edit files, create directories, and install other programs.

Trap door See *back door*.

Trusted Computer Security Evaluation Criteria (TCSEC) The U.S. DoD framework for system security evaluation now superseded by the Common Criteria.

Trusted Computing Base (TCB) The hardware, firmware, operating system, and software that effectively supports security policy.

Trusted Network Interpretation (TNI) The evaluation criteria for evaluating the confidentiality and integrity of communications networks.

Trusted Platform Module (TPM) A secure cryptoprocessor used to store cryptographic keys and perform some crypto functions.

Unibus An internal bus architecture used by Digital Equipment Corp. PDP-11 and VAX computers.

Universal Serial Bus (USB) A serial bus communications standard, used for the connection of peripheral devices to a computer including keyboards, mice, storage device, and network adaptors.

Virtual memory A memory management technique whereby the operating system can permit a process's memory to become fragment and even overflow onto secondary storage.

Web server A software component used to accept and process incoming requests for information sent from end users who are using Web browsers.

Review Questions

1. The framework for evaluating a system against a set of security requirements that supersedes TCSEC and ITSEC is:
   a. The Orange Book
   b. The CMMI
   c. The Common Criteria
   d. COBIT
2. An organization has completed the Certification of a new information system. The next step(s) is(are):
   a. Accreditation and business use
   b. Business use
   c. Coding, testing, and implementation
   d. Security testing and implementation
3. A computer's internal bus is used for:
   a. Enforcing process separation
   b. Communication with peripherals
   c. Communication between CPU and peripherals
   d. Communication between CPU, memory, and peripherals

4. The purpose for secondary memory is:
   a. Temporary storage
   b. Paging
   c. Permanent storage
   d. Virtual memory management
5. Most computers with multiple CPUs have what kind of architecture:
   a. Parallel
   b. Symmetric multiprocessing
   c. Asymmetric multiprocessing
   d. Linear
6. Code reviews are effective countermeasures for the following threats EXCEPT:
   a. Back doors
   b. Maintenance hooks
   c. Weak passwords
   d. Buffer overflow
7. All of the following are functions of an operating system EXCEPT:
   a. Database management
   b. Process management
   c. Resource management
   d. Access management
8. A security manager is developing security requirements for new end-user workstations and wishes to have a secure cryptoprocessor in systems to support security. What should the security manager specify be present?
   a. Trusted Computing Base
   b. Reference monitor
   c. Trusted Module Platform
   d. Trusted Platform Module
9. Firmware is most often used for:
   a. Small electronics
   b. BIOS
   c. Storage of operating parameters
   d. Storage of initial computer instructions used at startup time

10. The purpose of a program counter is:
    a. Keep track of which process the CPU is currently working on
    b. Keep track of which instruction in a program the CPU is currently working on
    c. Keep track of the number of active processes
    d. Keep track of the size of the active program
11. Another name for the Trusted Network Interpretation is:
    a. The Red Book
    b. The Orange Book
    c. SEI-CMMI
    d. SSE-CMM
12. A security manager is needs to simplify how user permissions are managed. The security manager should consider using:
    a. Discretionary access control (DAC)
    b. Mandatory access control (MAC)
    c. Role-based access control (RBAC)
    d. Authentication, authorization, and accounting (AAA)
13. The security model with *no read-down* and *no write-up* is:
    a. Multi-level
    b. Clark-Wilson
    c. Bell LaPadula
    d. Biba
14. A system that hides the activities of high-privilege users from low-privilege users employs the model known as:
    a. Non-interference
    b. Compartmented
    c. Access matrix
    d. Biba
15. SATA, SCSI, and USB are examples of:
    a. External bus architectures
    b. Internal bus architectures
    c. Peripheral command protocols
    d. Mass storage adaptors

Hands-On Projects

Project 9-1: Motherboard Specifications Review

In this project you will examine the specifications of selected PC motherboards and make a selection recommendation based upon the specifications and cost.

1. Using search tools, search for available motherboards from Abit, ASUS, AOpen, EPox, Intel, MSI, and XFX. Find specifications for currently available products.
2. Create a chart of the specifications that you feel are the most useful, but include at least eight specifications that you can compare among the different products. Include price in your specifications.
3. From the specifications you have gathered and charted, select the top two motherboards from the entire list. Describe why these two are the most favored and be prepared to justify your decision to others.

Project 9-2: Examine Running Processes

In this project you will examine running processes on your system.

1. Download Process Explorer from technet.microsoft.com.
2. Run Process Explorer on your Windows system.
3. In the main view, click the **Process** column header until you see a hierarchical view of the running processes on your system. What does this view depict?
4. Click **View > Show Lower Pane**, then **View > Lower Pane View > Handles**. Then click on different processes in the upper pane. What does this view depict?
5. In the upper pane, right-click a selected process and click **Properties**. View the available data on the different tabs. What do they show?
6. (For advanced users) Click Find. In the search field, type procexp.exe. Click different entries in the result and notice what is happening in the main Process Explorer window. What is Process Explorer showing you?

Project 9-3: Simple Port Scanning

In this project you will perform simple port scanning to discover open ports on nearby network systems.

Note: Port scanning may be considered a security violation in the work or school network. You must obtain permission from the network manager before downloading and using such a tool.

1. Download the Cyberkit tool from www.networkingfiles.com/cyberkit.
2. Install the tool on your computer.
3. Start the tool and switch to the Ping window by clicking **Window > Transform to > Ping**.

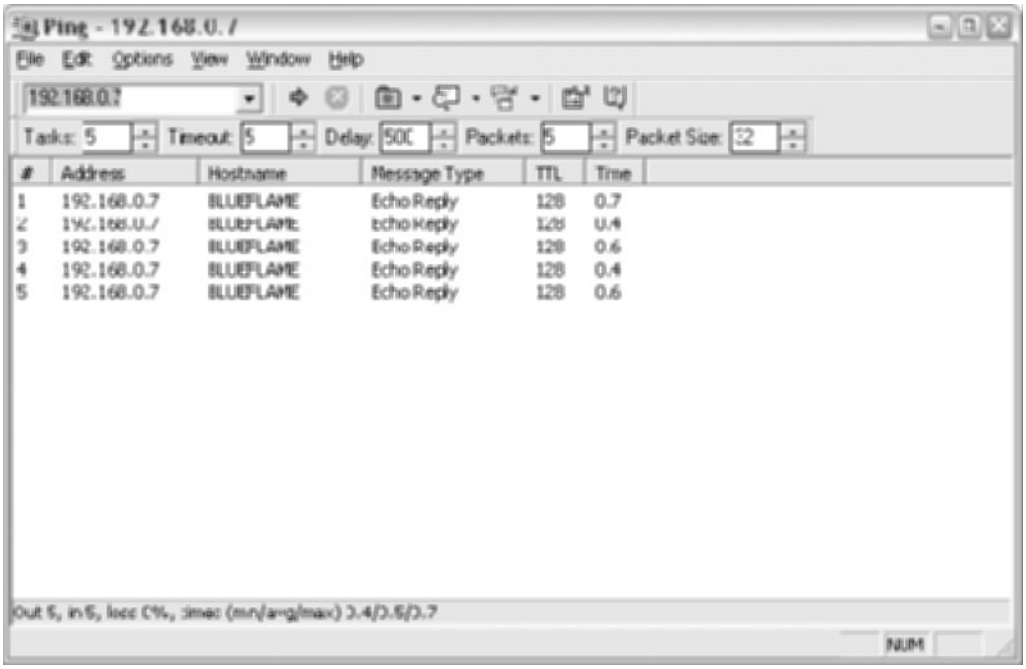


Figure 9-5 The Cyberkit tool used to ping a node on the network

Source: Course Technology/Cengage Learning

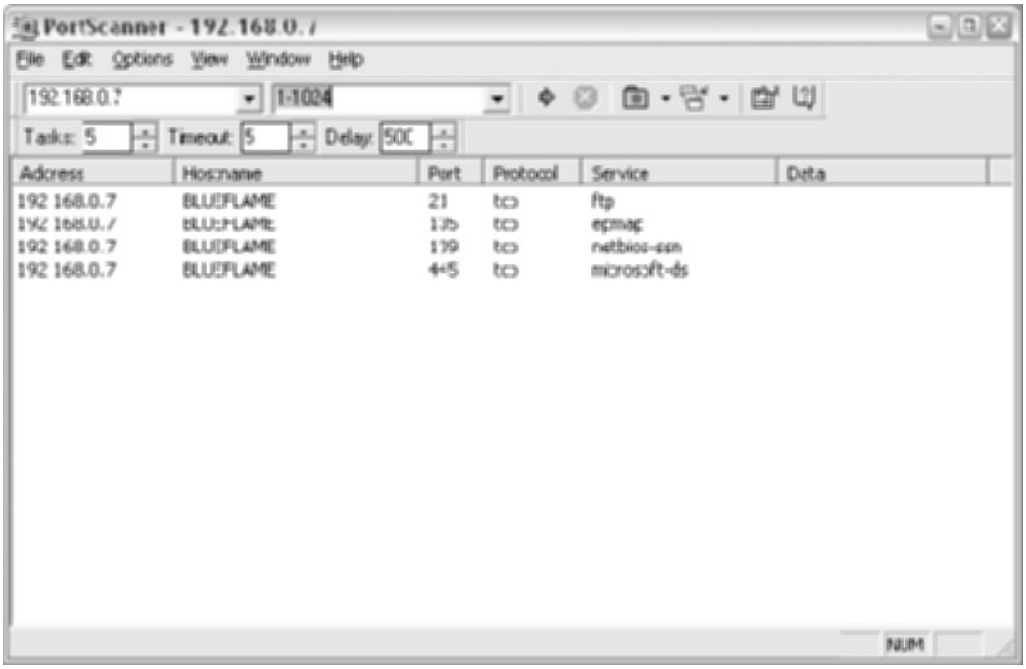


Figure 9-6 The Cyberkit tool used to scan for open ports

Source: Course Technology/Cengage Learning

4. Select an IP address for a known system on the network and use Cyberkit to send pings to the device. The target system should respond, as shown in Figure 9-5.
5. Switch Cyberkit to the PortScanner window by clicking **Window > Transform to > PortScanner**.
6. In the **Host** field, type the target IP address. In the **Port** field, type "1-1024." Click **Go** (the yellow arrow to the right of the Port field). Cyberkit will scan ports 1-1024 on TCP and UCP, as shown in Figure 9-6.

What open ports are shown? What is the function of these ports? Are there any security implications on account of these ports being open?

Case Projects

Case Project 9-1: Develop a Role-based Access Control Matrix

As a consultant with Best Security Consulting Co., you have been asked to develop a role-based access control matrix for the IT department in an insurance company, Overland Underwriting.

Overland Underwriting has provided a list of job titles and roles associated with access management. You are to develop an access matrix that specifies which job titles are permitted to perform which roles.

The job titles are: System Engineer I, System Engineer II, Network Administrator I, System Engineering Manager, Security Administrator I, Security Administrator II, Security Manager, and IT Manager.

The roles are: Review end user account request, Approve end user account request, Create end user account, Audit end user accounts, Review end user file server access request, Approve end user file server access request, Perform end user file server access change, Audit end user file system permissions.

When you map job titles to roles, make sure that there is adequate "separation of duties." For instance, someone who approves requests should not be the same person who fulfills requests—and someone else altogether needs to audit requests.

Case Project 9-2: Security Tools

As a consultant with the Waterfall Consulting Co., you have been assigned to a consulting project at the Hughes Paint Company, a small manufacturing company.

Hughes Paint is considering enacting a policy that will forbid all but security analysts to possess and use security tools such as scanning tools, password crackers, disassemblers, sniffers, and code analyzers.

Is this policy a good idea? How can it be enforced? Create a report that includes your recommendations.

Case Project 9-3: Software Development Process Improvements

As a consultant with the Alpha Security Advisors Co., you have been asked to develop a plan for improving systems engineering processes for your client, a large software company, Grid Software.

Grid Software had a recent security incident where a developer had planted a back door in an online web application and later exploited the back door after being terminated from the company.

The company is concerned that other back doors may exist in other applications that are waiting to be discovered and exploited. What steps do you recommend Grid Software take? Create a written report that includes your recommendations.

chapter 10

Telecommunications and Network Security

Topics in this Chapter:

- Wireline and Wireless Telecommunication Technologies
- Wired and Wireless Network Technologies
- Network Topologies and Cabling
- The OSI and TCP/IP Network Models
- TCP/IP Networks, Protocols, Addressing, Devices, Routing, Authentication, Access Control, Tunneling, and Services
- Network-Based Threats, Attacks, Vulnerabilities, and Countermeasures

The (ISC)^2 *Common Body of Knowledge* (CBK) defines the key areas of knowledge for Telecommunications and Network Security in this way:

Telecommunications and Network Security domain encompasses the structures, transmission methods, transport formats, and security measures used to provide integrity, availability, authentication, and confidentiality for transmissions over private and public communications networks and media.

The candidate is expected to demonstrate an understanding of communications and network security as it relates to voice communications; data communications in terms of local, wide area, and remote access; Internet/Intranet/Extranet in terms of Firewalls, Routers, and TCP/IP; and communications security management and techniques in terms of preventive, detective, and corrective measures.

In today's global marketplace, the ability to communicate with others is a mandatory requirement. The data communications domain encompasses the network structure, availability, authentication and confidentiality of the transmitted information over both private and public communication networks.

The candidate is expected to demonstrate an understanding of communications and network security as it relates to data communications in local area and wide area networks; remote access; intenet/intranet/extranet configurations, use of firewalls, network equipment and protocols (such as TCP/IP), VPNs, and techniques for preventing and detecting network-based attacks.

Key areas of knowledge:

- *Establish secure data communications*
- *Establish secure multimedia communications*
- *Develop and maintain secure networks*
- *Prevent attacks and control potential attack threats (e.g., Malicious Code, Flooding, Spamming)*
- *Remote access protocols (e.g., CHAP, EAP)*

Because many threats are propagated over networks or attack networks, a thorough knowledge on the inner workings of networks is essential knowledge for any security professional.

Telecommunications Technologies

Telecommunications providers, also known as *common carriers* or *telcos*, have developed and constructed numerous regional and world-wide networks that are used to carry voice and data communications between individuals and businesses. There are many wired and wireless technologies in use that are described in this section.

Wired Telecom Technologies

Also known as **wireline**, these technologies are all based upon copper or fiber optic cabling that can span a few miles in local communities or thousands of miles in above-ground or ocean floor cabling.

DS-1 **Digital signal 1**, known as **DS-1** or **T-1**, is a multiplexed telecommunications protocol family developed by Bell Labs and is used in North America, Korea, and Japan.

The line rate of a DS-1 circuit is 1.544 Mbit/sec. When used to carry voice traffic, a DS-1 carries 24 voice channels (each called a **DS-0**) at 64 kbit/s each. When used to carry data traffic, a DS-1 can be divided into 24 data channels at 64 kbit/s each, into a smaller number of faster channels, or a single data channel at 1.544 Mbit/sec.

Other rates of this type of technology are available, as shown in Table 10-1.

European T-carrier protocols are similar to those used in North America, and shown in Table 10-2. The European protocols are used in most of the remainder of the world.

When higher data rates are required, SONET technology is often employed. SONET is discussed later in this section.

SONET **Synchronous optical networking** (**SONET**) is the prevalent standard in North America for transporting voice and data over optical fiber. SONET is a physical-layer technology that can be used to encapsulate network technologies such as ATM, and TCP/IP. SONET is also used to encapsulate slower DS-1 type technologies.

Name	Rate	Voice Channels
DS0	64 kbit/s	1
DS-1, aka T-1	1.544 Mbit/s	24
DS-2	6.312 Mbit/s	96
DS-3, aka T-3	44.736 Mbit/s	673
DS-4	274.176 Mbit/s	4,032
DS-5	400.352 Mbit/s	5,760

Table 10-1 North American T-carrier protocols

Name	Rate	Voice Channels
E0	64 kbit/s	1
E1	2.048 Mbit/s	32
E2	8.558 Mbit/s	128
E3	34.368 Mbit/s	512
E4	139.264 Mbit/s	2,048
E5	565.148 Mbit/s	8,192

Table 10-2 European T-carrier protocols

Name	Rate
OC-1	48.960 Mbit/sec
OC-3	150.336 Mbit/sec
OC-12	601.344 Mbit/sec
OC-24	1,202.688 Mbit/sec
OC-48	2,405.376 Mbit/sec
OC-96	4,810.752 Mbit/sec
OC-192	9,621.504 Mbit/sec

Table 10-3 SONET data rates

The data rates available for SONET are shown in Table 10-3.

Higher SONET rates are in development including OC-768, OC-1536, and OC-3072, whose rates are 38 Gbit/s, 77 Gbit/s, and 154 Gbit/s, respectively.

Frame Relay **Frame Relay** is an early packet-switched telecommunications network technology that permitted business customers to transmit data between locations at a lower cost than dedicated DS-1 circuits. Frame relay permitted the creation of Switched Virtual Circuits (SVCs) and Permanent Virtual Circuits (PVCs) that emulated the permanence of a dedicated DS-1 by providing the appearance of a dedicated circuit that actually employed the transmission of packets in a shared medium.

Frame Relay is a data link-layer protocol that is built on DS-1 (and faster) network technology with special equipment that facilitated the creation of SVCs and PVCs.

Frame Relay is considered a successor to the older and slower X.25 technology, but is now giving way to newer technologies such as DSL, MPLS, and VPN.

ATM **Asynchronous Transfer Mode** (**ATM**) is a packet-switching network protocol that uses a fixed-size packet called a *cell* to transport data. ATM is a data link-layer protocol that is transported on various physical-layer media, usually twisted-pair copper, fiber optics, or SONET. ATM's cell size is 53 bytes—48 bytes of data and 5 bytes of header.

ATM is connection-oriented; before data is transmitted between nodes, a virtual circuit is established.

ATM was intended to replace Ethernet and TCP/IP in local area networks that required higher performance, but this was not realized, as organizations were more apt to adopt faster Ethernet technologies that were more familiar to them. However, ATM is used in wide area networks by larger organizations and service providers, but even there it is giving way to MPLS.

DSL **Digital Subscriber Line** (**DSL**), also known as **xDSL**, is a group of technologies used to deliver digital data services over telephone wires. DSL is primarily used by residents and

small businesses that require higher speed data services but cannot afford dedicated DS-1 or Frame Relay service.

DSL uses the same pair of wires that are used for a telephone customer's voice service. Data is carried over the wires on a high frequency band, while analog telephones continue to use the lower voice frequency band. Small filters are used to block the high frequencies from the data signal from interfering with telephones that are connected to the same wires.

DSL service employs a modem-like device on the subscriber end and a **Digital Subscriber Line Access Multiplexer** (**DSLAM**) on the service provider's network.

Typical DSL topology is shown in Figure 10-1.

MPLS **Multiprotocol Label Switching** (**MPLS**) is a packet switched technology that is used for both voice and data and can be used to carry IP, ATM, SONET, and Ethernet frames over **Wide Area Networks** (**WANs**). MPLS is ideal for carrying both voice and data because of its QoS (Quality of Service) capabilities that permit the network to transport voice and other streaming media at acceptable rates even during times of heavy data usage.

Telecommunications service providers have MPLS networks that subscriber companies connect their networks to, usually for wide-area transport of voice and IP traffic.

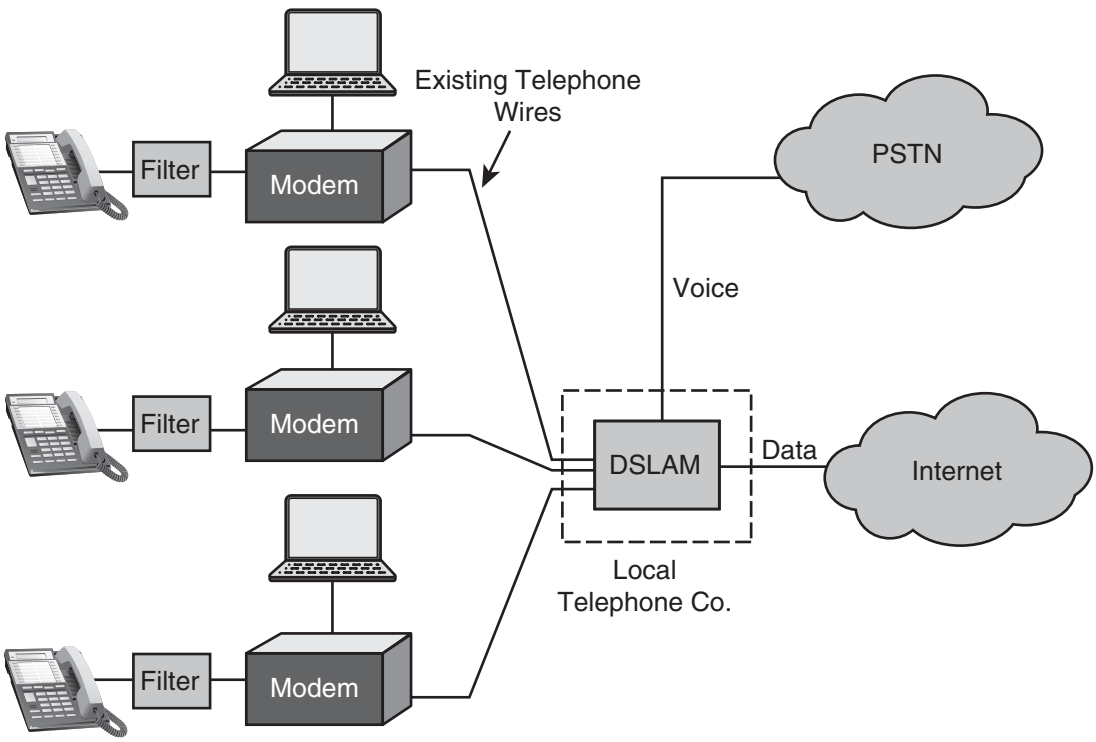


Figure 10-1 DSL architecture

Source: Course Technology/Cengage Learning

MPLS is replacing Frame Relay and ATM, and is expected to overshadow them by 2010.

Other Wireline Technologies Other telecommunications technologies that are provided over wired networks include:

- **Data Over Cable Service Interface Specification (DOCSIS).** This is the technology that facilitates Internet access over *hybrid fibre coaxial* (HFC) television networks through popular *cable modems*. Because a part of the HFC network is a shared medium, data between the service provider and the subscriber are encrypted. Service providers also employ MAC-layer security to prevent unauthorized parties from accessing the network.
- **Public Switched Telephone Network (PSTN) .** This is the voice telephone network that has been in place for over a century. This is also known as *POTS* (plain old telephone service). PSTN is *circuit-switched*, which means that a telephone call uses a physical circuit for the duration of the call (this is not *exactly* true any more—the core of a telco network converts PSTN calls from circuit-switched at the edge of the network to packet-switched at the core).
- **Integrated Services Digital Network (ISDN).** This is a newer digital service designed for voice, data, or both. Introduced in the late 1980s, ISDN was used to extend digital-based corporate phone networks to subscribers' residences and also for Internet connectivity. The maximum throughput is 128kbit/s, which was soon overcome by DSL and DOCSIS and has contributed to the decline of ISDN.
- **Synchronous Digital Hierarchy (SDH).** Is the prevalent standard for voice and data communications over fiber networks outside of North America. It is the functional equivalent of SONET, which is used in North America.
- **X.25** is a packet-switched network that is transported over lease lines, ISDN, and regular phone lines. X.25 is now in rapid decline and is being replaced by other technologies such as MPLS, DSL, ISDN, and frame relay.

Wireless Telecom Technologies

Several wireless data-centric technologies are provided by wireless telecommunications providers for business and personal use. Many technologies in use are discussed in this section.

CDMA2000 **CDMA2000 (code division multiple access)** is a mobile radio technology used to transmit voice and data between subscriber devices (usually cellular phone handsets and PCMCIA modems) and network providers' base stations, for purposes of voice and data communications. Some of the data transport standards used by CDMA2000 are:

- 1xRTT, capable of 153 kbit/sec
- EVDO, capable of 2.4 Mbit/sec
- EVDV, capable of 3.1 Mbit/sec

GPRS **General Packet Radio Service (GPRS)** is a data-centric mobile radio technology used in **Global System for Mobile Communications (GSM)** network. GPRS devices include mobile handsets and PCMCIA-based modems for PCs. The maximum throughput for GPRS is 114kbit/sec. The successor to GPRS is EDGE, discussed next.

EDGE **Enhanced Data rates for GSM Evolution (EDGE)** and **Enhanced GPRS (EGPRS)** are the successors to GPRS and provide bandwidths up to 1 Mbit/sec.

UMTS **Universal Mobile Telecommunications System (UMTS)** is another data centric mobile radio technology found in wireless handsets and PC card modems. UMTS is usually transported over W-CDMA networks and supports up to 14 Mbits/sec throughput.

WiMAX **Worldwide Interoperability for Microwave Access (WiMAX)** is a data centric radio technology for point-to-point and mobile access. Based on IEEE 802.16, WiMAX is a wireless competitor to DSL and cable modems but also competes with the strictly-mobile data standards such as CDMA2000, GPRS, EDGE, and UMTS.

Throughput for WiMAX subscribers depends upon distance from the nearest base station. Rates can range from 2 to 12 Mbits/sec, but could theoretically go as high as 70 Mbits/sec. Like other wireless technologies, WiMAX is a shared medium, meaning that more simultaneous users means lower effective throughput.

Other Wireless Telecom Technologies Some other wireless data technologies include:

- **CDPD (Cellular Digital Packet Data)**. An early mobile data service that utilized bandwidth on the *AMPS* (Advanced Mobile Phone System—the original analog cellular technology used in North America).
- **Packet radio**. A method of transmitting data over amateur radio bands. The *AX.25* standard defines the protocols used to transport data over amateur radio.

Network Technologies

Many network technologies for use within businesses and educational institutions have been developed in the past five decades, and some of these are still in use today. These technologies are used to facilitate communications between computers in building and campus environments.

There are many wired and wireless technologies in use that are discussed in this section.

Wired Network Technologies

This section describes several wired network technologies that are used in organizations to connect networks to each other.

Ethernet **Ethernet** is a family of frame-based technologies that is used to connect computers in a **Local Area Network (LAN)** (a computer network covering a small geographic area such as a residence, building, or group of buildings.). Ethernet is a data link-layer standard that defines frames and error correcting measures.

Ethernet Cable Types Ethernet runs over many types of cabling including:

- **10BASE-T**. This is the commonly twisted-pair network cable that supports the Category 3, 5, 5e, 6, or 7 ANSI standard. This cable has 8 conductors, of which 4 are

used. An 8-pin RJ45 connector is used to connect a cable to a device, as shown in Figure 10-2.

- **100BASE-TX**. The same twisted-pair network cable (Category 5 and 6) and connectors as 10BASE-T, and also uses just 4 of the 8 conductors. This is designed for 100Mbit/sec network signals.
- **1000BASE-T**. The same twisted-pair network cable and connectors as 100BASE-TX, except that all 8 conductors are used. This is designed to carry 1000Mbit/sec network signals.
- **10BASE2**. The old *thinnet* coaxial cabling with twist-lock BNC connectors—rarely used.
- **10BASE5**. The old *thicknet* coaxial cabling that is rarely used. One interesting feature of 10BASE5 is the ability to install a vampire tap that allows the addition of a node to the network while existing nodes continue communicating.

Ethernet Frame Layout Ethernet is a frame-based network protocol, meaning data is transported in blocks of characters instead of one at a time. An Ethernet frame consists of a header, payload, and checksum as follows:

- **Header**. The Ethernet header consists of 14 bytes that includes:

  Preamble. This consists of 7 octets of 10101010.

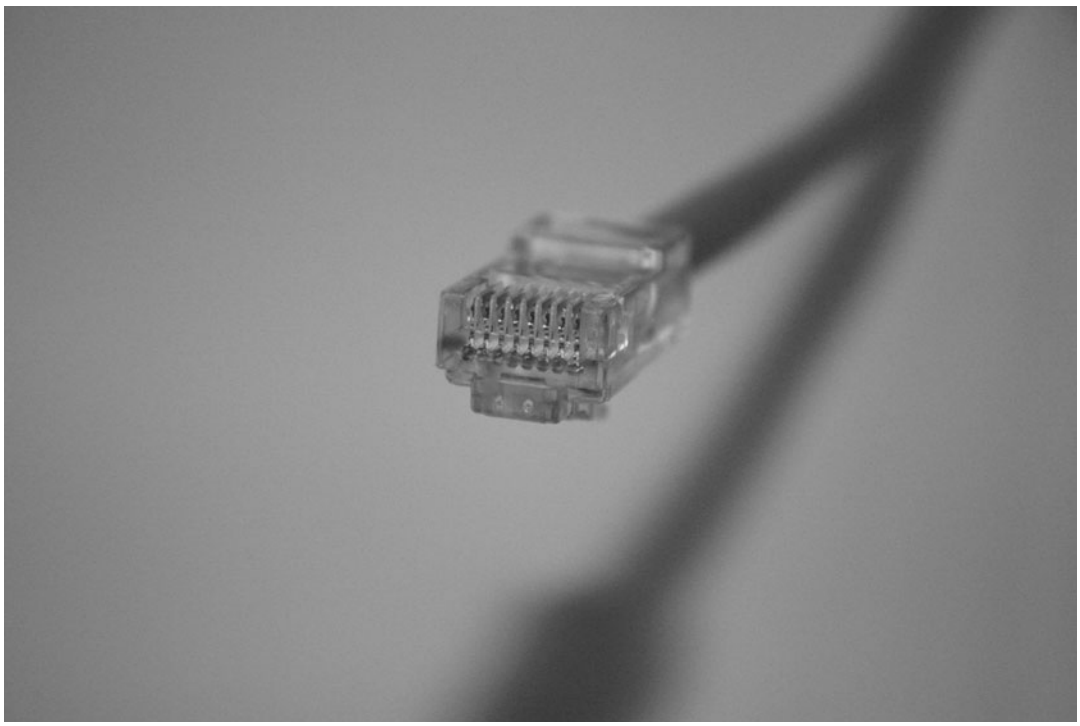


Figure 10-2 100BASE-TX cabling with RJ45 connector

Photo by Rebecca Steele

Start of frame. This consists of 1 octet of 10101011.

6 byte destination MAC address.

6 byte source MAC address.

2 byte Ethernet frame type.

- **Payload**. This is the *data* in the Ethernet frame that is of variable length, from 46 to 1500 bytes.
- **Checksum**. This is a 4 byte CRC (Cyclic redundancy check) that is used to verify the integrity of the entire frame. The CRC is calculated by the sending node and placed in the header; the destination node calculates the CRC and compares it to the value in the header; if they match, the packet arrived correctly; if they do not match, the packet is dropped.
- **Interframe gap**. After the frame is transmitted, the sending station pauses for 960 ns before sending the next frame.

Ethernet Error Detection Ethernet is a **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)** network protocol. This means that any station that wants to transmit frames on the network first listens to see if any other station is transmitting. This is the *carrier sense* part of CSMA.

If a station that is transmitting detects that another station is also transmitting, a *collision* has occurred. The station stops transmitting, sends a *jam signal*, (a pattern of 16 "1-0" bit combinations that essentially means, "Everybody stop transmitting!"), and then waits for a random length of time before transmitting again. The wait interval is known as a *backoff delay*; the length of the delay is calculated using the *truncated binary exponential backoff algorithm*, which is designed to help prevent Ethernet networks from crashing due to excessive traffic. This is the *collision detection* part of CSMA/CD.

In Full Duplex Ethernet (where transmits and receives occur on different wires), collision detection is not implemented because collisions cannot occur, since every node is connected to a switch. In this case, Ethernet is really not a shared medium but a point-to-point medium.

Ethernet MAC Addressing On an Ethernet network, stations are uniquely identified by their **Media Access Control (MAC) address**. A MAC address is 6 bytes in length and is permanently assigned to a device, such that no two devices in the world have the same MAC address. The first three bytes of a MAC address are known as the **Organizationally Unique Identifier (OUI)**, which identifies the organization that manufactured the device. The last three bytes are assigned by the device's manufacturer and must be unique.

A MAC address is usually shown in hexadecimal format with colons or dashes separating the bytes. A typical MAC address is 00-14-4F-C1-05-4D. The first three bytes (00-14-4F) identify the device as being manufactured by Sun Microsystems.

Some manufacturers of computer equipment permit an administrator to change a device's MAC address; this is not the norm, however.

Ethernet Devices Several types of devices are used to connect computers to one another on a network. These devices are:

- **Hub**. An early type of network device, a hub is a device used to connect multiple computers together to form a network. A hub can be considered a *multiport repeater*, which is to say that every packet that is present on the network is transmitted to all computers on the network. Once the only way to create computer networks, hubs are still sometimes used in very small business or home networks.
- **Repeater**. A repeater is a device that is used to receive and re-transmit the signal of a network connection, usually in a situation where a very long cable run is necessary to reach one or more distant computers in a network. Repeaters are seldom used, as there are other more effective means for getting signals to distant computers, for instance, fiber optic cables that transmit signals over greater distances.
- **Switch**. A switch is a network device used to connect multiple computers to form a network. While the physical appearance is the same, a switch differs from a hub by sending packets only to only a destination computer on a network, instead of to every computer as a hub does. A switch is able to do this by listening to network traffic and learning which system(s) are present on each connection. After learning which MAC (or IP) address(es) are present on each port, a switch can send packets to only the ports where destination computers are present. This technique improves the potential throughput of the entire network.
- **Router**. A router is a device that connects multiple networks together. In a larger organization with many networks, routers are used to connect the networks together so that systems on one network can communicate with systems on other networks. In any sized organization, a router is used to connect one or more internal networks with one or more external networks such as the **Internet** (the global network of interconnected networks). Each interface on a router is connected to a different network, usually to a hub or switch that is connected to other computers.
- **Gateway**. A gateway is a device or system that translates various types of network communications together. Strictly speaking, a router is a type of gateway, but other types exist, including frame relay switches, ATM to IP switches, and so on.

Token Ring

Token ring is a LAN technology developed by IBM. While initially successful, Token ring gave way to Ethernet and its inexpensive cabling and easily used *RJ-* style connectors. Token ring cables had large, fragile connectors that resulted in a relatively low density of connectors in a device; an enterprise with many Token ring devices would have to consume considerable rack space for token ring hubs, which were called *Multistation Access Units*, or MAUs.

A token ring network is a physical star. Each station on the network is connected to a *Multistation Access Unit*, or *MAU*, by a cable. The first token ring networks operated at a rate of 4 Mbits/sec; later token ring networks operated at 16 Mbits/sec.

A token ring network is a logical ring. Data transmission is facilitated by the use of a logical token, only the station in possession of the network's token may transmit data. The token is passed from station to station; when a station has nothing to transmit, it merely passes the token to the next station. When a station does have data to transmit, it is attached to the token and passed along. When the token (with its payload) reaches the

destination station, the payload is removed, and the destination station then passes an empty token along.

USB Universal Serial Bus (USB) is a serial bus communications standard, used for the connection of peripheral devices to a computer. USB is the successor to RS-232 serial, IEEE 1284 parallel, as well as PC keyboard and mouse connection standards.

- USB 1.0/1.1—the first version (1996) with two speeds: 1.5Mbits/s and 12Mbits/s.
- USB 2.0—the current version (2000) with a higher speed of 480Mbits/s, which makes USB highly suited for external hard drives.
- USB 3.0—the new version (2008) with a higher speed of 4.8Gbits/s.

USB permits hot-plugging of devices, which permits peripherals to be connected and disconnected while the computer and its operating system are running.

The types of devices that can be connected to a computer via USB include keyboards, mice, printers, scanners, mass storage devices (disk drives and memory devices), and network adaptors to connect to Wi-Fi, Bluetooth, and Ethernet networks.

The USB standard includes the use of a 4-port hub (1 port that connects to the host computer and 4 open ports) that facilitates the connection of additional peripherals.

RS-232 RS-232, also known as *serial*, is an older serial communications technology that was widely used with computers from the 1960s through the 2000s, but is now being displaced by USB. RS-232 has been (and is still) used for many applications including:

- Connecting terminals to central computers
- Connecting printers to computers
- Connecting modems to computers
- Connecting mice to computers
- Connecting miscellaneous peripherals to computers

The RS-232 standard accommodated many throughput speeds ranging from 110bps to 56kbps. Flow control has been implemented in several ways including hardware signaling (through various additional connector pins) and software signaling (through the use of *XON* and *XOFF* (ASCII Ox11 and 0x13, respectively).

The computer end of an RS-232 connection is often called DCE (Data Circuit-terminating Equipment); the peripheral end is often called DTE (Data Terminal Equipment).

Other Wired Network Technologies

- **RS-449**. A serial communications standard that is similar to RS-232 and with a maximum bandwidth of 2Mbit/s.
- **High Speed Serial Interface (HSSI)**. A high speed serial protocol often used to connect WAN devices such as routers together. HSSI's bandwidth is 52Mbits/s, and its maximum cable length is 50'.
- **Fiber Distributed Data Interface (FDDI)**. A token network technology transmitted over fiber optic cable, to a maximum distance of 200km (124 miles). Largely displaced by Gigabit Ethernet and SONET.

- **Fibre Channel**. A gigabit network protocol usually used in storage area networks (SANs). There are three modes of fibre channel:
  - FC-P2P. Point to point.
  - FC-AL. Fibre Channel Arbitrated Loop, similar to Token Ring.
  - FC-SW. Switched Fabric, similar to an Ethernet switched network.

Network Cable Types While some of the types of network cabling are explicitly or implicitly mentioned earlier in this section, all of the common types are listed here.

- **Coaxial cable**. This type of cable consists of a single or dual inner conductor, a dielectric insulator, a metallic shield, and an outer plastic jacket. Once common in computer networks, it is now rarely found in commercial applications. Coaxial cable is still commonly used to transmit television broadcasting together with voice and data into a residence or business.
- **Twisted pair cable**. This includes several types of copper conductor cable that utilizes the twisting of conductors in order to resist interference and improve throughput. Figure 10-3 shows twisted pair cable with part of the outer jacket removed to reveal the four twisted pairs of conductors. Classes of twisted pair cabling include:

  Category 3. Consists of four twisted pairs in a single jacket. Suitable only for 10Mbit/s Ethernet. Superseded by Category 5 and 5e.

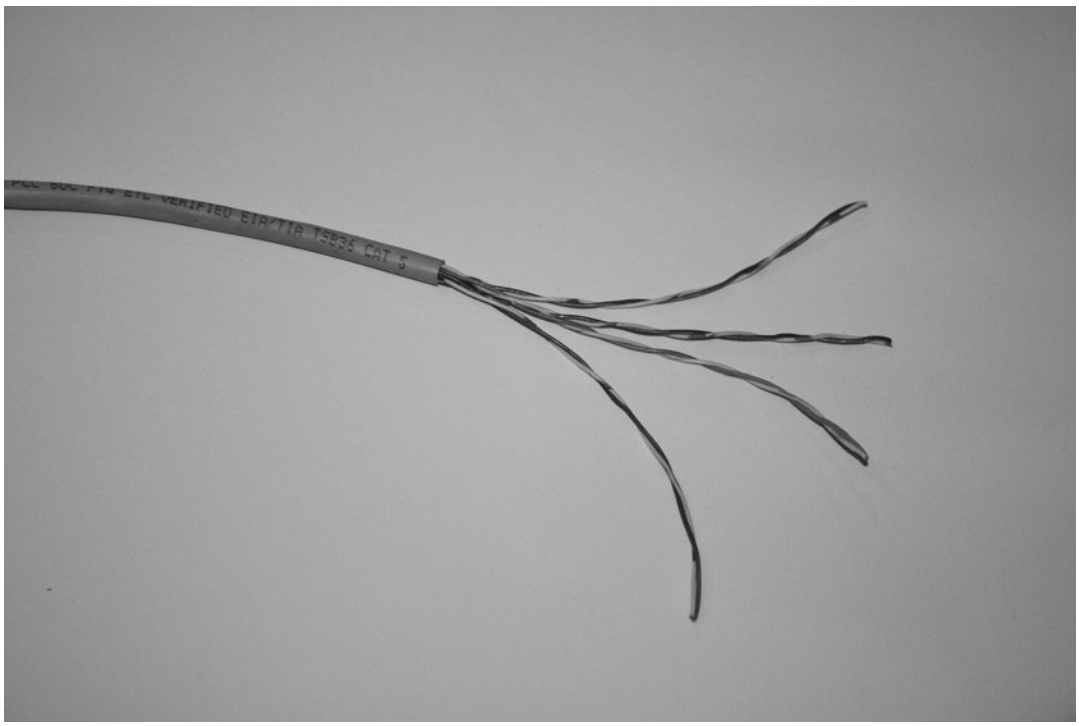


Figure 10-3 Twisted pair cabling

Photo by Rebecca Steele

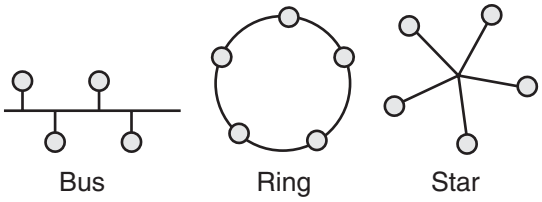


Figure 10-4 Network topologies

Source: Course Technology/Cengage Learning

Category 5. Consists of four twisted pairs in a single jacket. Maximum length is 100m. Suitable for 100Mbit/s and can be used for Gigabit Ethernet.

Category 5e. Supersedes Category 5 and includes specifications for far end crosstalk. Maximum length is 100m.

Category 6. Backward compatible with Category 5 and 5e, but higher specifications for noise and crosstalk, making it more suitable for Gigabit Ethernet. Maximum cable length is 100m.

Category 7. Even more stringent than Category 6 cabling, Cat-7 is suitable for 10Gbit/s networks. Maximum length is 100m.

- **Optical fiber**. This is a cable type used to carry signals in the form of light instead of electricity as is used in copper cabling. While more expensive, optical fiber can carry signals over greater distances and with far greater bandwidth than copper cable.

Network Topologies The topology of a network refers to its physical as well as logical arrangement. The three principle physical network topologies are:

- **Bus**. In a bus network, all of the nodes in the network are connected to a single conductor. A break in the network conductor will cause some or the entire network to stop functioning. Early Ethernet networks consisting of thinnet coaxial cabling were bus networks.
- **Ring**. All of the nodes are connected to exactly two other nodes, forming a circular loop. Breaking any conductor will cause the network to stop functioning.
- **Star**. All nodes are connected to a central device. A break in a conductor will disconnect only one node, and the remaining nodes will continue functioning. Ethernet networks are physical stars, with computers connected to central hubs or switches. Token ring networks, while operating logically as a ring, are physically wired as a star.

Bus, ring, and star topologies are depicted in Figure 10-4.

Wireless Network Technologies

This section describes commonly used wireless network technologies that provide connectivity between computers and devices.

Wi-Fi Known by several names including ***Wireless LAN, WLAN***, and **IEEE 802.1a/b/g/n, Wi-Fi** is the common name for a radio frequency-based data link-layer (OSI layer 2) network protocol used in computer networks. With bandwidths of up to 54Mbit/s over a

distance of 100m, Wi-Fi is a practical alternative to wired Ethernet networks in businesses and residences. Wi-Fi is also the basis for hundreds of thousands of public *hot spots* equipped with free or fee-based Internet connectivity in airports, hotels, resorts, coffee shops, as well as municipal public access networks.

Wi-Fi is not considered a low-power consumption protocol, so it is not suited for mobile devices such as cell phones or headsets; instead it is most often found in laptop computers and digital cameras.

A Wi-Fi network originates from an **access point**, a device that performs radio frequency communications and allows wireless devices to connect to it if they have the correct configuration and security credentials.

Wi-Fi Standards Several technical standards for Wi-Fi radio technology have been developed since its inception in 1997. These standards are shown in Table 10-4.

Wi-Fi Security Several capabilities improve the security of a Wi-Fi network, in order to make it resistant to eavesdropping, including:

- **No broadcast**. A Wi-Fi access point (AP) can be configured so that it does not broadcast the network's SSID (service set identifier), making it more difficult for a node to discover available Wi-Fi networks.
- **SSID**. A Wi-Fi network's SSID can be changed to a value that is not easily guessed.
- **MAC Access Control**. A Wi-Fi network access point can be configured so that only pre-authorized nodes, based upon their MAC addresses, may connect.
- **Authentication**. Workstations that wish to join a Wi-Fi network can be required to furnish a userid and password. Userid-password pairs can be stored in an access point, or the access point can refer to an authentication service such as RADIUS.
- **Encryption**. Wi-Fi over-the-air communications can be encrypted by one of several means:
  - **Wired Equivalent Privacy (WEP)** an encryption algorithm that has been compromised and can be broken within minutes.
  - **Wi-Fi Protected Access (WPA)** a protocol standard that is a replacement for WEP. WPA is a subset of the IEEE 802.11i-2004 (WPA2) specification.

Standard	Spectrum	Data Rate	Range	Released
802.11a	5 GHz	54 Mbit/sec	120 m	1999
802.11b	2.4 GHz	11 Mbit/sec	140 m	1999
802.11g	2.4 GHz	54 Mbit/sec	140 m	2003
802.11n	2.4/5 GHz	248 Mbit/sec	250 m	2009
802.11y	3.7 GHz	54 Mbit/sec	5000 m	2008

Table 10-4 Wi-Fi standards

– **WPA2** is the full IEEE 802.11i-2004 specification, a superset of WPA. Both WPA and WPA2 can operate in a PSK (pre-shared key) mode, where the encryption key is stored in the Wi-Fi access point; otherwise, WPA access points will use an external authentication source, such as RADIUS.

Bluetooth

Bluetooth is a wireless **personal area network** (**PAN**) technology for relatively low speed data communication over short distances.

Typical Bluetooth applications include wireless mobile phone headsets, computer mice and keyboards, wireless stereo headphones, and GPS receivers. Because Bluetooth uses radio spectrum, devices do not require line-of-sight to connect.

Bluetooth data rates range from 1Mbit/s—3Mbit/s. Bluetooth's power consumption is very low, which makes it suitable for low power devices. The maximum range for communications is 10 meters.

Bluetooth devices can authenticate through a process called *pairing*, during which two devices can exchange a cryptographic secret key that the two devices can later use to securely identify themselves. Communications between paired devices can also be encrypted.

IrDA

Infrared Data Association (**IrDA**) is the governing body that has developed a number of line-of-sight optical protocols known as IrDA. IrDA operates in the infrared light spectrum from 2.4kbit/s to 16Mbit/s. Once popular with laptop computers, PDAs, printers, and other devices, IrDA has been largely replaced by Wi-Fi and Bluetooth, both of which require no line-of-sight for connectivity.

Wireless USB

Wireless USB (**WUSB**) is a wireless protocol designed for wireless connectivity of various computer peripherals such as printers, digital cameras, hard disks, and other high-throughput devices. WUSB's bandwidth ranges from 110 Mbit/s at 10 meters to 480 Mbit/s at 3 meters, and occupies the wireless spectrum from the 3.1 to 10.6 GHz frequency range.

Near Field Communication

Near Field Communication (**NFC**) is an extremely short-range (10cm, or ~4") network technology generally used by mobile phones for mobile payment and other applications. NFC's data rates are 106, 212, or 424 kbit/s.

NFC can operate in passive mode and active mode. In passive mode, one device is acting as a transponder, not unlike an RF-powered key card. In active mode, both devices are actively communicating to one another.

NFC's short range makes it ideal for use as a mobile wallet application where a mobile device such as a wallet card or cell phone can be used as a payment token for a merchant transaction or ticketing application.

Network Protocols

Network protocols are the standards by which network messages are constructed. The protocols themselves are complicated enough that layered models have been developed to describe them. The two most common models are the OSI network model and the TCP/IP network model. These two models are described in detail in this section.

The OSI Network Model

Prior to discussion about specific network protocols, it's first helpful to understand the **Open Systems Interconnect** (**OSI**) network model. OSI is a seven-layer model whose layers represent various abstractions of communication. Each layer provides services to the layer above it, and receives services from the layer beneath. The common terminology for these layers is a *protocol stack*.

The layers in the OSI model are:

- Physical
- Data link
- Network
- Transport
- Session
- Presentation
- Application

These layers are shown in Figure 10-5. Some of the phrases that can help the reader remember the layers are:

- Please Do Not Take Sales People's Advice
- Please Do Not Throw Sausage Pizza Away
- Please Do Not Touch Steve's Pet Alligator
- People Desperately Need to See Pamela Anderson
- All People Seem To Need Data Processing (this one is backwards)

These layers are discussed in more detail below.

Physical The **physical layer** of the OSI model is concerned with a network's physical media, whether electrical, optical, or radio frequency, as well as details such as voltages and frequencies. Several standards in use at the physical layer include: RS-232, RS-422, T1, E1, 10Base-T, SONET, DSL, 802.11a physical, and Twinax.

The physical layer provides services to the data link layer.

Data link The **data link layer** of the OSI model is concerned with the transfer of data between nodes. The data link layer also manages error correction for any errors that take place at the physical layer.

In most physical media, bits in the physical layer are arranged into **frames**.

Examples of standards found in the data link layer are: 802.3 (Ethernet), 802.11a MAC, GPRS, AppleTalk, ATM, FDDI, Fibre Channel, Frame Relay, PPP, SLIP, Token Ring, and Wi-MAX.

The data link layer uses services provided by the physical layer, and provides services to the network layer.

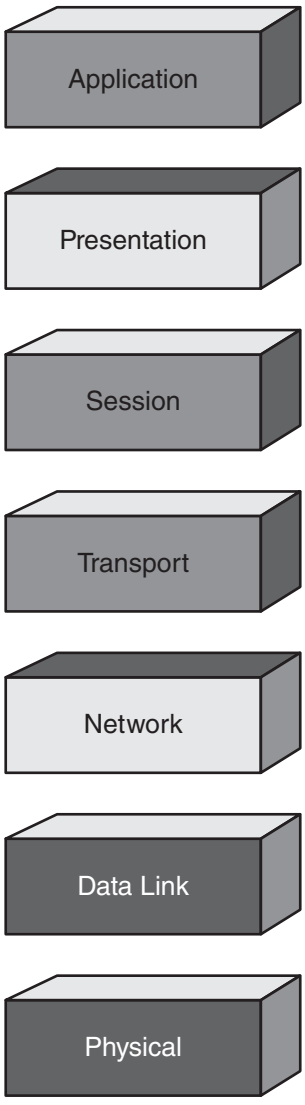


Figure 10-5 The seven layers of the OSI network model

Source: Course Technology/Cengage Learning

Network The **network layer** is used to transport variable-length data sequences between nodes. Where devices cannot handle frames or packets of certain lengths, the network layer manages fragmentation and reassembly. Communications at the network layer are point-to-point, and there is no notion of a *connection*," nor to the order of delivery of data.

Examples of standards used in the network layer are: IP, ICMP, ARP, and IPX.

The network layer uses services provided by the data link layer and provides services to the transport layer.

Transport The **transport layer** in the OSI model manages the delivery of data from node to node on a network, even when there are intermediate devices such as routers and a variety of physical media between the nodes. The transport layer manages *connections* that can guarantee the order of delivery of data packets, packet reassembly, and error recovery.

Examples of transport layer standards are: UDP, TCP, IPsec, PPTP, L2TP, and SPX.

The transport layer uses services provided by the network layer and provides services to the session layer.

Session The **session layer** manages connections between nodes, including session establishment, communication, and teardown.

Examples of standards found in the session layer include: NetBIOS, TCP sessions, and SIP.

The session layer uses services provided by the transport layer and provides services to the presentation layer.

Presentation The **presentation layer** deals with the presentation or representation of data in a communications session. Activities that can occur at this layer include character set translation, compression, and encryption.

Examples of presentation-layer standards include SSL, TLS, MIME, and MPEG.

The presentation layer uses services provided by the session layer and provides services to the application layer.

Application The **application layer** is the top-most layer in the OSI network model. This layer is concerned with the delivery of data to and from applications.

Examples of application layer standards are: DNS, NFS, NTP, DHCP, SMTP, HTTP, SNMP, SSH, Telnet, and WHOIS.

TCP/IP

The TCP/IP network protocol is built on a four-layer model that is similar to the seven-layer OSI model. The four layers in the TCP/IP model are:

- Link
- Internet
- Transport
- Application

These layers operate similarly to the seven-layer OSI model, which is to say that the layers are hierarchical and employ encapsulation. TCP/IP encapsulation is illustrated in Figure 10-6. The layers in the TCP/IP model are shown in Figure 10-7.

TCP/IP Link Layer The **link layer** is layer 1 in the TCP/IP model. Examples of link layer technologies include:

- Wi-Fi
- Ethernet

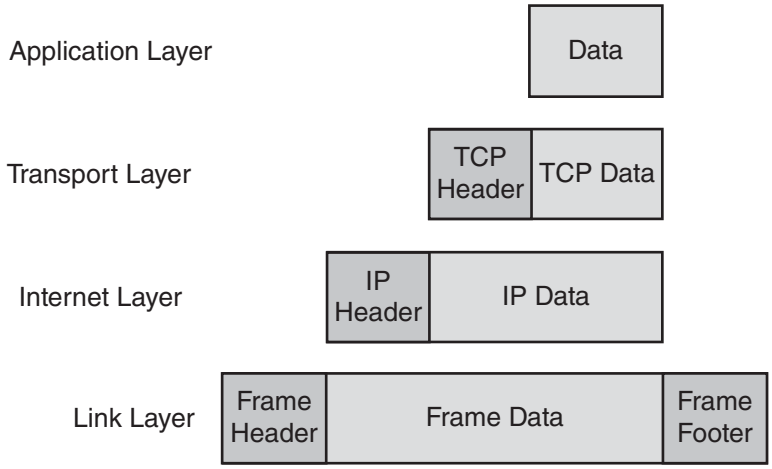


Figure 10-6 Encapsulation in the TCP/IP network model

Source: Course Technology/Cengage Learning

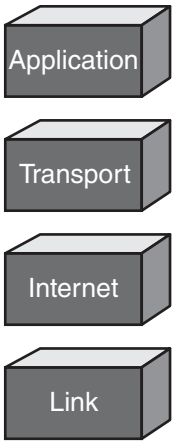


Figure 10-7 Layers of the TCP/IP network model

Source: Course Technology/Cengage Learning

- Token Ring
- ATM
- Frame Relay
- PPP

Node addressing at this layer is accomplished through some type of MAC addressing. Ethernet MAC addressing is described in detail earlier in this chapter.

TCP/IP Internet Layer The **internet layer** is layer 2 in the four-layer TCP/IP model. The internet layer is the layer that is concerned with end-to-end packet delivery, whereas layer one is concerned with node-to-node delivery. End-to-end delivery means that a packet can originate at one node, and pass through several intermediate nodes (usually routers) before arriving at the destination node.

Internet Layer Protocols Some of the protocols used at the internet layer include:

- **Internet Protocol version 4 (IPv4)**. The original Internet Protocol, IPv4 is usually referred to as simply IP. This is the core layer 2 protocol in the TCP/IP protocol suite on which most layer 3 protocols are built. IP uses a 32-bit addressing scheme that is expressed as the four octets, *xx.xx.xx.xx*. Network addressing is described in more detail in the section later in this chapter, "Network layer addressing".
- **Internet Protocol version 6 (IPv6)**. Generally expressed as IPv6, this newer version of the Internet Protocol was developed to address some of the shortcomings of IPv4, primarily the size of the address space and the lack of security. IPv6 uses a 128-bit address space that is expected to forever alleviate the current shortage of available addresses in the IPv4 Internet.
- **Address Resolution Protocol (ARP)**. This protocol is used to translate a network IP address into a network MAC address. For instance, if a node wants to send a network packet to a node at address 192.168.5.2, it will send an ARP request onto the network that asks, essentially, what station has IP address 192.168.5.2? If a node on the network has that address, it will answer and provide its MAC address in the response.
- **Reverse Address Resolution Protocol (RARP)**. This protocol is used to translate a known MAC address into an IP address. RARP has been superseded by DHCP, which has a richer feature set than merely MAC to IP translation.
- **Internet Control Message Protocol (ICMP)**. ICMP is a protocol used for error messages and utility functions such as **PING** (a tool used to test connectivity to another node on a network) and **TRACEROUTE** (a tool used to discover the node-by-node path to a destination node). When a node sends a message to another node that is temporarily unreachable, the router on the destination node's network will send a "destination host unreachable" error back to the requesting node. There are 255 different messages types available in ICMP that are used for different purposes; for instance, Echo Request is message number 8 while Echo Reply is message number 0.
- **Internet Group Management Protocol (IGMP)**. This protocol is used to manage multicast groups, and is analogous to ICMP which is used for unicast.
- **IP security (IPsec)**. This is a suite of protocols used for securing IP communications with authentication and encryption. IPsec is typically used as a tunneling protocol, wherein messages at higher levels of the TCP/IP protocol (layers 4 and 5) are encapsulated within encrypted IPsec packets. This use is typically found in remote access and site-to-site tunneling over the Internet.

Internet Layer Routing Protocols Routing protocols are used by network routers to determine how to send network packets to destination networks. Some network routing protocols exist in the internet layer including:

- RIP
- OSPF
- IS-IS
- BGP

Network routing protocols are described in more detail later in this chapter.

Internet Layer Addressing TCP/IP's internet layer addressing is designed to uniquely identify nodes on networks including the global Internet. Network addresses in IPv4 are 32 bits in length and are expressed as a dot-decimal notation, xx.xx.xx.xx, where the range of each 'xx' is 0-255 decimal. A typical network address is 141.204.13.200.

The TCP/IP internet layer addressing scheme has several characteristics including:

- **Subnets and subnet masking**. While an IP address consists is 32 bits in length and expressed in the dot-decimal notation, an IP address is, for some purposes, actually divided into two parts: the network address and the node address. For instance, the first 24 bits of an IP address may be a network address (that is, the IP address of a *network* rather than a single station), and the remaining 8 bits is the station address. Nodes on the network need to know what part of the IP address is for the network; this is determined by the network's **subnet mask**. A typical subnet mask is 255.255.255.0, which in this case indicates that the first three decimal numbers (or the first 24 bits) of an IP address is the network identifier, and the last decimal number (or the last 8 bits) is a node address. When a node wants to send a packet to another node, it will mask the destination's address with the subnet mask to determine whether the destination node is on the same network or a different network; if the same network, the node will send the packet directly; if a different network, the node will send the packet to the network's gateway, which is usually a router.
- **Gateways**. Every network has a *gateway*, which is usually a router that is connected to other networks. When a node wants to send a packet to another node, it must first determine whether the destination node is on the same network by masking the destination's IP address with the subnet mask. If the destination node is on a different network, the node sends the packet to the node at the gateway IP address; that node is usually a router that will consult its routing tables to determine how to forward the packet to its destination.
- **Address allocation**. Organizations that wish to communicate with other nodes on the Internet must obtain routable addresses from a Regional Internet Registry (RIR), usually an ISP (Internet Service Provider). The RIR/ISP will assign a single address or a block of addresses (usually a subnet or a part of a subnet). The organization then assigns individual addresses to devices on its network.
- **Reserved address blocks**. Not all network addresses are available for general use. Some address blocks that are reserved include:

  10.0.0.0-10.255.255.255—private networks. Organizations are encouraged to assign private network IP addresses to nodes in its internal networks and then utilize Network Address Translation (NAT) at its border routers to dynamically translate those private network addresses into one of its allocated addresses.

  127.0.0.1-127.0.0.255—loopback. This is a special address that is used to signify a node's own address. In the vernacular, 127.0.0.1 is always "me" on a network.

  172.16.0.0-172.31.255.255—private networks. Used for the same purpose as 10.0.0.0-10.255.255.255.

  192.168.0.0-192.168.255.255—private networks. Used for the same purpose as 10.0.0.0-10.255.255.255.

  224.0.0.0-239.255.255.255—multicast. Reserved for multicast traffic.

- **Network Address Translation (NAT)**. This is a scheme whereby an organization's border router (the router connecting its internal networks to its external networks—usually the Internet) will dynamically translate the address of packets crossing the network boundary from internal, private addresses to routable, public addresses. NAT was developed as one of the stopgap measures to forestall the impending shortage of allocate IP addresses by requiring that organizations assign private network addresses to nodes in its internal networks.
- **Classful networks**. Originally, the entire available IP address space was divided into two parts: the network number that consisted of the first 8 bits of an IP address, and the host address that consisted of the remaining 24 bits. This resulted in only 256 possible networks in the entire Internet, which was infeasible. The concept of *classful networks* was introduced, which results in a far greater number of smaller networks. The network classes that were developed are:

  Class A. A *Class A* network consists of an 8 bit network address and a 24 bit host address. Thus, a Class A network could contain 16,777,214 nodes. 126 such networks were created for the very largest organizations.

  Class B. A *Class B* network consists of a 16-bit network address and a 16-bit host address. Each network could contain 65,534 nodes; 16,382 of these networks were created.

  Class C. A *Class C* network consists of a 24-bit network address and an 8-bit host address. Thus, a Class C network could contain 254 nodes; over 2 million such networks were created.

  This scheme of classful networks would prove to be short-lived; this gave rise to Classless Inter-Domain Routing, discussed next.

- **Classless Inter-Domain Routing (CIDR)**. *Classless Inter-Domain Routing* did away with the rigid scheme of only Class A, B, and C networks and permitted the creation of any length subnet mask (called a *Variable Length Subnet Mask*, or *VLSM*), from 8 bits to 31 bits. This permitted ISPs to be able to allocate very small networks to customers that did not require more than a very few addresses. The introduction of CIDR led to a far more efficient allocation of available IP addresses on the Internet.
- **Addressing**. The internet layer provides for different addressing types that will result in messages being sent to one or more destination nodes. These types are:

  Unicast. The most common type of addressing where a packet is sent to a single IP address destination.

  Broadcast. A packet is sent to a network's *broadcast address*, which causes the packet to be sent to all nodes on a network. DHCP and ARP utilize broadcast.

  Multicast. A packet is sent to a group of receiving nodes. A packet is sent to a multicast address (in the range 224.0.0.0 to 239.255.255.255), and routers in the network track recipients and propagate packets to destinations as needed.

  Anycast. A packet is sent to only one of a group of nodes, whichever is closest or most available.

TCP/IP Transport Layer The **transport layer** is layer 3 in the four-layer TCP/IP model. The two protocols that are principally used in the transport layer are TCP and UCP; each is explained below.

TCP Transport Protocol **Transmission Control Protocol (TCP)** is a *connection-oriented* transport protocol used to carry messages within a *session* between two nodes. In TCP, two nodes can establish a persistent connection, over which messages can be sent back and forth.

Protocols in the application layer (layer 4) that use TCP include: FTP, HTTP, and TELNET).

Characteristics of the TCP protocol are:

- **Connection**. A node that wishes to communicate to another via TCP will do so by establishing a connection. This is accomplished via a *three-way handshake* that consists of three messages that are sent between the two nodes to establish the connection:

  The requesting station sends a SYN to the destination station

  The destination station responds with a SYN-ACK

  The requesting station responds with an ACK

  At this point the connection is established.

- **Port number**. Packets in TCP have a *source port* number and a *destination port* number. This permits two stations to establish several unique connections that are distinguished by different port numbers. When a connection is established, the connection will first begin on a well known port (for instance, FTP's port number is 21 and TELNET's is 23), then the stations will agree to higher-numbered *ephemeral ports* over which their connection will take place. You could say that a TCP session is established on a well known port number and transferred to unique, unused ports. It's like two people meeting in a restaurant and then agreeing to go someplace else.
- **Reliability**. By design, a packet sent over the TCP protocol is guaranteed to be delivered to its destination—provided the destination exists and is reachable. Packets that are lost are retransmitted, and duplicate packets are discarded.
- **Sequencing**. Packets sent over the TCP protocol are guaranteed to be delivered in the same order that they were sent. TCP packets include sequence numbers that permit device drivers within nodes to assure the correct order of delivery.
- **Flow control**. TCP by its design cannot send data faster than the receiving node can accept it. This is accomplished by the receiving station acknowledging the successful receipt of packets. Upon establishment of the connection, the two stations agree to the size of the *sliding window*, which is the number of in-transit packets that can exist at any given time.

UDP Transport Protocol The **User Datagram Protocol (UDP)**—sometimes coined the *unreliable datagram protocol*) is a connectionless protocol used to carry messages between nodes. UDP is very lightweight in comparison to TCP—it's a low-overhead protocol that is suitable for some types of connections. Some of the protocols that use UDP include: DNS, VoIP, and TFTP.

The characteristics of the UCP protocol are:

- **Connectionless**. Unlike TCP, UDP has no sense of a connection or a session. When a station wants to send a packet over UDP to a destination, it just sends it.
- **Unreliable**. UDP does not guarantee that a packet will be delivered to a destination. If a UDP packet is lost because of some error or congestion on the network, the destination station will not receive it.
- **No sequencing**. There is no sequencing of packets. If several UDP packets are sent from one station to another, they *may* arrive in the correct order, but there is no guarantee of it.
- **No flow control**. If a sending station is able to send stream of UDP packets faster than the destination station can process them, then some packets may be lost.
- **Port number**. Like TCP, applications using UDP use reserved port numbers (for example, DNS uses port 53), but because there are no connections in UDP there are no *ephemeral ports*.

TCP/IP Application Layer The **application layer** is layer 4—the topmost layer—of the TCP/IP model. The protocols in the application layer provide application functions for application programs, some of which are used directly by computer users.

There is a multitude of protocols in the application layer of the TCP/IP stack. A few of them are described here:

- **Dynamic Host Configuration Protocol (DHCP)**. This protocol is used to configure basic network configuration settings for network nodes such as workstations. A workstation sends a broadcast query on the network, which is answered by a DHCP server that responds with parameters that the workstation uses to configure its network interface, including: IP address, subnet mask, default gateway, and DNS servers.
- **Domain Name Service (DNS)**. This is the protocol that is used to translate domain names (such as www.cengage.com) to an IP address (such as 129.24.75.66). DNS servers throughout the Internet contain databases of domain names and their corresponding IP addresses.
- **Finger**. This protocol is used to make queries about the status of computer users. Finger is primarily supported on UNIX systems.
- **File Transfer Protocol (FTP)**. This protocol is used for batch and human attended file transfers between computers.
- **Hypertext Transfer Protocol (HTTP)**. This is the protocol used by web browsers and web servers to exchange HTML and XML content.
- **Lightweight Directory Access Protocol (LDAP)**. This is a protocol used to authenticate users and provide directory services.
- **Network File Service (NFS)**. This protocol is used to share file systems across a network.
- **Network Information Service (NIS)**. This is the original directory service protocol developed by Sun Microsystems. NIS has been replaced by the more secure and

versatile NIS+. NIS and NIS+ are used to centralize authentication and system configuration information for computers in a network.

- **Network Time Protocol (NTP)**. This protocol provides high-precision time-of-day information so that participating computers' clocks will be more accurate. The clocks in computers are notoriously imprecise, which led to the development of this protocol.
- **Remote login (Rlogin)**. This protocol is used to log in to another computer over a network. This protocol is now considered unsafe, and has been superseded by the SSH protocol.
- **Remote Procedure Call (RPC)**. This protocol provides the means for one computer requesting the execution of a subroutine or procedure on another computer.
- **Remote shell (Rsh)**. This protocol is used to execute commands on another computer. Now considered unsafe, Rsh is superseded by the SSH protocol.
- **Session Initiation Protocol (SIP)**. This is a signaling protocol used to establish voice or video communications sessions. SIP is often used to set up a VoIP telephone call.
- **Simple Mail Transport Protocol (SMTP)**. This is the protocol that is used to transport e-mail among e-mail servers and across the Internet.
- **Simple Network Management Protocol (SNMP)**. This is a network management protocol that is used to remotely monitor and manage network devices and systems.
- **TELNET**. This is a protocol used to establish a raw TCP session over a network to a service on another computer. It is possible to establish a session to virtually any service, such as DNS, SMTP, SNMP, or NFS, and then type commands in by hand and observe responses. TELNET is one of the first Internet standards
- **Trivial File Transfer Protocol (TFTP)**. This is a file transfer protocol that is a subset of FTP. TFTP has no authentication and is considered unsecure for most applications.
- **Voice over Internet Protocol (VoIP)**. This protocol is used to transport voice traffic in Internet-based telephone calls.
- **Whois**. This protocol is used to query a whois server. Whois is usually used by Internet registrars that issue and manage Internet domain names and IP address space.

TCP/IP Routing Protocols

A routing protocol is a router-to-router communication protocol used by routers to help determine the most efficient network routes between two nodes on a network.

In a routing protocol, routers communicate information about network destinations to neighboring routers. This sharing of routing information gives each router greater visibility of the greater network, which makes it more capable of making good routing decisions.

Prior to routing protocols, routers employed only static routes, in which each router was configured with information about neighboring networks. No dynamic route information was available. Today, routers in some environments are often configured with a limited number of static routes, usually for adjacent endpoints such as servers.

RIP One of the earliest routing protocols, the **Routing Information Protocol (RIP)** uses hop count as the primary routing metric. The fewer number of hops for a given destination, the

more favored a destination will be, regardless of the actual link speeds involved. The maximum number of hops supported by RIP is 15, which seemed adequate when it was invented in the 1970s, but this limitation is one of several reasons why RIP has given way to more scalable and reliable protocols, such as OSPF and IS-IS.

RIP runs over the UDP protocol on port 520.

IGRP Cisco's proprietary **Interior Gateway Routing Protocol** (**IGRP**) was developed to overcome the limitations of RIP (mostly that its only routing metric was *hop count*). IGRP supports multiple metrics; bandwidth, delay, load, MTU, and reliability. IGRP's maximum hop count is 255. IGRP has been replaced by EIGRP, which is discussed later in this section.

IGRP does not use TCP or UDP but runs directly over IP.

EIGRP **Enhanced Interior Gateway Routing Protocol** (**EIGRP**) is a Cisco proprietary routing protocol that replaces IGRP through a number of improvements, including variable length subnet masks and improved algorithms.

OSPF The **Open Shortest Path First** (**OSPF**) routing protocol is a widely used routing protocol in large enterprise networks. Routers in an OSPF routed network form peer relationships with neighbors called *adjacencies*.

An OSPF network is divided into *areas*; *area zero* is the backbone, or core, of an OSPF network. Other areas logically and physically connect to area zero. Route information is communicated from area zero routers to routers in other areas of the network.

OSPF can operate securely through the use of passwords in cleartext or hashed using MD5.

OSPF does not use TCP or UDP, but instead uses IP directly, using IP protocol 89.

IS-IS The **Intermediate system to intermediate system** (**IS-IS**) routing protocol is primarily used by ISPs and other network service providers. It is based on *areas*, similar to OSPF, but does not rely on a central *area zero*.

IS-IS does not use TCP, UDP, or IP, but instead communicates at the data link layer. Routing information is established by neighboring routers that each build a table of routes based upon information accumulated through all of the network's adjacent router relationships.

BGP The **Border Gateway Protocol** (**BGP**) routing protocol is the protocol that is used for the Internet's main backbone routers. BGP peers (adjacent routers) are established through manually configuration. BGP routers build massive routing tables (with tens of thousands of entries) based upon the accumulation of peer relationships. The BGP protocol uses TCP port 179.

Remote Access/Tunneling Protocols

Several TCP/IP-based protocols have been developed that permit the *tunneling* of network traffic between computers, networks, and between a computer and a network. A **tunnel** provides packet encapsulation and can serve one of several purposes:

- **Protect communications**. A tunnel can utilize encryption, which will prevent an intermediate party from being able to eavesdrop on the communication.

- **Authenticate communications**. A tunnel can include authentication, in order to determine whether the party is permitted to communicate through the tunnel to the target network.
- **Hide a service provider network**. A service provider can provide a tunnel between the customer and the target network, thereby hiding its network from its customers.

Some examples of tunneling are shown in Figure 10-8.

VPN Virtual Private Network (VPN) is a generic term that signifies any of the remote access tunneling protocols, including those discussed in this section. VPN does not refer to a specific protocol or technology, but instead is a term that could mean *SSL, IPsec, L2TP*, or another protocol.

SSL/TLS **Secure Sockets Layer (SSL)** is a TCP/IP layer 4 tunneling protocol. An encrypted protocol that utilizes several encryption algorithms and key lengths, SSL is most often used to encrypt user application sessions such as:

- **HTTPS:** User HTTP sessions to web servers encrypted with SSL are known as **HTTPS**.
- **FTPS:** File transfer protocol (FTP) protected with SSL.
- **Remote access:** Some remote access software is designed to utilize the SSL software that is built-in to client operating systems.

SSL is superseded by Transport Layer Security (TLS), which is very similar to SSL.

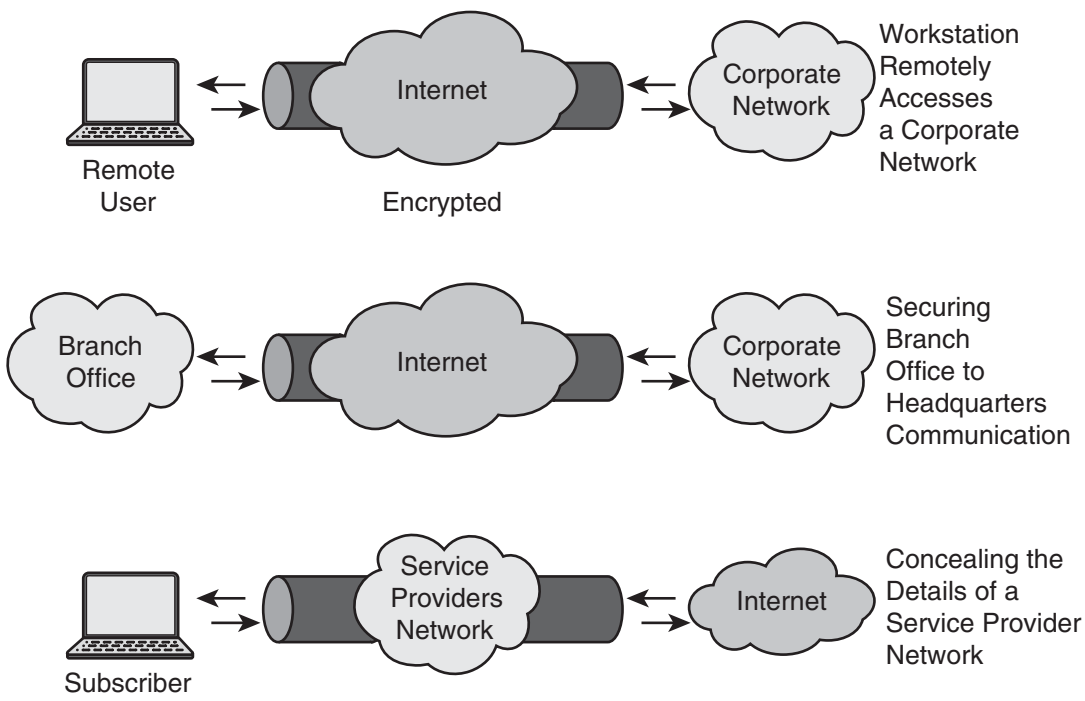


Figure 10-8 Examples of network tunneling

Source: Course Technology/Cengage Learning

SSH **Secure Shell (SSH)** is a TCP/IP layer 4 protocol that facilitates secure communications between systems. SSH began its life as a secure (encrypted) replacement for rsh (remote shell), rcp (remote copy), rlogin (remote login), and telnet, but it can also be used to tunnel other protocols including:

- **File transfer**. The secure file transfer protocol, SFTP, is essentially FTP over an SSH channel.
- **File backup and mirroring**. The *rsync* program uses SSH for file backup and mirroring.
- **Secure filesystem**. SSH permits the remote mounting of the SSH Filesystem over a network.
- **VPN**. SSH can be used as the basis for a full fledged VPN connection.
- **X11**. SSH can be used to protect X11 (X-Windows) connections between systems.

IPsec IPsec (IP security) is a suite of protocols used to secure network communications with authentication and encryption. It is typically used as a tunneling protocol to encapsulate messages at higher levels of the TCP/IP protocol (layers 3 and 4). IPsec is typically used in remote access and site-to-site tunneling over the Internet.

L2TP **Layer 2 Tunneling Protocol (L2TP)** is a TCP/IP protocol used to protect TCP/IP communications at higher levels through encapsulation.

L2TP emulates a data link layer protocol like Ethernet, but it is actually transported over UDP from network to network. When an L2TP tunnel is set up between two endpoints, the L2TP tunnel appears as a virtual network interface; packets for specific destination networks are sent to the L2TP *interface*, where they are actually encapsulated within UDP packets. L2TP tunnels are usually encrypted with IPsec.

PPTP **Point to Point Tunneling Protocol (PPTP)** is an early tunneling/encapsulation protocol that has been largely superseded by L2TP and IPsec. PPTP was implemented in early versions of Microsoft Windows as a dial-up remote access protocol that was easy to configure because it required only a password and no shared keys. Internally PPTP is a PPP session that is transported over a *GRE* (*General Routing Encapsulation*) tunnel.

PPP **Point to Point Protocol (PPP)** is a data link layer (TCP/IP layer 2) protocol that is commonly used for dial-up Internet access. Because it is a data link layer protocol, PPP can encapsulate not only TCP/IP but also NetBIOS, IPX (Novell), and AppleTalk.

SLIP **Serial Line Interface Protocol (SLIP)** is an early implementation for transporting TCP/IP over serial lines, fiber connections, and dial-up connections. SLIP has been largely superseded by PPP.

Network Authentication Protocols

There are several network-based protocols that are used for *authentication*, which is the verified identification of an individual who desires to access a resource.

There are two types of protocols used in network authentication: those that interact between a user and an access point or gateway, and those that occur between an access point or gateway and an authentication/authorization/accounting (*AAA*) server. Both types of protocols are often used in environments in which users are required to authenticate to a system or network.

RADIUS The **Remote Authentication Dial In User Service (RADIUS)** protocol that is used to support the authentication of user access to networks and systems. The RADIUS server may store user credentials itself, or the RADIUS server may obtain them from an LDAP, Kerberos, Active Directory, or other authentication server.

Upon authentication, a RADIUS server will return information to the requesting client access device such as assigned IP address, permitted connection duration, and access restrictions. RADIUS also includes message types that are used for accounting—that is, the ability to measure a user's utilization of a network resource.

RADIUS messages travel between an access device and an *AAA* (authentication, authorization, and accounting) server. Figure 10-9 shows a typical access scenario, user access to the Internet via a wireless service provider.

Diameter Diameter is an AAA protocol that is the successor to the RADIUS protocol. Diameter is not an acronym, but a pun on the term RADIUS (a circle's diameter is twice its radius).

Like RADIUS, the Diameter protocol is found between a network access point or gateway and an AAA server such as LDAP or Active Directory.

TACACS Terminal Access Controller Access-Control System (TACACS) is a remote authentication protocol used to authenticate user access to a computer or network-based resource.

Like RADIUS, the TACACS protocol occurs between an access point or gateway and an AAA server such as LDAP.

TACACS has been largely replaced by two successors, TACACS+ and RADIUS.

802.1X **IEEE 802.1X** is a standard that is used for port-level network access control. A network that uses 802.1X requires all devices to authenticate to the network before the device will be able to communicate on the network. This is separate from any user authentication that may be required.

CHAP **Challenge-Handshake Authentication Protocol (CHAP)** is a protocol that is used to authenticate a user to a system or (usually) network resource. The CHAP protocol occurs between a user terminal or workstation and an access point or gateway.

CHAP works by using a *three-way handshake* as follows:

1. gateway sends a challenge message to the user system
2. user system responds with a value that is a hash of the challenge plus a shared secret that both the user and the gateway know

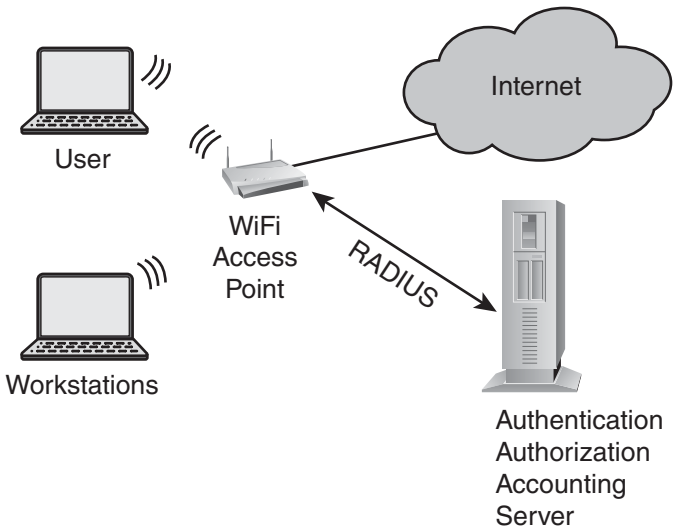


Figure 10-9 RADIUS support of a Wi-Fi access point

Source: Course Technology/Cengage Learning

3. gateway compares user system's hashed value with its own; if they match, the connection is permitted; if they do not match, the connection is terminated

The PPP protocol uses CHAP to authenticate the PPP connection.

EAP The **Extensible Authentication Protocol** (**EAP**), is an authentication framework used to authenticate users in wired and wireless networks. EAP is used for authentication in WPA and WPA2 wireless network standards.

Several EAP protocols exist, including:

- **EAP-PSK**. This is a mutual authentication protocol using a Pre-Shared Key (PSK), usually to protect a network-based resource using a single password for all users.
- **EAP-IKEv2**. This is authentication based upon the Internet Key Exchange Protocol (IKE).
- **EAP-AKA**. This is used for authentication in UMTS (Universal Mobile Telecommunications System), a mobile communications standard.
- **EAP-SIM**. Used for authentication in GSM (Global System for Mobile Communications), a global standard for mobility devices such as cell phones and wireless broadband modems.
- **LEAP**. This is the *Lightweight Extensible Authentication Protocol* that is a proprietary EAP protocol developed by Cisco Systems prior to the establishment of the 802.11i standard.

PEAP **Protected Extensible Authentication Protocol** (**PEAP**) (and sometimes known as *Protected EAP*), is a protocol used in wireless networks to authenticate users. PEAP uses an SSL/TLS tunnel to encrypt authentication information that is exchanged between the client and the authentication server or device.

PAP The **Password Authentication Protocol (PAP)** is a simple authentication protocol used by PPP to authenticate users. PAP is considered unsecure because user credentials are passed unencrypted.

Network-Based Threats, Attacks, and Vulnerabilities

By their nature, networks are vulnerable to *threats* and *attacks*. Large networks connect vast numbers of users together, and in many networks there is no overt control over the types of devices that users can connect to a network; hence, there is often little or no control over the nature of the traffic that a user can transmit over a network. These points are especially true of the global Internet, where hundreds of millions of computers are connected to millions of networks.

Sometimes the terms *threat*, *attack*, and *vulnerability* are interchanged or misused. They are defined in this section.

Threats A *threat* is the expressed potential for the occurrence of a harmful event such as an attack. There are many types of threats including:

- Malware in the wild that is spreading to vulnerable systems
- A disgruntled employee with the ability to do harm
- The high rate of stolen laptops

Attacks **Attacks** are actions taken against a target resource with the intention of doing harm. There are many kinds of attacks that can take place over a network, including:

DoS A Denial of Service (DoS) attack is an attempt, on the part of the attacker, to incapacitate a target system or resource. The attack can take one of two forms:

- **High volume**. The attack may consist of a high volume of traffic that is designed to incapacitate the target, by causing its resources to become exhausted.
- **Malfunction**. The attack may consist of one or more specially crafted messages that are designed to disable the target by causing its malfunction.

The intention of a DoS attack is to make the target resource unavailable for its intended use.

DDoS A Distributed Denial of Service (DDoS) attack is an attack that is designed to overwhelm a target with a vast amount of incoming traffic that originates from many sources. A DDoS attack may originate from dozens, hundreds, or thousands of systems.

A DDoS attack can originate from a *Botnet*, which is a collection of zombie computers that are remotely controlled by a botnet operator who uses software to control them. Figure 10-10 depicts a typical DDoS attack.

Teardrop A **teardrop** attack is one in which the attacker sends mangled packet fragments with overlapping and oversized payloads to a target system. Earlier versions of operating systems had bugs in the fragment reassembly code in their TCP/IP drivers that would cause the system to crash.

Sequence Number A **sequence number attack** consists of an attacker who attempts to hijack or disrupt an existing TCP session by injecting packets that pretend to originate from

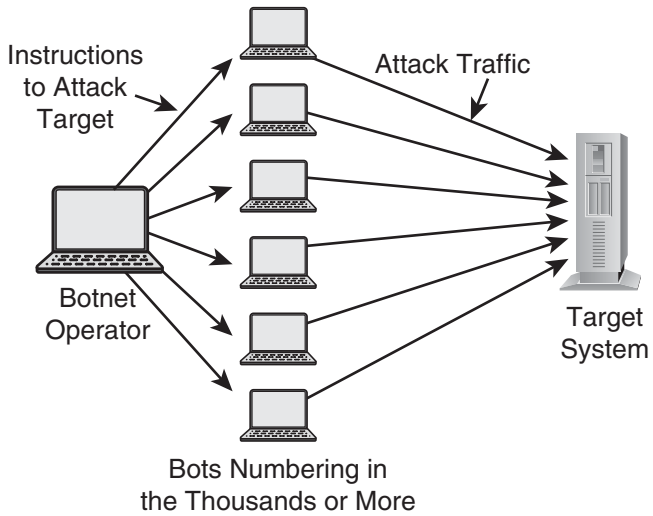


Figure 10-10 Distributed Denial of Service (DDoS) attack

Source: Course Technology/Cengage Learning

one of the two computers in the session. The attack can be successful if the attacker correctly guesses the sequence numbers and the timing of packet injection; the target system may accept some or all of the spoofed packets instead of the legitimate ones.

Smurf A **smurf** attack consists of a large number of forged ICMP echo requests. The packets are sent to a target network's broadcast address, which causes all systems on the network to respond. The packets are forged with the *from* address of the target system, resulting in a large number of ICMP echo reply messages from all of the systems on the network.

Ping of Death The Ping of Death (PoD) is an attack on a system where the attacker sends a ping packet of length 65,535 bytes to the target system. The TCP/IP protocol will fragment this packet as it travels through the network; it is then reassembled on the target system, causing a buffer overflow.

This is a historic attack; most systems have been fixed and are no longer vulnerable.

SYN Flood A **SYN flood** attack is a Denial of Service attack in which the attacker sends a large number of SYN packets to the target system. This attack is designed to overwhelm the resources of the target system until it is unable to respond to legitimate traffic.

A SYN packet is the first packet in a TCP connection *three-way handshake*. By sending a SYN packet to a system, it allocates resources in memory. When large numbers of SYN packets are sent to a system, the number of simultaneous TCP sessions will be exhausted, resulting in the system failing to respond to new, legitimate network messages.

Worms A worm is a type of *malware* that has the means for automatic self-replication. They spread by exploiting known vulnerabilities that permit the malicious program to infect new victims.

The most "successful" worms are able to spread quickly by virtue of efficient mechanisms used to locate and infect new hosts.

Worms usually inflict damage on account of the high volume of network traffic that they cause when large numbers of infected systems are searching for more victims.

Spam Spam is the common term for **unsolicited commercial e-mail** (**UCE**). Spam greatly adds to the volume of e-mail traffic on the Internet. Often, the volume of spam is so high that over 90% of all e-mail on the Internet is spam.

Spam's effect on networks is the degradation of performance through network and e-mail server congestion, as well as the machine cycles required to filter and remove spam messages.

Phishing Phishing is a type of spam where the contents of a message is designed to masquerade as a trustworthy organization, with the intention of defrauding the recipient by luring them to an authentic-looking website where they will enter secret information such as userids, passwords, bank account or credit card numbers, date of birth, social insurance numbers, and so on. Figure 10-11 shows a typical phishing e-mail.

From: Nationwide Online (accounts@nationwide.co.uk)
To:
Date: Saturday, January 19, 2008 7:11:52 AM
Subject: Your account has been compromised

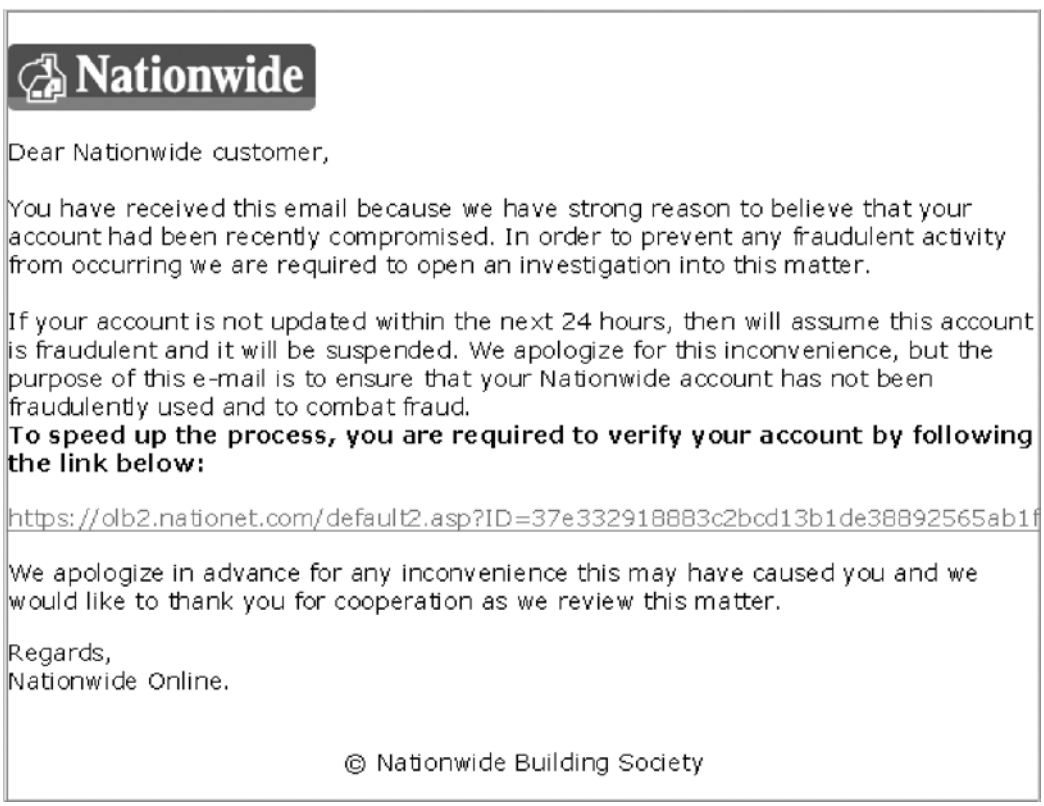


Figure 10-11 Typical phishing scam e-mail message

Source: Course Technology/Cengage Learning

A phishing message can also ask its victim to simply reply to the e-mail, providing secret information in the reply message.

Vulnerabilities Vulnerabilities are defined as weaknesses that make targets susceptible to attack, resulting in harm or compromise of sensitive information. Several types of network oriented vulnerabilities are discussed in this section.

Unnecessary Open Ports An *open port* is a network-based listener that is associated with a program or service that runs on a system and that communicates via network messages. An unnecessary open port is such a program or service that is not necessary for the system to carry out its functions.

Most vulnerabilities that are identified on systems are found within the software programs that accept messages through network ports. If a system has many such ports open, then the probability that the system as a whole contains serious vulnerabilities increases accordingly.

Unpatched Systems Security vulnerabilities in software programs and operating systems are found fairly regularly. Often, these vulnerabilities are known to hackers who create malicious code that is able to exploit these vulnerabilities, resulting in the compromise of the security of target systems.

The makers of software programs and operating systems usually respond quickly to news of vulnerabilities and create security patches, which are fixes to the programs so that the vulnerabilities are no longer present. But many systems do not have these patches installed, which make them continually vulnerable and open to attacks.

Poor and Outdated Configurations The techniques used by hackers to break into systems are advancing regularly, resulting in systems that were once considered secure to become vulnerable to these new techniques. But frequently, systems are built that are not secure to begin with. Also, systems are sometimes moved from a low-threat area to a high-threat area, leaving them open to attack.

Exposed Cabling Any network cabling (other than what is usually found at a user's workstation) that is exposed can be targeted by an attacker. With the right tools and techniques, most cable types can be penetrated and network traffic intercepted and tampered with.

Network Countermeasures

Personnel at all layers of the technology stack, including network engineers, system engineers, database administrators, and application designers, all need to enact countermeasures to make their environments less susceptible to attack. Many of the common techniques for repelling network-borne attacks are discussed in this section.

Access Control Lists

The earliest, but still common, technique used to block unwanted traffic is the use of **Access Control Lists** (**ACLs**), on network routers. ACLs, while they may lack the fortitude to handle some of the more complex types of TCP/IP sessions that include the use of dynamically allocated ports, they often represent a good first line of defense to block several types of unwanted traffic. If nothing else, this can relieve firewalls of many types of unwanted messages, improving overall throughput.

Firewalls

Invented in the 1980s, firewalls are devices placed at a network boundary that are designed to block unwanted incoming or outgoing traffic. A firewall works by examining each packet and consulting a list of *rules* to determine whether the packet should be permitted to pass through the firewall or be blocked. In a large organization, the list of rules in a firewall can become unwieldy, possibly resulting in unwanted traffic entering or leaving the network.

There have been three generations of firewalls, which are:

- **Packet filters**. The earliest firewalls made pass-or-drop decisions by examining the source and destination IP addresses and port numbers. They were unaware of TCP sessions and did not handle many of the advanced characteristics of TCP sessions that include the dynamic changes in port numbers that occur.
- **Stateful packet filters**. The second generation of firewalls overcame the problems in the first generation by being smarter about the techniques used by some TCP/IP protocols and how their use of dynamic port numbers confused early routers.
- **Application layer filters**. These are the newest types of firewalls that go one big step further by examining the payloads of network packets to determine whether they contain malicious patterns or content.

Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDS), are programs or devices that are designed to observe network communications and generate alerts if any harmful or malicious traffic is detected.

There are two primary types of IDS, which are:

- **Network-based IDS** (**NIDS**). A NIDS usually takes the form of a standalone appliance, or a blade in a modular network router or switch.
- **Host-based IDS** (**HIDS**). An IDS program can be installed on a server. The HIDS will watch incoming network traffic and possibly other types of events on the system that indicate tampering.

The primary characteristic of an IDS is that it is passive. An IDS generates alert messages when unwanted traffic and other events occur, but does nothing else about them.

A common complaint about IDS systems is the number of *false positives*, or alerts that do not actually signify malicious traffic that warrants attention.

Intrusion Prevention Systems (IPS)

An **intrusion prevention system (IPS)** is a device or program that not only senses unwanted traffic but also blocks that unwanted traffic. IPS is considered an evolution of passive IDSs that only generate alerts.

There are two primary types of IPS, which are:

- **Network-based IPS (NIPS)**. A network-based IPS can block individual packets, or even logically disconnect a suspected malicious device from the network. Like a NIDS, a NIPS can be a standalone appliance or a blade in a router or switch. A NIPS usually communicates with a router, firewall, or switch in order to cooperate in blocking traffic from offending IP addresses.
- **Host-based IPS (HIPS)**. A host-based IPS is a program on a server that can both detect as well as block unwanted events.

A potential risk of IPS systems is the possibility that traffic from legitimate systems may be blocked, resulting in disruption or downtime for applications or services.

Protect Network Cabling

All exposed network cabling should be moved, covered, or placed in conduits, so that they will not be subject to deliberate tampering or accidental damage.

Anti-Virus Software

Anti-virus software that is installed on servers can detect worms and other malware and prevent them from installing themselves.

Private Addressing

While the primary purpose of private addressing was to conserve publicly-routable IP addresses, a desirable side effect is the fact that systems with private IP addresses are a lot more difficult to attack. Many home-based and SOHO-based broadband routers rely only on private addressing to protect systems on the home or small business network.

Close Unnecessary Ports and Services

A highly effective method to reduce the probability of successful attack is to close all unnecessary and unused ports and services on systems and devices. Unused and unnecessary programs only increase the *attack surface* without providing any actual benefit—they are only a liability. Examining a system and eliminating everything that does not support the system's core purpose will reduce the likelihood that a system can be compromised.

Install Security Patches

All applicable security patches should be installed on servers and network devices as soon as it is practical to do so. In most cases, it is inadvisable to immediately install security patches, as doing so may impair legitimate functions. Instead it is recommended that patches are installed on less-critical systems first to ensure that the patches do not negatively affect their function. Then, when it's considered safe, security patches should be installed on production systems and devices.

Usually this process should take no less than 30 days, but there are times when patches are much more urgent, necessitating their installation within hours or days of release.

UTM

Unified Threat Management (**UTM**) is a term used to describe security devices and appliances that perform many functions in order to simplify the defenses in a network. A UTM system can contain one or more of the following:

- Firewall
- IDS
- IPS
- Anti-virus
- Anti-spam
- World Wide Web content filtering

Gateways

A gateway is a general term to mean a system or device that provides some intermediary or translating function in a network. Routers, firewalls, and e-mail servers are examples of gateways, but many more types exist.

In terms of security countermeasures, a gateway is a system or device that provides some protection against one or more threats. Examples of this type of use include:

- **E-mail gateway**. Rather than having e-mail from the Internet be delivered directly to an enterprise e-mail server, incoming e-mail can instead be delivered to an e-mail relay that resides in the DMZ. If a successful attack were launched against an e-mail server, such an attack on a DMZ e-mail relay could prove far less harmful than a successful attack on an internal e-mail server.
- **Multi-tier application architecture**. Many web-based applications are designed so that web services, application services, and database services reside on different servers. By providing a multi-tiered application architecture (especially when firewalls are used in between the layers), the servers containing data are protected by a deep defense in depth.
- **World Wide Web content filter**. Because so many attacks are delivered via compromised web servers to end user systems via web browsers, employing Web content filters reduce the risk that malicious code will reach an end user workstation. Organizations often use Web content filters to block users from visiting unwanted sites that have no business purpose, on the presumption that doing so will reduce wasted time at work.

Chapter Summary

- Telecommunications networks include many types of wired and wireless network technologies. The wired technologies include DS-1 (T-1), SONET, Frame Relay, ATM, DSL, and MPLS. Wireless technologies include CDMA2000 (which includes 1xRTT and EVDO), GPRS, EDGE, UMTS, and WiMAX.

- Organizations build wired and wireless networks using a variety of technologies. The dominant wired technology is Ethernet, although ATM, Token Ring, and other technologies still have limited use. USB and RS-232 are used for limited and/or short distance applications. Wireless technologies include Wi-Fi and Bluetooth; IrDA, which is based on infrared light, is declining in use.
- Ethernet is a frame-based network standard in which nodes on a network transmit data in a *frame* that includes source and destination information, plus a *payload*. Ethernet has error correction capabilities that enable re-transmission of frames when errors occur.
- Stations in an Ethernet network are addressed with a MAC (media access control) address that consists of six 8-bit octets. MAC addresses are unique in the world, to avoid the possibility that two devices with the same MAC address could ever be on the same network.
- Ethernet devices consist of hubs, switches, repeaters, routers, and gateways.
- Network cabling is typically one of three types: coaxial, twisted pair, and fiber optic. Fiber optic is the cable of choice for longer distances and the highest speed connections, while twisted pair is prevalent in office environments.
- The three network topologies are bus, ring, and star. Ethernet networks are a physical star, but a logical bus.
- Wi-Fi wireless networks can be made more secure by turning off SSID broadcast, changing to a non-default SSID, utilizing WPA or WPA2 encryption, using user-based authentication, and MAC-based access control. The WEP encryption standard has been compromised and is considered unsafe.
- Bluetooth and Wireless USB are two other wireless technologies used to create personal area networks (PANs). Near field communications (NFC) is a short range network technology.
- The OSI network model is a seven layer model whose layers are: physical, data link, network, transport, session, presentation, and application. The TCP/IP network model is a four-layer model consisting of: link, internet, transport, and application layers.
- The physical layer in the TCP/IP network model consists of the various cabling and wireless media such as twisted pair cable, coaxial cable, fiber optic cable, Wi-Fi, USB, and Bluetooth.
- The link layer in the TCP/IP network model includes various framing protocols such as Ethernet, Token Ring, ATM, Frame Relay, and PPP.
- The internet layer in the TCP/IP network model contains the lowest level protocols including IPv4, IPv6, ARP, RARP, ICMP, IGMP, and IPsec. Most TCP/IP routing protocols operate in the network layer and include: RIP, OSPF, IS-IS, and BGP.
- Node addressing in the TCP/IP internet layer in IPv4 uses 32-bit addresses expressed in a dotted decimal notation xx.xx.xx.xx. Networks are divided into subnets and are notated with a subnet mask that divides a node address into a network portion (the most significant bits) and a node portion (the least significant bits). The subnet mask indicates which bits belong to each portion. Standard subnet masks are established for Class A networks (which can contain 16,777,214 nodes), Class B networks (which can contain 65,534 nodes), and Class C networks (which can contain 255 nodes).

Classless Inter-Domain Routing (CIDR) does away with Class A, Class B, and Class C networks and introduces flexible subnet masking for more efficient allocation of addresses in networks.

- IP addresses are allocated by Regional Internet Registries and Internet Service Providers. Blocks of reserved private addresses are used for organizations' internal nodes, and Network Address Translation (NAT) is used to dynamically allocate addresses and ports for nodes with private addresses that communicate directly with nodes on the Internet.
- The transport layer in the TCP/IP network model includes the two primary transport protocols: TCP and UDP. The TCP protocol is connection-oriented and guarantees delivery of packets, flow control, and order of delivery, whereas the UDP protocol is connectionless and does not guarantee packet delivery or flow control.
- The application layer in the TCP/IP network model includes the protocols that communicate directly with computer applications and tools. Some of the protocols found in the application layer include DHCP, DNS, FTP, HTTP, LDAP, NTP, RPC, SIP, SMTP, SNMP, TELNET, TFTP, and VoIP.
- Tunneling protocols are used to encapsulate TCP/IP packets. The reasons for tunneling include confidentiality (the payload in tunneling protocols can be encrypted) and authentication. Common tunneling protocols in use include SSL, SSH, IPsec, L2TP, PPTP, and PPP. These protocols support the creation of Virtual Private Networks (VPNs) that are often used to facilitate remote access to a private network.
- Authentication protocols are used to authenticate users who wish to use network or computing resources. Common authentication protocols in use include RADIUS, Diameter, CHAP, EAP, and PEAP. The older protocols TACACS and PAP are not often used.
- Common network-based attacks include Denial of Service (DoS), Distributed Denial of Service (DDoS), Teardrop, Sequence number, Smurf, Ping of Death, SYN flood, worms, spam, and phishing.
- Common network-based vulnerabilities include unneeded open ports, unpatched systems and devices, and misconfigured systems and devices.
- Effective countermeasures against attacks and vulnerabilities include access control lists (ACLs), firewalls, intrusion detection systems, intrusion prevention systems, private addressing, closing unnecessary ports and services, installing security patches, and using gateways. UTM devices that perform many defensive functions are gaining use.

Key Terms

10BASE Any of a group of twisted pair or coaxial network cabling types used to carry network traffic up to 10Mbit/s. Types include 10BASE-T, 10BASE2, and 10BASE5.

100BASE Any of a group of twisted pair network cabling types used to carry network traffic up to 100Mbit/s, including 100BASE-TX.

1000BASE-T A twisted pair network cabling type used to carry network traffic up to 1Gbit/s.

802.1a/b/g/n See *IEEE 802.1a/b/g/n*.

802.1X See *IEEE 802.1X*.

Access Control List (ACL) A method for filtering network packets on a router.

Access point A device used to connect multiple computers together to form a wireless network.

Address Resolution Protocol (ARP) A TCP/IP protocol that is used to translate a network IP address into a network MAC address.

Anycast A type of IP network communications where a packet is sent to only one of a group of available nodes.

Application layer Layer 7 of the OSI network model (and layer 4 of the TCP/IP network model) that provides communications to end user processes and programs.

Asynchronous Transfer Mode (ATM) A packet-switching network protocol that uses a fixed-size packet called a cell to transport data.

Attack An action taken against a target resource with the intention of doing harm.

Bluetooth A wireless network technology for low-speed and low-power data communication over short distances.

Border Gateway Protocol (BGP) A TCP/IP routing protocol primarily used by the Internet's backbone routers.

Broadcast A type of network communications where packets are sent to all nodes in a network.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) A data link layer protocol type where notes verify the absence of traffic on the network before transmitting data. Nodes are able to detect collisions and back off before retransmitting.

Category 3/5/5e/6/7 Standards for twisted-pair network cabling that support bandwidths from 10Mbit/s to 10Gbit/sec.

CDMA2000 A mobile radio technology used to transmit voice and data between subscriber devices and base stations for voice and data communication.

Challenge-Handshake Authentication Protocol (CHAP) A network-based authentication protocol used to authenticate a user to a system or network resource. CHAP is used to authenticate a PPP connection.

Checksum A method used to ensure the integrity of a packet or frame.

Coaxial cable A type of cable that consists of a single or dual inner conductor, a dielectric insulator, a metallic shield, and an outer plastic jacket.

Data link layer Layer 2 of the OSI network model that consists of protocols for transmitting frames over a network medium.

Data Over Cable Service Interface Specification (DOCSIS) The standard for delivery of Internet connectivity over television broadcast cable networks.

Digital Subscriber Line (DSL) A group of telecommunications technologies used to deliver digital data services (such as Internet connectivity) over telephone wires.

Digital Subscriber Line Access Multiplexer (DSLAM) A multiplexer node on a DSL service provider network that connects individual DSL subscribers to data networks such as the Internet.

Domain Name Service (DNS) A TCP/IP layer 4 protocol used to translate (via lookup) host and domain names into IP addresses.

DS-0 A single 64kbit/s voice or data channel on a DS-1 circuit.

DS-1 The base North American telecommunications carrier protocol used to carry up to 24 64 kbit/s voice or data channels.

Dynamic Host Configuration Protocol (DHCP) A TCP/IP layer 4 protocol used to assign IP addresses and other configuration settings to nodes on a network.

E1 The base European telecommunications carrier protocol used to carry up to 32 64 kbit/s voice or data channels. See also *DS-1*.

Enhanced Data rates for GSM Evolution (EDGE) A wireless telecommunications standard that is a successor to GPRS that provides bandwidth up to 1 Mbit/s.

Enhanced GPRS (EGPRS) A wireless telecommunications standard that is a successor to GPRS that provides bandwidth up to 1 Mbit/s.

Enhanced Interior Gateway Routing Protocol (EIGRP) A Cisco proprietary routing protocol that is an enhancement of its earlier IGRP protocol. See also *IGRP*.

Ethernet A family of frame-based wired network technologies used to connect computers in a local area network (LAN).

Extensible Authentication Protocol (EAP) An authentication framework of protocols used to authenticate users to system or network resources. Several variants exist, including EAP-PSK, EAP-IKEv2, EAP-AKA, and EAP-SIM.

Fiber Distributed Data Interface (FDDI) A token network technology transmitted over fiber optic cable.

Fibre Channel A gigabit network protocol usually used in storage area networks (SANs), and transported over fiber optic or copper cable.

File Transfer Protocol (FTP) A TCP/IP layer 4 protocol used to transfer files between computers.

Finger A TCP/IP layer 4 protocol used to make queries about users on network-attached computers.

Frame A data packet at the data link layer in a network.

Frame Relay An early packet switched telecommunications network technology used to connect together entities for data communications.

FTPS File transfer protocol (FTP) protected with SSL.

Gateway A device or system on a network that translates various types of network communications.

General Packet Radio Service (GPRS) The data-centric mobile radio technology used in GSM (Global System for Mobile Communications) network.

Global System for Mobile Communications (GSM) One of the prevalent standards for wireless mobile voice and data telecommunications.

Header The portion of a network frame or packet that includes information such as the source address, destination address, and type of message.

High Speed Serial Interface (HSSI) A high-speed serial communications protocol, usually used to connect nearby WAN devices together.

Host-based Intrusion Detection System (HIDS) An Intrusion Detection System (IDS) that is a part of a host computer. See also *Intrusion Detection System*.

Host-based Intrusion Prevention System (HIPS) An Intrusion Prevention System (IDS) that is a part of a host computer. See also *Intrusion Prevention System*.

Hypertext Transfer Protocol (HTTP) A TCP/IP layer 4 protocol used to transmit HTML and XML content from World Wide Web servers to client browsers.

Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) A TCP/IP layer 4 protocol used to transmit HTML and XML content from World Wide Web servers to client browsers that is protected with SSL/TLS encryption.

IEEE 802.1a/b/g/n A family of wireless network standards. See also *Wi-Fi*.

IEEE 802.1X A network-based device authentication protocol that is based on EAP.

Infrared Data Association (IrDA) The governing body that has developed a number of line-of-sight optical protocols known as *IrDA*. Largely superseded by Bluetooth.

Integrated Services Digital Network (ISDN) A digital voice and data telecommunications service over copper wires.

Interframe gap A pause between transmitted frames on an Ethernet network.

Interior Gateway Routing Protocol (IGRP) A Cisco proprietary TCP/IP routing protocol that utilizes bandwidth, delay, load, MTU, and reliability metrics for determining the best path between endpoints.

Intermediate System to Intermediate System (IS-IS) A TCP/IP routing protocol used by ISPs and other network service providers.

Internet layer Another name for layer 3 of the OSI network model.

Internet The global network of interconnected TCP/IP networks.

Internet Control Message Protocol (ICMP) A TCP/IP protocol used primarily for error messages and utility functions such as PING and TRACEROUTE.

Internet Group Management Protocol (IGMP) A TCP/IP protocol used to manage multicast groups. Analogous to ICMP.

Intrusion Detection System (IDS) A program or device that generates alerts when unwanted network traffic is detected. See also *Intrusion Prevention System*.

Intrusion Prevention System (IPS) A program or device that blocks unwanted traffic when it is detected. See also *Intrusion Detection System*.

IPv4 (Internet Protocol version 4) The original Internet Protocol (IP) that is layer 3 in the TCP/IP network model.

IPv6 (Internet Protocol version 6) The extended Internet Protocol, layer 3 in the TCP/IP network model that included extended addressing and security features.

Layer 2 Tunneling Protocol (L2TP) A TCP/IP layer 2 tunneling protocol used to encapsulate network traffic.

Lightweight Directory Access Protocol (LDAP) A TCP/IP layer 4 protocol used to query and modify directory services. LDAP is often used for authentication.

Link layer Layer 1 in the TCP/IP network model.

Local Area Network (LAN) A computer network covering a small geographic area such as a residence, building, or group of buildings.

Media Access Control (MAC) layer A sublayer of the data link layer that provides channel access on a network.

Media Access Control (MAC) address A notation for uniquely identifying nodes on a network, usually expressed as six octets.

Metropolitan Area Network (MAN) A computer network covering a geographic area the size of a city or region.

Multicast A method for efficiently transmitting network packets to groups of destination nodes. See also *unicast*.

Multiprotocol Label Switching (MPLS) A packet switched telecommunications network technology used to transport voice and data.

Near Field Communication (NFC) A short-range (10cm) network technology generally used by mobile phones and other hand-held devices for mobile payment and other applications.

Network A computer network covering any size geographic area from a few inches to International. See also *PAN*, *LAN*, *MAN*, and *WAN*.

Network layer Layer 3 of the OSI network model that consists of low level protocols used to transport data from computer to computer.

Network-based Intrusion Detection System (NIDS) An Intrusion Detection System (IDS) that is connected to a network. See also *Intrusion Detection System*.

Network-based Intrusion Prevention System (NIPS) An Intrusion Prevention System (IDS) that is connected to a network. See also *Intrusion Prevention System*.

Network File Service (NFS) A TCP/IP layer 4 protocol that is used to share file systems over a network.

Network Information Service (NIS) A TCP/IP layer 4 protocol that is used to centralize authentication and system configuration information for computers on a network.

Network Time Protocol (NTP) A TCP/IP layer 4 protocol that is used to synchronize the time clocks on computers.

Open Shortest Path First (OSPF) A TCP/IP routing protocol used in large enterprise networks.

Open Systems Interconnect (OSI) The seven layer network model whose layers are: Physical, Data link, Network, Transport, Session, Presentation, and Application.

Optical fiber A cable type used to carry high-speed communications signals in the form of light over a glass-like fiber.

Organizationally Unique Identifier (OUI) The first three octets of a MAC address that is assigned to an equipment manufacturer, in order to guarantee uniqueness of MAC addresses.

Packet filter A router with an Access Control List (ACL) or an early generation firewall. See also *Access Control List*, *Firewall*.

Password Authentication Protocol (PAP) An authentication protocol used by PPP to authenticate users. PAP is unsafe because login credentials are not encrypted.

Payload The data that is contained in a network packet or frame.

Personal Area Network (PAN) A computer network that spans a distance close to one person.

Physical layer Layer 1 of the OSI and TCP/IP network models that consists of a network's physical medium.

PING A tool used to send an ICMP Echo Request to a specific node on a network.

Ping of Death (PoD) An attack where an attacker sends PING packets of length 65,535 bytes to the target system in hopes that the target system will crash.

Point to Point Protocol (PPP) A TCP/IP layer 2 protocol that is usually used for dial-up Internet access.

Point to Point Tunneling Protocol (PPTP) An early TCP/IP tunneling protocol that has been largely replaced by L2TP and IPsec.

Port number A numbering scheme in which messages of various types are distinguished.

Presentation layer Layer 6 of the OSI network model that provides various methods for presenting data, for instance in different character sets or encryption algorithms.

Protected Extensible Authentication Protocol (Protected EAP or PEAP) A wireless network protocol used to authenticate users.

Public Switched Telephone Network (PSTN) The well known public telephone network. Also known as *POTS* (plain old telephone service).

Remote Authentication Dial In User Service (RADIUS) An authentication protocol used to authenticate a user, control access rights through authorization, and provide accounting (usage) information for billing.

Remote login (Rlogin) A TCP/IP layer 4 network protocol that is used to log in to another computer over a network.

Remote Procedure Call (RPC) A TCP/IP layer 4 protocol used to permit a computer to execute a subroutine or procedure on another computer.

Remote Shell (Rsh) A TCP/IP layer 4 protocol used to execute commands on other computers on a network.

Repeater A network device used to receive and re-transmit a network signal, usually to extend the physical length of a network connection.

Reverse Address Resolution Protocol (RARP) A TCP/IP protocol that is used to translate a known MAC address into an IP address. Superseded by DHCP.

Ring A network topology where each node is connected to exactly two other nodes in a circular pathway.

Routing Information Protocol (RIP) An early TCP/IP routing protocol that uses hop count as the primary metric for determining the lowest cost of a route between endpoints.

RS-232 A serial communications technology used to connect computers to low speed peripherals such as mice, printers, modems, and terminals. Superseded by USB.

RS-449 A serial communications standard that is similar to RS-232 and with a maximum bandwidth of 2Mbit/s.

Secure Shell (SSH) A TCP/IP layer 4 tunneling protocol used for secure remote management of systems. Supersedes Rsh, Rcp, Rlogin, and Telnet.

Secure Sockets Layer (SSL) A TCP/IP layer 4 tunneling protocol used to protect network traffic through encryption. Superseded by TLS. See also *TLS*.

Sequence number attack An attack in which an attacker injects packets with guessed sequence numbers that pretend to originate from one of the two computers in the session.

Serial Line Interface Protocol (SLIP) An early implementation for transporting TCP/IP over serial connections.

Service set identifier (SSID) A name that is used to identify a specific Wi-Fi wireless network.

Session layer Layer 5 of the OSI network model that controls connections between computers.

Session Initiation Protocol (SIP) A TCP/IP layer 4 protocol that is used to establish and tear down voice and video communications sessions.

Simple Mail Transport Protocol (SMTP) A TCP/IP layer 4 protocol used to transmit e-mail messages from one e-mail server to another.

Simple Network Management Protocol (SNMP) A TCP/IP layer 4 protocol used to remotely monitor and manage network devices and systems over a network.

Smurf An attack that consists of a large number of forged ICMP echo requests, which are sent to a network's broadcast address with a forged *source* address. Systems that receive the attack packets send large numbers of *reply* packets to the target.

Star A network topology where all nodes are connected to a central device such as a hub or switch.

Subnet A range of network addresses in a network.

Subnet mask A numeric value, expressed in the same manner as an IP address, that is used to determine the network and host portions of an IP address.

SYN flood A Denial of Service (DoS) attack where the attacker sends large numbers of TCP SYN packets to the target system, hoping to overwhelm it and exhaust its resources.

Synchronous optical networking (SONET) The standard in North America for transporting voice and data over optical fiber.

Synchronous Digital Hierarchy (SDH) The prevalent standard for voice and data communications over fiber networks outside of North America. See also *SONET*.

T1 See *DS-1*.

Teardrop An attack in which an attacker sends mangled packet fragments with overlapping and oversized payloads to a target system in an attempt to crash the target system.

TELNET A TCP/IP layer 4 protocol that is used to establish a raw TCP session over a network to a service on another computer.

Token ring A network technology consisting of a logical ring and the passing of a logical 'token' from node to node over the network. Only a node in possession of a token may transmit data.

TRACEROUTE A tool used to determine the network path to a specific destination.

Transmission Control Protocol (TCP) A connection-oriented TCP/IP transport protocol used to carry messages within a session between two nodes. TCP guarantees delivery, order of delivery, and flow control.

Transport layer Layer 4 of the OSI model and layer 3 in the TCP/IP network model that provides reliable data transfer.

Trivial File Transfer Protocol (TFTP) A TCP/IP layer 4 protocol used to transfer files over a network.

Tunnel Any of several network protocols that use packet encapsulation to deliver packets to an endpoint.

Twisted pair A type of cable that utilizes pairs of twisted copper conductors.

Unicast A type of network communications where packets are sent to a single node. See also *multicast*.

Unified Threat Management (UTM) A security device or appliance that performs many security functions such as firewall, IDS, IPS, anti-virus, anti-spam, or Web content filtering.

Universal Mobile Telecommunications System (UMTS) A wireless telecommunications protocol for data communications.

Unsolicited Commercial E-mail (UCE) See *spam*.

User Datagram Protocol (UDP) A connectionless TCP/IP transport protocol used to carry messages within a session between two nodes. UDP does not guarantee delivery, order of delivery, or flow control.

Voice over Internet Protocol (VoIP) A TCP/IP layer 4 protocol used to transport voice traffic over a network.

Whois A TCP/IP layer 4 protocol that is used to query a whois server, usually to determine the owner of a domain name or IP address.

Wide Area Network (WAN) A computer network covering large geographic areas spanning metropolitan, regional, national, or international.

Wireless USB (WUSB) A wireless protocol designed for wireless connectivity of various computer peripherals such as printers, digital cameras, hard disks, and other high-throughput devices.

Wireline Any of the telecommunications services that is transported over copper or optical fiber.

Worldwide Interoperability for Microwave Access (WiMAX) A wireless telecommunications standard for fixed-base and mobile voice and data communications.

X.25 A packet-switched telecommunications network.

X11 The GUI based window system that is used in UNIX and Linux operating systems.

xDSL See *Digital Subscriber Line* (*DSL*).

Review Questions

1. The capacity of a DS-1 circuit is:
   a. 24 voice channels of 64 kbit/s each
   b. 32 voice channels of 64 kbit/s each

c. 24 voice channels of 48 kbit/s each

d. 16 data channels of 64 kbit/s each

2. Which of the following statements is true about MPLS:

a. MPLS can be used to transport voice and data, and its traffic should be protected with encryption.

b. MPLS can be used to transport voice and data, and its traffic does not need to be protected with encryption.

c. MPLS is used for data only, and its traffic should be protected with encryption.

d. MPLS is used for voice only, and its traffic should be protected with encryption.

3. A network architect is designing a remote access solution for mobile workers with laptops and will use GPRS technology for over-the-air communications. Because workers access sensitive information, what protection is required to protect GPRS traffic?

a. GPRS's over-the-air encryption is sufficient and no VPN is needed.

b. GPRS's over-the-air encryption has been compromised and a VPN is needed.

c. GPRS has no over-the-air encryption and a VPN is needed.

d. GPRS is not suitable for Internet communications and should not be used.

4. A security manager is concerned about the security of its WEP-encrypted Wi-Fi network. How can security be improved to prevent eavesdroppers from viewing sensitive business information:

a. Require VPN for all users using the Wi-Fi network

b. Require SSL VPN for all users using the Wi-Fi network

c. Upgrade authentication to EAP

d. Upgrade authentication to PEAP

5. What protection is needed for a banking organization's internal 802.3 network:

a. WEP

b. WPA

c. WPA-2

d. None

6. A security engineer is using a sniffer to determine the source of apparently-hostile traffic on an organization's internal routed network. When the engineer examines individual frames, he sees that the source MAC address for the hostile packets matches the MAC address for the router on the local network. What is the best explanation for this:

a. The packets are encapsulated in a tunneling protocol such as PPTP.

b. The packets have a spoofed originating MAC address in order to make identification of the hostile node more difficult.

c. Frames carrying IP traffic originating on another network will have a MAC address for the local network's router.

d. The packets are IPX protocol, not IP.

7. What steps should be taken to lock down a Wi-Fi network:
   a. No SSID broadcast, non-default SSID, MAC access control, and WEP encryption
   b. No SSID broadcast, non-default SSID, MAC access control, and WPA-PSK encryption
   c. SSID broadcast, non-default SSID, MAC access control, and WPA-PSK encryption
   d. SSID broadcast, non-default SSID, MAC access control, WEP encryption, and RADIUS authentication
8. The layers in the OSI model are:
   a. Physical, Data link, Network/Internet, Transport, Session, Application
   b. Physical, Data link, Network, Transport, Socket, Presentation, Application
   c. Physical, Data link, Network/Internet, Transport, Application
   d. Physical, Data link, Network, Transport, Session, Presentation, Application
9. GPRS, ATM, FDDI, and SLIP are examples of:
   a. Data link layer protocols
   b. Physical layer protocols
   c. Network layer protocols
   d. Encryption protocols
10. A packet filter firewall is blocking ICMP protocols. This means that:
   a. Pings cannot pass through the firewall
   b. Pings and Traceroute cannot pass through the firewall
   c. Traceroute cannot pass through the firewall
   d. IS-IS cannot pass through the firewall
11. A requesting station sends a TCP SYN to a destination station. The destination station responds with a SYN-ACK. The requesting station responds with an ACK. What has occurred?
   a. An attacker was launching a SYN attack that has failed.
   b. A user is running Traceroute.
   c. A TCP connection was established.
   d. A TCP connection was torn down.
12. The purpose of the DHCP protocol is:
   a. Assign IP address and subnet mask to a station
   b. Assign default gateway address to a station
   c. All of these
   d. Assign DNS and WINS server addresses to a station
13. The rlogin protocol should no longer be used because:
   a. SSH is more efficient
   b. Its password encryption has been compromised

c. It cannot be routed on an IPv6 network
d. Credentials are passed in the clear

14. PPP is a poor choice for an Internet-based remote access protocol because:
    a. It does not utilize header compression
    b. PPP traffic is not encrypted
    c. PPP credentials are not encrypted
    d. It is not routable over IPv6 networks
15. The best countermeasure for a SYN attack is:
    a. Block SYN packets on border routers
    b. Block SYN packets at the firewall
    c. Increase the number of open SYN requests on the firewall
    d. Increase the number of open SYN requests on servers

Hands-On Projects

Project 10-1: Classful Subnet Mask Calculator

In this project you will calculate and observe subnet masks required for Class A, B, and C networks.

Visit the web site www.subnet-calculator.com.

1. Click **C** under **Network Class**. Observe the default values shown for the IP address 192.168.0.1 with subnet mask 255.255.255.0. Refer to Figure 10-12.
2. How many subnet bits are there? How many mask bits are there? How many subnets are available? How many hosts can be on each subnet?
3. Change the subnet mask to 255.255.255.224. Now how many subnet mask bits are there? How many mask bits? How many subnets are available, and how many hosts can be on each subnet?
4. Change the subnet mask to 255.255.255.252. How many subnets are available? How many hosts can be on each subnet? Why is the total number of hosts available on all subnets fewer than the number of hosts when the subnet mask is 255.255.255.0?
5. Keep your web browser open if you will be doing Project 10-2.

Project 10-2: Classless Subnet Mask Calculator

In this project you will calculate and observe subnet masks required for networks with Classless Inter-Domain Routing (CIDR).

1. Visit the web site www.subnet-calculator.com.
2. Click the **CIDR** link.
3. In the **IP address field**, enter the IP address 10.0.0.1.

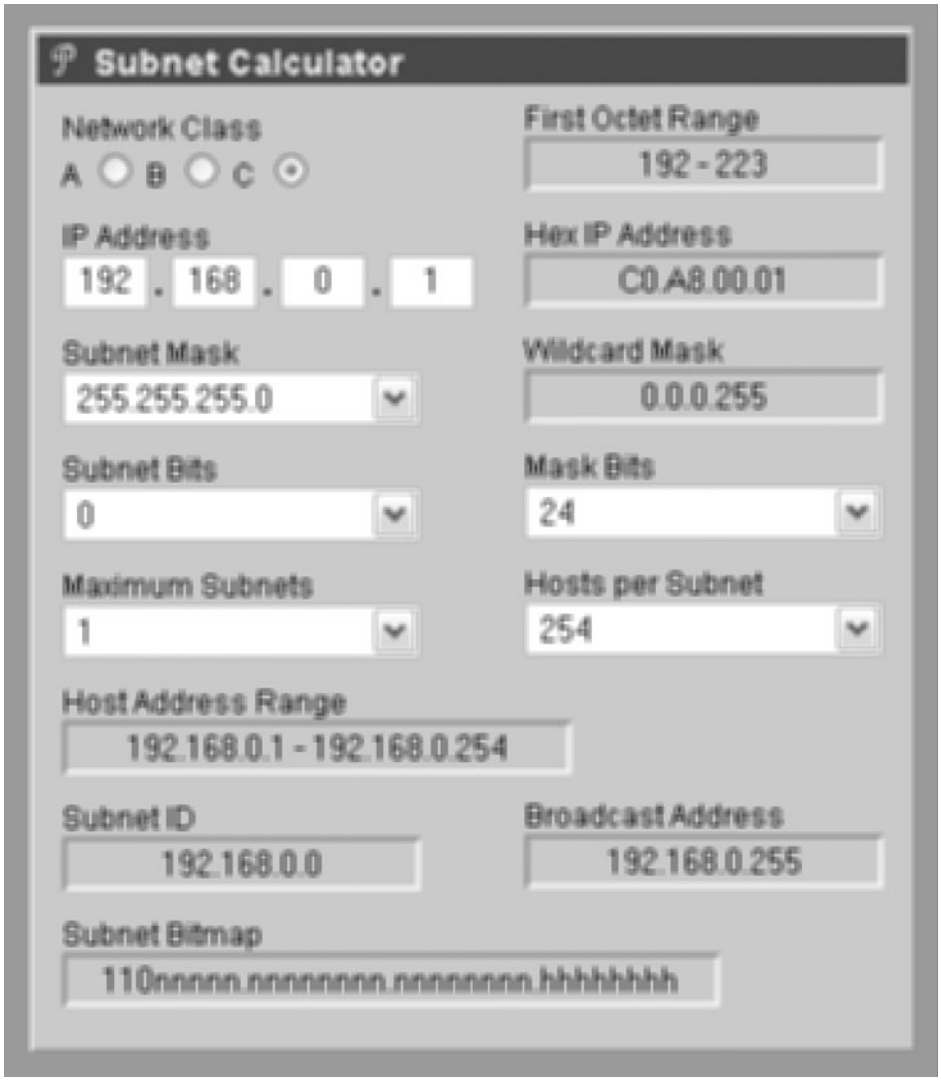


Figure 10-12 Classful subnet calculator

Source: Course Technology/Cengage Learning

4. Select **CIDR Netmask 255.0.0.0**. Refer to Figure 10-13.
5. Observe the values shown. How many mask bits are there? How does relate to the CIDR Notation? What is the range of IP addresses?
6. Change the IP address to 192.168.0.0, and the subnet mask to 255.255.254.0. What is the range of available IP addresses? Why is this called a "supernet"?

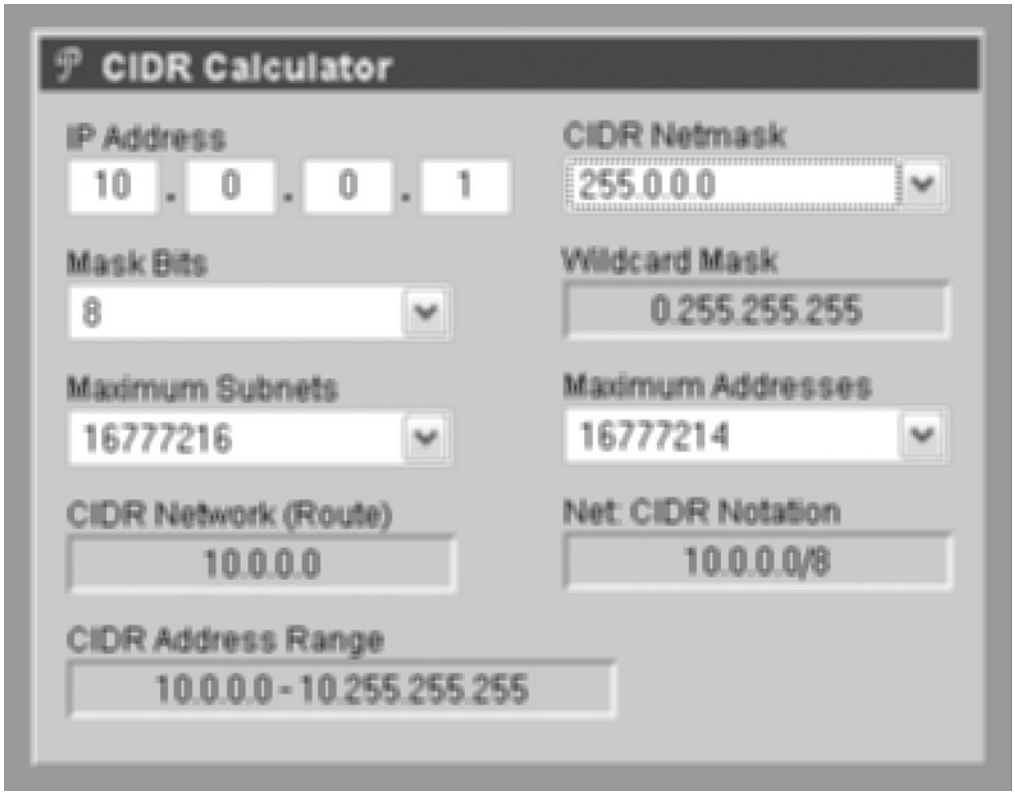


Figure 10-13 CIDR subnet calculator

Source: Course Technology/Cengage Learning

Project 10-3: Network Sniffer

In this project you will capture network traffic with a sniffer.

In order to avoid any potential problems, you should first ask for permission to perform this project. You should not run a sniffer on a network unless you have explicit permission.

1. Download Wireshark from www.wireshark.com.
2. Install Wireshark using procedures available on the Wireshark web site.
3. Start Wireshark.
4. Ensure that Wireshark is going to capture packets on the correct interface. Select **Capture > Options**, and see what interface is selected. Select the proper interface from the drop-down menu. Make sure **Capture packets in promiscuous mode** and **Update list of packets in real time** are selected. Refer to Figure 10-14.

Figure 10-14 Selecting packet capture options in Wireshark

Source: Course Technology/Cengage Learning

5. Begin capturing web traffic for your own workstation. Click **Start**.
6. After some packets have been captured, slick **Capture > Stop**.
7. Click on a packet in Wireshark's upper window. What does Wireshark show you about the packet in the lower window? Examine the detail in each section (for example: Frame, Ethernet II, Internet Protocol, Transmission Control Protocol, Hypertext Transfer Protocol). What can you learn about the packet(s) that you are examining?

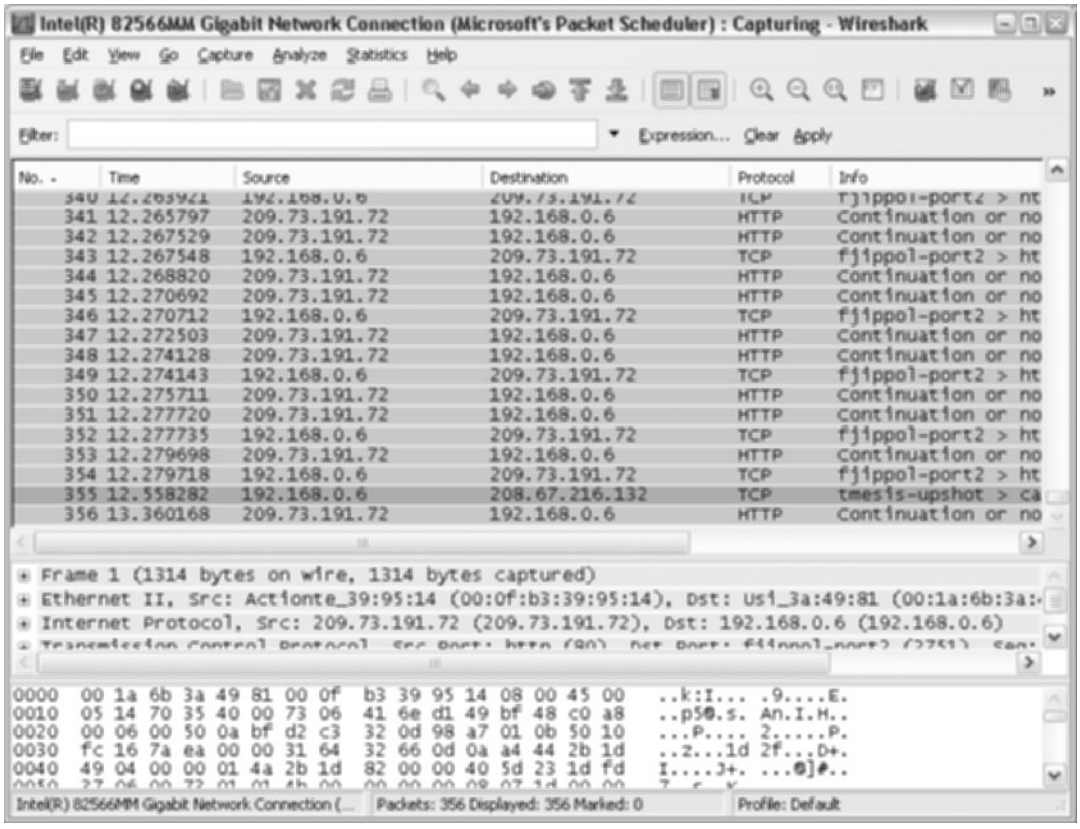


Figure 10-15 Examining captured packets with Wireshark

Source: Course Technology/Cengage Learning

Project 10-4: Port Scanner

In this project you will perform simple port scanning to discover open ports on nearby network systems.

Note: Port scanning may be considered a security violation in the work or school network. You must obtain permission from the network manager before downloading and using such a tool.

1. Download the SuperScan tool from www.foundstone.com. Click on **Tools**, scroll and look for **SuperScan**, then download it.
2. Start the tool. Refer to Figure 10-16.

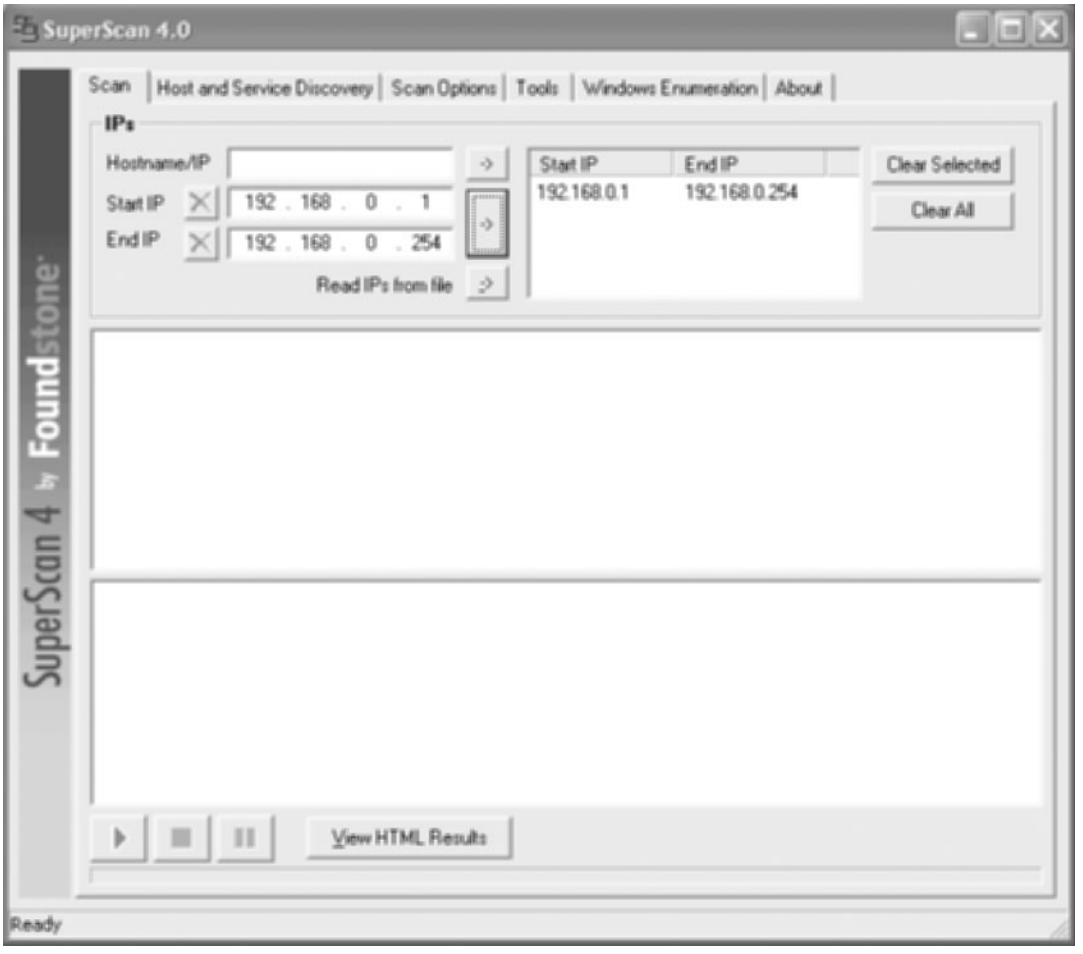


Figure 10-16 Scanning for network vulnerabilities with SuperScan

Source: Course Technology/Cengage Learning

3. Click the **Scan** tab. Input a range of IP addresses to scan, then click the blue **Start** button at the bottom of the window.
4. SuperScan will then scan the network and identify active hosts and security information about each. Click **View HTML Results** to see a detailed report.
5. What did SuperScan tell you about the network you scanned? Did it find any vulnerable computers?

If SuperScan identified any vulnerabilities in any of the systems that it scanned, you should notify the system owner as soon as possible.

Project 10-5: Wireless Network Scanner

In this project you will perform wireless network scanning to discover nearby wireless networks.

Note: Wireless network scanning may be considered a security violation in the work or school network. You must obtain permission from the network manager before downloading and using such a tool.

1. Download the Netstumbler tool from www.netstumbler.com.
2. Install the Netstumbler tool.
3. Start the tool. If there are Wi-Fi access points nearby, Netstumbler should soon discover them and list them on the screen. Refer to Figure 10-17.

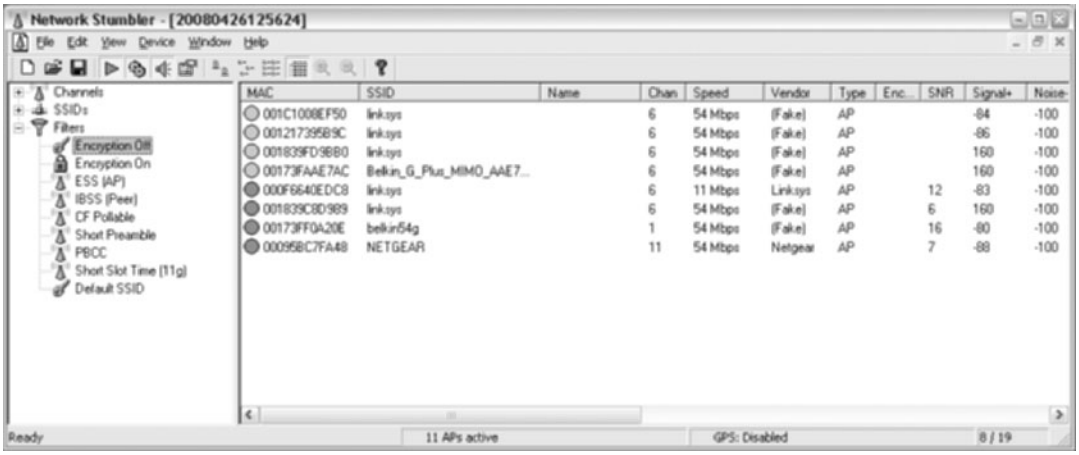


Figure 10-17 Scanning for wireless networks with Netstumbler

Source: Course Technology/Cengage Learning

4. In the left-hand pane, click the + next to **Filters**. Click on **Encryption Off**. Are any access points listed in the right pane? Click on **Filters**.
5. In the left-hand pane, click the + next to **Filters**. Click on **Default SSID**. Are any access points listed in the right pane?
6. What have you learned about nearby access points?
7. Are you able to discern the owners of any access points based upon their SSID?

Even if you find open (unencrypted) access points, you should not attempt to connect to them without obtaining written permission from its owner. Doing so is a crime in many jurisdictions.

Case Projects

Case Project 10-1: Network Address Allocation

As a network engineer in the Have-A-Java Roasting Company, you need to develop a plan to re-IP address the entire network.

The network consists of the following systems on the local network:

2 DNS servers
2 routers
1 firewall
1 VPN server
E-mail server
External web server
Internal file server
300 user workstations
6 printers

Your ISP has requested that you return the 2 Class C network addresses that it assigned to your company ten years ago. They will allocate to you 6 externally routable IP addresses for any external-facing systems.

How will you allocate the six IP addresses among the externally facing systems and devices that require Internet access?

How will user workstations be able to access web servers on the Internet?

Case Project 10-2: Wireless Network Survey

As a consultant with the Sleuth Security Consulting Co., you have been asked to perform a wireless access point survey at the Good Software Company offices. Good Software is concerned that there may be rogue (unauthorized) Wi-Fi access points in use in their company.

What tools will you use to look for rogue access points? Will you use a Wi-Fi sniffer such as Netstumbler? What are the pros and cons of using this tool? Will you perform any LAN searches for rogue access points?

Case Project 10-3: Network Evaluation

As a consulting network engineer for the Excellent Network Consulting Co., you have been requested to perform an evaluation of the data network at the Zoom Trucking Company, which has just moved in to an eighty-year-old office building.

Zoom Trucking's network engineer has not been able to get the network functioning on the network cable that was in the building when Zoom Trucking moved in. Part of the network uses coaxial thinnet cabling, and part of it uses Cat-3 network cabling. Less than half of the user workstations connected via Cat-3

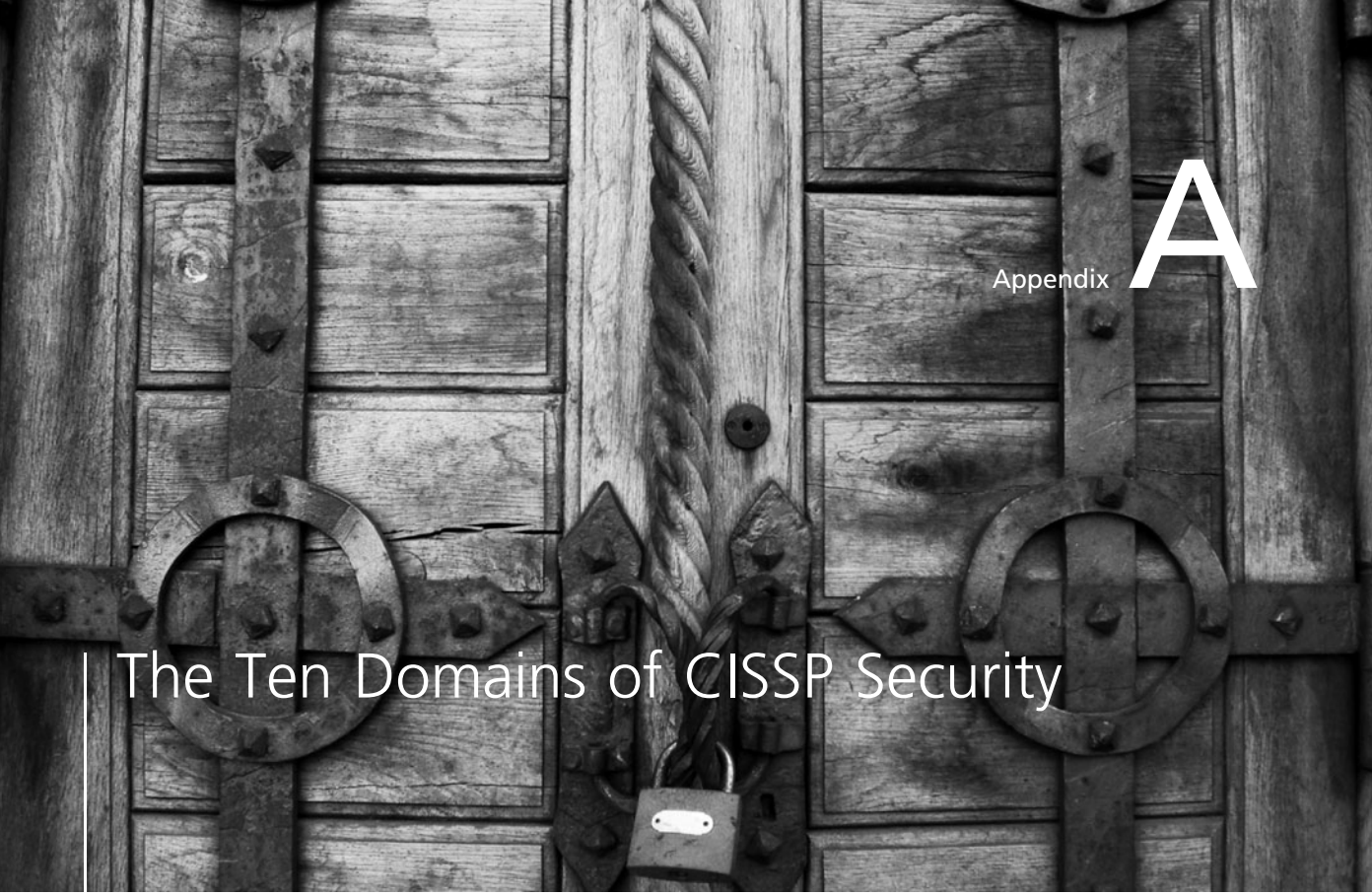
cabling are working, and none of the workstations connected to coaxial cable are working because none of the user workstations have the right connectors.

Some specifics about Zoom Trucking:

Employees with workstations: 75
Servers: 8 servers located in a server room
Building size: 2 floors, 100' x 200'
Construction: wood frame and masonry exterior

Your job is to create a list of recommendations to Zoom Trucking: what steps should it take to get its data network working as soon as possible?

This page intentionally left blank



Appendix A

The Ten Domains of CISSP Security

Topics in this Chapter:

- An introduction to the CISSP certification
- The ten domains of CISSP security

The **International Information Systems Security Certification Consortium**, or $(ISC)^2$ (pronounced "I-S-C-squared"), is the governing body and owner of the CISSP certification. **CISSP**, or **Certified Information Systems Security Professional**, is one of the highest rated professional certifications for information and business security. The reputation is due to several factors, including:

- Longevity. The CISSP certification was introduced in 1989, many years before information security was "cool." Computer, network, and physical security were well established in government and military establishments, and the Internet was just getting air under its wings.
- Industry acceptance. The CISSP certification is the first security credential accredited by the ANSI/ISO/IEC 17024:2003 standard in the field of information security. The U.S. DoD Directive 8570.1 requires its information security workers to obtain an ANSI-accredited commercial certification, such as CISSP.
- Wide recognition. CISSP is probably the most recognized security certification in all of the information technology profession. Having CISSP in one's title means that this is a security professional at the top of the security profession.
- High standards. The CISSP certification is considered the top-most certification in the information- and business-protection profession. It is difficult to earn the certification: the qualifying exam consists of six hours of mind-numbing multiple-choice questions that can trip up even the most senior professionals. The certification also requires that the candidate have five years of verifiable security experience, and a background free of association with hackers and convictions related to crimes of dishonesty.
- Remains current and relevant. $(ISC)^2$ actively offers educational opportunities for CISSP certification holders so that they can stay sharp and informed on the latest technologies, threats, and methods. The CISSP exam is continually updated to reflect the latest developments in security technology and techniques. New exam questions are written by experienced CISSPs in exam-writing workshops that occur several times each year.

The entire body of knowledge that comprises the CISSP certification is arranged in a living document called the **Common Body of Knowledge** (**CBK**). It has often been said that the CBK is overly broad, yet shallow, "a mile wide and an inch deep." I'm not sure that I agree with this metaphor. It is true that the CBK contains a great many topics, and that the scope of knowledge that a CISSP candidate is expected to know is constantly expanding. But the knowledge and experience required to earn the CISSP certification and be an effective security professional requires that your knowledge of security be a lot more than an inch deep.

This and every other book on the $(ISC)^2$ CISSP *Common Body of Knowledge* (CBK) should be considered a guide on the concepts that the reader should know, rather than a discrete list of topics and no more. The purpose of the CBK is to outline the technologies, practices, and laws that are related to the protection of an organization's information-related assets.

The ten domains in the CISSP CBK are:

- Domain 1: Access Controls
- Domain 2: Application Security
- Domain 3: Business Continuity and Disaster Recovery Planning

- Domain 4: Cryptography
- Domain 5: Information Security and Risk Management
- Domain 6: Legal, Regulations, Compliance, and Investigations
- Domain 7: Operations Security
- Domain 8: Physical (Environmental) Security
- Domain 9: Security Architecture and Design
- Domain 10: Telecommunications and Network Security

Each of these domains is described briefly in the remainder of this chapter, and more fully in individual chapters in this book.

Changes in the CBK

$(ISC)^2$ changes the structure of the CBK from time to time, as the state of the art of security technology and management continue to mature and change. Because publications are not immediately updated, you may even see inconsistencies between various $(ISC)^2$ publications. In a major restructuring of the CBK in 2006-2007, $(ISC)^2$ re-ordered the domains and changed the wording in many of them. In fact, this book's author found an inconsistency in the CBK in 2008 that resulted in a rather hasty update. Further changes to the CBK are likely in the future.

$(ISC)^2$ does not require CISSP candidates to know the names of the CBK domains or which specific security topics are contained in each part of the CBK.

The Common Body of Knowledge

The $(ISC)^2$ common body of knowledge contains ten domains, which are the major categories of business and data security. Activities in the ten domains work together to protect the confidentiality, integrity, and availability (CIA) of business information, information systems, and other important business assets.

The information in this section is a summary of the information published by $(ISC)^2$ in the Candidate Information Bulletin, a guide for aspiring CISSP candidates who wish to earn the CISSP certification.

Domain 1: Access Controls

Access controls are used to control user access to computer systems, networks, and workspaces, as well as the functions they are permitted to perform. A variety of techniques and technologies are used to manage access in organizations; in larger organizations, there tends to be a greater use of automation to manage user access.

Access controls are found in many layers of technology including network, remote access, operating system, database, and application. At each layer, access controls may be administered by different teams using different tools.

Access controls are the means through which legitimate users gain access to a system or workspace, and are also frequently the target of many forms of attack by intruders. Security professionals must understand attack methods as well as techniques to ensure that access controls are not vulnerable to these attacks.

Domain 2: Application Security

Software applications are used to store and manage information in support of key business processes. While the majority of line-of-business applications* are acquired in the form of common off-the-shelf (COTS) or software-as-a-service (SaaS), most enterprises still perform software development in the form of customizations, integrations, applets, agents, and tools. Programmers, software developers, and software engineers need to know the principles of security in application design and coding.

Software applications need to have a sound design that includes any required application-level access and authorization management that cannot be circumvented. The database management systems and data warehouses that support applications must be properly configured and administered in order to reduce or eliminate security vulnerabilities that could otherwise threaten the confidentiality, integrity, and availability of data.

Discipline is required in the software development life cycle (SDLC) to ensure that software applications are properly developed to meet the needs of the business and not contain flaws that could result in malfunctions or security issues.

Beyond the SDLC, an organization must have sound practices such as change management, configuration management, and vulnerability management, to ensure that software vulnerabilities cannot be introduced into an application environment.

Domain 3: Business Continuity and Disaster Recovery Planning

Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) are two closely related activities that are concerned with the survival of the organization in the face of man-made and natural disasters.

The ability for an organization to survive a disaster requires the development of contingency plans that are activated when a disaster occurs. These plans are periodically tested to ensure that they will successfully support critical business processes in a disaster.

In order to allocate resources properly, a Business Impact Analysis is performed that identifies which business processes are most critical; it is for these processes that most contingency plans are developed.

Business continuity and disaster recovery planning also involve the identification of measures that can be taken to reduce the impact of a disaster or prevent its effect altogether.

BCP and DRP are a part of the CBK because these activities help to assure the availability of business information and information systems, even in extreme circumstances such as man-made and natural disasters.

*Common enterprise applications include Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), Materials Resource Planning (MRP), Manufacturing Resource Planning (MRP II).

Domain 4: Cryptography

Cryptography is the science of hiding information that is in plain sight. A form of access control, cryptography is an effective means to prevent unauthorized parties from accessing sensitive or critical data that is protected by encryption.

Numerous encryption technologies are used to protect information. Data can be encrypted as it is transmitted from place to place, so that any eavesdroppers who are able to intercept the transmission will be unable to decipher the information. Data can also be encrypted when it is stored on a system, so that people who do (and don't) have access to the system but should not have access to the data are likewise unable to read it.

Hashing is a companion technology that can be used to verify the integrity and the source of a message or file. Hashing is the technology that creates digital signatures in e-mail messages. Hashing is also used as "one-way encryption" to protect information such as passwords.

Public key infrastructures (PKIs) are used as certification authorities (CAs) to store public encryption keys and digital certificates that can be used to verify messages and services.

Domain 5: Information Security and Risk Management

Security management is the management-level activity that creates security policy, establishes security governance, and aligns with and supports key business objectives. Risk management utilizes analysis methodologies that identify and quantify risks and propose risk treatments to reduce risks to acceptable levels.

Security managers must understand and utilize the concepts of defense in depth, avoidance of single paths of failure, and the pillars of security that are confidentiality, integrity, and availability. They must establish security requirements to ensure that systems and processes support security policy, awareness programs so that personnel are aware of security policies and procedures, and sound hiring practices to ensure that new staff are vetted and have verified professional backgrounds.

Security management is responsible for creating security standards, security architectures, document classification and handling guidelines, and ensuring that suppliers are properly vetted and will not introduce unwanted risks to the business. They must uphold the $(ISC)^2$ code of ethics and other codes of ethics in situations where good judgment is necessary.

Domain 6: Legal, Regulations, Compliance, and Investigations

For decades, information and business security was introduced primarily as a means of incident avoidance, but in recent years security has been codified in numerous international, national, and local jurisdictions and in many industries such as banking, health care, and energy. Many security standards have been developed, some of which carry the weight of law. Increasingly, businesses are shifting their security efforts from risk management to compliance management.

Security management is responsible for the development of incident handling procedures that must also comply with applicable regulations and also ensure the preservation of evidence for potential prosecution. Management must undertake efforts such as internal audit and testing to ensure continued compliance with policy and regulations.

Domain 7: Operations Security

Security operations are the day-to-day activities that provide continuous protection to an organization's information, information systems, and other assets. Many activities fall under the category of operations security including security monitoring, vulnerability management, change management, configuration management, and information handling procedures.

Many key security concepts are operational in nature including need-to-know, least privilege, separation of duties, and job rotation.

In the $(ISC)^2$ CBK, operations security also encompasses operational support of highly available systems, fault tolerance, and mitigation of security-related cyber attacks.

Domain 8: Physical (Environmental) Security

Physical and environmental security in the $(ISC)^2$ CBK includes the means for protecting assets from physical harm, which embodies the use of several types of physical controls to prevent unauthorized personnel from accessing valuable assets. These controls include surveillance, entry controls, guards, and perimeter controls such as security fencing and lighting.

This CBK domain also includes the development and management of a proper environment for information systems that includes suitable power management systems that may consist of uninterruptible power supplies, power conditioners, electric generators, and power distribution units. Information systems also require proper heating, cooling, and humidification controls, fire detection and suppression systems, and controls to avoid problems associated with water leaks and the presence of other unwanted substances.

This domain also includes techniques for choosing proper facilities for housing staff, information systems, and other assets, by identifying and understanding site-and location-related risks.

Domain 9: Security Architecture and Design

Security architecture and design is concerned with the abstract security models that are used to better understand both existing security structures as well as to assist in the design of new ones. Like any model, security models simplify protection concepts so that architects and designers can ascertain whether assets can be properly secured.

In addition to abstract models, security professionals are also expected to be intimately familiar with the inner workings of computer hardware and software. Like the other disciplines of security, the security professional can only protect something that he fully understands.

The security professional must understand threats and weaknesses such as covert channels, state attacks, emanations, as well as countermeasures to counteract them.

Domain 10: Telecommunications and Network Security

Like the preceding domain where the security professional is required to fully understand the inner workings of computer systems, this domain requires the security professional to fully understand computer networking and the telecommunications technologies that facilitate long-distance networking. Because most security-related threats, vulnerabilities, and attacks are network-related, this requires intimate knowledge of the workings of network protocols, network devices, network-based services, and the way that computers communicate with each other using networks.

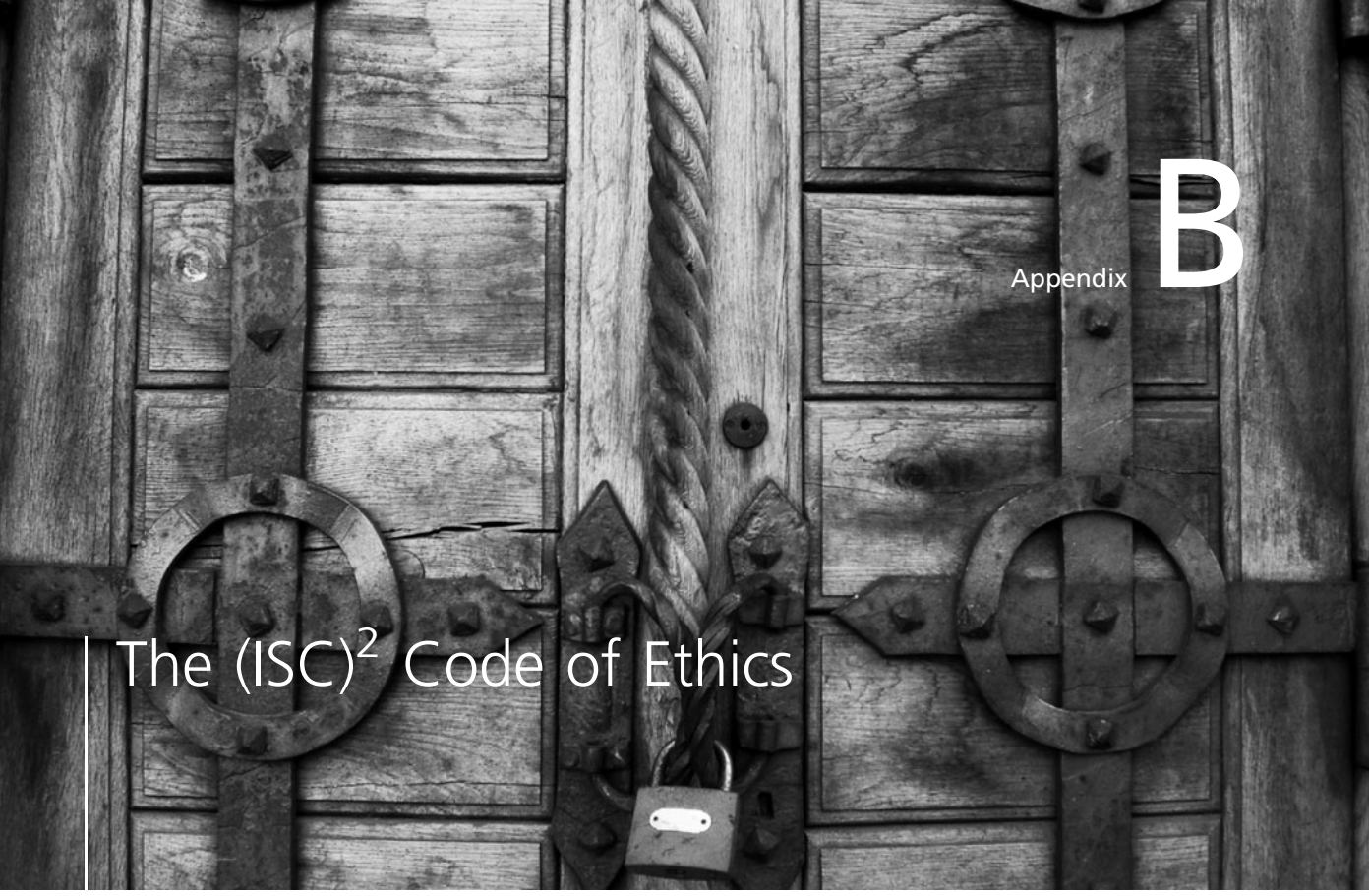
Almost without exception, to protect an organization requires protection of its networks. A security professional must understand how secure networks are designed, built, and verified to be secure.

Key Terms

Certified Information Systems Security Professional (CISSP) The highly esteemed data and business security certification that is the topic of this book.

Common Body of Knowledge (CBK) The entire collection of concepts, methodologies, and practices that a candidate for CISSP certification is required to understand.

International Information Systems Security Certification Consortium (ISC)^2 The organization that created and manages the CISSP and other security certifications.



Appendix B

The (ISC)^2 Code of Ethics

All information systems security professionals who are certified by (ISC)^2 recognize that such certification is a privilege that must be both earned and maintained. In support of this principle, all (ISC)^2 members are required to commit to fully support this Code of Ethics (the "Code"). (ISC)^2 members who intentionally or knowingly violate any provision of the Code will be subject to action by a peer review panel, which may result in the revocation of certification. There are only four mandatory canons in the code. By necessity, such high-level guidance is not intended to be a substitute for the ethical judgment of the professional.

Additional guidance is provided for each of the canons. While this guidance may be considered by the board of directors in judging behavior, it is advisory rather than mandatory. It is intended to help professionals identify and resolve the inevitable ethical dilemmas that they will confront during the course of their information security career.

Code of Ethics Preamble:

- Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.
- Therefore, strict adherence to this Code is a condition of certification.

Code of Ethics Canons:

- Protect society, the commonwealth, and the infrastructure.
- Act honorably, honestly, justly, responsibly, and legally.

- Provide diligent and competent service to principals.
- Advance and protect the profession.

The following additional guidance is given regarding pursuit of these goals.

Objectives for Guidance

In arriving at the following guidance, the committee is mindful of its responsibility to:

- Give guidance for resolving good-versus-good and bad-versus-baddilemmas.
- To encourage right behavior such as:
  - Research
  - Teaching
  - Identifying, mentoring, and sponsoring candidates for the profession
  - Valuing the certificate
- To discourage such behavior as:
  - Raising unnecessary alarm, fear, uncertainty, or doubt
  - Giving unwarranted comfort or reassurance
  - Consenting to bad practice
  - Attaching weak systems to the public network
  - Professional association with non-professionals
  - Professional recognition of or association with amateurs
  - Associating or appearing to associate with criminals or criminal behavior

These objectives are provided for information only; the professional is not required or expected to agree with them.

In resolving the choices that confront him or her, the professional should keep in mind that the following guidance is advisory only. Compliance with the guidance is neither necessary nor sufficient for ethical conduct.

Compliance with the preamble and canons is mandatory. Conflicts between the canons should be resolved in the order of the canons. The canons are not equal, and conflicts between them are not intended to create ethical binds.

Protect Society, the Commonwealth, and the Infrastructure

- Promote and preserve public trust and confidence in information and systems.
- Promote the understanding and acceptance of prudent information security measures.
- Preserve and strengthen the integrity of the public infrastructure.
- Discourage unsafe practice.

Act Honorably, Honestly, Justly, Responsibly, and Legally

- Tell the truth; make all stakeholders aware of your actions on a timely basis.
- Observe all contracts and agreements, express or implied.

- Treat all members fairly. In resolving conflicts, consider public safety and duties to principals, individuals, and the profession, in that order.
- Give prudent advice; avoid raising unnecessary alarm or giving unwarranted comfort. Take care to be truthful, objective, cautious, and within your competence.
- When resolving differing laws in different jurisdictions, give preference to the laws of the jurisdiction in which you render your service.

Provide Diligent and Competent Service to Principals

- Preserve the value of their systems, applications, and information.
- Respect their trust and the privileges that they grant you.
- Avoid conflicts of interest or the appearance thereof.
- Render only those services for which you are fully competent and qualified.

Advance and Protect the Profession

- Sponsor for professional advancement those best qualified. All other things equal, prefer those who are certified and who adhere to these canons. Avoid professional association with those whose practices or reputation might diminish the profession.
- Take care not to injure the reputation of other professionals through malice or indifference.
- Maintain your competence; keep your skills and knowledge current. Give generously of your time and knowledge in training others.

Glossary

10BASE any of a group of twisted pair or coaxial network cabling types used to carry network traffic up to 10Mbit/s. Types include 10BASE-T, 10BASE2, and 10BASE5.

100BASE any of a group of twisted pair network cabling types used to carry network traffic up to 100Mbit/s, including 100BASE-TX.

1000BASET a twisted pair network cabling type used to carry network traffic up to 1Gbit/s.

802.1a/b/g/n *See* IEEE 802.1a/b/g/n.

802.1X *See* IEEE 802.1X.

Access Control List (ACL) a method for filtering network packets on a router.

Access controls any means used to control which subjects are permitted to access objects.

Access log a record that contains building or computer access attempts.

Access management the policies, procedures, and controls that determine how information is accessed and by whom.

Access Matrix a security model that consists of a two-dimensional matrix of subjects, objects, and the permissions for each subject's access to each object.

Access point a device used to connect multiple computers together to form a wireless network.

Accreditation the process of formally approving the use of a system.

Active Directory a Microsoft implementation of LDAP.

Active-Active an operating mode in a cluster where all of the servers in the cluster actively operate and process incoming requests.

Active-Passive an operating mode in a cluster where one or more servers actively operate and process incoming requests and one or more servers remain in a standby mode.

Address Resolution Protocol (ARP) a TCP/IP protocol that is used to translate a network IP address into a network MAC address.

Administrative controls the policies, procedures, and standards put in place in an organization to govern the actions of people and information systems.

Administrative law the branch of law in the U.S. that defines the rules and regulations that govern activities in executive departments and agencies in the U.S. government.

Advanced Encryption Standard (AES) the encryption standard established in 2001 by the U.S. government. AES uses the Rijndael algorithm.

Adware cookies, web beacons, and other means used to track individual Internet users and build behavior profiles for them.

Agent small, standalone programs that perform some task for a larger application environment.

Alarm system a system of sensors and a control unit that is designed to detect intrusions into a building or room and send an alarm signal if an intrusion is detected.

Annual loss expectancy (ALE) the yearly estimate of loss of an asset, calculated as: ALE = ARO × SLE.

Annualized rate of occurrence (ARO) the probability that a loss will occur in a year's time.

Anti-rookit software uses techniques to find hidden processes, hidden registry entries, unexpected kernel hooks, and hidden files in order to find rookits that may be present on a system.

Anti-spyware software that is designed to detect and remove spyware.

Anti-virus software software that is used to detect and remove viruses and other malicious code from a system.

Anycast a type of IP network communications where a packet is sent to only one of a group of available nodes.

Applet a small program that runs within the context of another program.

Application a collection of programs and tools that fulfill a specific business purpose.

Application firewall a firewall that examines the contents of incoming messages in order to detect and block attempted attacks on an application.

Application layer layer 7 of the OSI network model (and layer 5 of the TCP/IP network model) that provides communications to end user processes and programs.

Application scanning the task of identifying security vulnerabilities in an application.

Application vulnerability scanning a means of testing an application to identify any vulnerabilities.

Arithmetic Logic Unit (ALU) the portion of a CPU where arithmetic and logic operations are performed.

Asset an object of value to the organization. An asset may be a physical object such as a computer or it can be information.

Asymmetric cryptography a class of cryptographic algorithms that utilize public-private encryption keys.

Asymmetric multiprocessing (ASMP) a multi-CPU computer architecture consisting of master and slave CPUs or some other asymmetric arrangement.

Asynchronous Transfer Mode (ATM) a packet switching network protocol that uses a fixed-size packet called a cell to transport data.

Attack an action taken against a target resource with the intention of doing harm.

Audit log the record of events that occur in an application environment.

Audit log analysis An activity used to detect unwanted events that are recorded in an audit log.

Authentication the act of proving one's identity to an information system by providing two or more pieces of information, such as a userid and a password, in order to gain access to information and functions.

Authorization the process of permitting a user to perform some specific function or access some specific data.

Availability the concept that asserts that information systems can be accessed and used when needed.

Back door a feature in a program that allows access that bypasses security.

Background verification the process of verifying an employment candidate's employment, education, criminal, and credit history.

Backup the process of copying important information from a computer or storage system to another device for recovery or archival purposes.

Bell LaPadula a security model that addresses the confidentiality of information.

Biba a security model that addresses data integrity.

Biometrics a means for measuring a physiological characteristic of a person as a means for positively identifying him or her.

Birthday attack a cryptanalysis attack against a message digest.

Blackmail *see* Extortion

Block cipher an encryption algorithm that operates on fixed blocks of data.

Bluetooth a wireless network technology for low-speed and low-power data communication over short distances.

Bollard a heavy upright post used to restrict vehicle traffic.

Border Gateway Protocol (BGP) a TCP/IP routing protocol primarily used by the Internet's backbone routers.

Bot malicious software that allows someone to remotely control someone else's computer for illicit purposes.

Botnet a collection of software robots (or "bots") under centralized control that run autonomously and automatically.

Broadcast a type of network communications where packets are sent to all nodes in a network.

Buffer overflow an attack on a system by means of providing excessive amounts of data in an input field.

Bus a hardware subsystem used to transfer data among a computer's internal components including its CPU, storage, network, and peripherals.

Business attack an attack that targets a computer or network owned by a business, for the purpose of gaining intelligence, financial gain, or denial of service.

Business continuity plan a contingency plan that governs the business response to a disaster in order to keep critical business functions operating.

Business Continuity Planning (BCP) the activities required to ensure the continuation of critical business processes in an organization.

Business Impact Analysis (BIA) the task of identifying the business impact that results from the interruption of a specific business process.

Bypass an attack that attempts to bypass security controls to access or alter information.

Card reader a device used to read the contents of a key card.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) a data link layer protocol type where notes verify the absence of traffic on the network before transmitting data. Nodes are able to detect collisions and back off before retransmitting.

Category 3/5/5e/6/7 standards for twisted-pair network cabling that support bandwidths from 10Mbit/s to 10Gbit/sec.

CDMA2000 a mobile radio technology used to transmit voice and data between subscriber devices and base stations for voice and data communication.

Central processing unit (CPU) the portion of a computer where program instructions are executed.

Certificate Authority (CA) an entity that issues digital certificates.

Certification the process of evaluating a system against a specific criteria or specification.

Certified Information Systems Security Professional (CISSP) The highly esteemed data and business security certification that is the topic of this book.

C.F.R. *see* U.S. Code of Federal Regulations

Chain of custody the procedures and paper trail that tracks forensic evidence in a legal investigation.

Challenge-Handshake Authentication Protocol (CHAP) a network based authentication protocol used to authenticate a user to a system or network resource. CHAP is used to authenticate a PPP connection.

Change management the management process where proposed changes in an environment are formally planned and reviewed prior to implementing them.

Checksum a method used to ensure the integrity of a packet or frame.

Chosen ciphertext attack (CCA) a cryptanalysis attack where the attacker has chosen ciphertexts decrypted and obtain cleartext results.

Chosen plaintext attack (CPA) a cryptanalysis attack where the attacker is able to have chosen plaintexts encrypted and obtain the ciphertext results.

CIA Confidentiality, Integrity, and Availability.

Cipher feedback (CFB) a block cipher mode where the result of encrypting a block of plaintext is used to encrypt the next block.

Cipher-block chaining (CBC) a block cipher mode where ciphertext output from each encrypted plaintext block is used in the encryption of the next block.

Ciphertext the result of applying an encryption algorithm to plaintext.

Ciphertext-only attack (COA) a cryptanalysis attack where the attacker has only ciphertext.

Civil law the branch of laws that deal with disputes between individuals and/or organizations.

Clark-Wilson a security model that addresses data integrity that is a rebuttal to the Bell LaPadula and Biba models.

Class the defining characteristics of an object.

Classification *See* Data Classification.

Client-server application an application in which user interface logic resides on a client system and data storage and retrieval logic resides on a server.

Closed Circuit Television (CCTV) A standard for the transmission of video signals over a cable, often used in video surveillance systems. *See also* IP camera.

Cluster a group of two or more servers that operate functionally as a single logical server, and will continue operating as a single logical server in the event that one of the servers fails.

Coaxial cable a type of cable that consists of a single or dual inner conductor, a dielectric insulator, a metallic shield, and an outer plastic jacket.

Code of conduct a policy statement published by an organization that defines permitted and forbidden activities.

Code of ethics a code of responsibility statement that is used in an organization to define specific permitted and forbidden activities.

Collision an occurrence where two different messages are found to compute to the same hash value.

Common Body of Knowledge (CBK) The entire collection of concepts, methodologies, and practices that a candidate for CISSP certification is required to understand.

Common Criteria the current framework for evaluating the security of a system.

Compartmented security mode one of the security modes of operation where users can access some data based upon their need to know and formal access approval.

Compensating control a control that compensates for the absence or ineffectiveness of another control.

Competitive intelligence activities regarding the acquisition of information and secrets about a competing organization's products, services, financials, and other business activities.

Complex Instruction Set Computer (CISC) a microprocessor architecture in which each instruction can execute several operations in a single instruction cycle.

Compromising Emanations (CE) emanations of electromagnetic radiation (EMR) that disclose sensitive information.

Confidentiality the concept of information and functions being protected from unauthorized access and disclosure.

Configuration management the process of recording configuration changes that are made in an environment.

Configuration management database (CMDB) a database containing all of the changes made to a system or environment.

Control an activity, process, or apparatus that ensures the confidentiality, integrity, or availability of an asset.

Control flow a computer language methodology where instructions are followed sequentially until a "goto" type statement is encountered, in which case the control is transferred to the location specified by the goto statement.

Control Objectives for Information and related Technology (COBIT) a controls framework for the management of information technology and security.

Cookie a mechanism used to store identifying information, such as a session ID, on a web client system.

Copyright the legal right to exclusive use that is given to the creator of an original work of writing, music, pictures, and films.

Corrective control an activity that occurs after a security event has occurred in order to prevent its reoccurrence.

Counter (CTR) a block cipher mode that uses a one-time random number and a sequential counter.

Countermeasure a control or means to reduce the impact of a threat or the probability of its occurrence.

Covert channel an unauthorized channel of communications that exists within a legitimate communications channel.

COSO (Committee of Sponsoring Organizations of the Treadway Comission) a controls framework for the management of information systems and corporate financial reporting.

Crash gate a movable device that can be used to restrict the entry or exit of a vehicle.

Criminal law the branch of law that enforces public order against crimes such as assault, arson, theft, burglary, deception, obstruction of justice, bribery, and perjury.

Criticality Analysis the process of ranking business processes according to their criticality to the organization.

Crossover Error Rate (CER) the point where False Reject Rate and False Accept Rate are equal.

Cross-site request forgery (XSRF) this is an attack where malicious HTML is inserted into a Web page or e-mail that, when clicked, causes an action to occur on an unrelated site where the user may have an active session.

Cross-site scripting (XSS) an attack where an attacker can inject a malicious script into HTML content in order to steal session cookies and other sensitive information.

Cryptanalysis the process of attacking a cryptosystem in order to discover its method of operation and/or its encryption and decryption keys.

Cryptography the science of hiding information, usually through the use of algorithms based upon mathematical operations.

Cutover test a test of a disaster recovery or business continuity plan in which backup or recovery systems or processes are operated in place of normal business operations.

Cyberterrorism acts of violence against civilians and governments that are carried out in cyberspace.

Data classification the process of assigning sensitivity levels to documents and data files in order to assure their safekeeping and proper handling.

Data confidentiality model a security model whose chief concern is the confidentiality of data.

Data destruction the process of discarding information that is no longer needed, in a manner that will render it irretrievable.

Data integrity model a security model whose chief concern is data integrity.

Data link layer layer 2 of the OSI network model that consists of protocols for transmitting frames over a network medium.

Data Over Cable Service Interface Specification (DOCSIS) the standard for delivery of Internet connectivity over television broadcast cable networks.

Data remanence the unintentional data that remains on a storage device or medium.

Data replication see replication.

Data warehouse a database management system that is designed and built to store archival data for decision support and research purposes.

Database an ordered collection of data that exists for a common purpose.

Database management system (DBMS) a system used to manage one or more databases.

Debriefing a meeting or conference during which the details of an incident are discussed, in order to learn from the incident and the organization's response to it.

Decipher another word for decrypt.

Decryption the process of turning ciphertext back into original plaintext.

Dedicated security mode one of the security modes of operation where all users can access all data.

Defense in depth a strategy for protecting assets that relies upon several layers of protection. If one layer fails, other layers will still provide some protection.

Degaussing the process of bulk-erasing magnetic-based storage media by imposing a strong magnetic field onto the media.

Demilitarized zone (DMZ) a means of protecting application servers and the remainder of an enterprise network by placing them on a separate firewalled network.

Denial of service (DoS) attack an attack against a computer or network that is designed to incapacitate the target.

Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) the process used to certify and accredit information systems used by the U.S. military.

Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) the process used to certify and accredit information systems used by the U.S. military; superseded by DIACAP.

Destruction the process of discarding information in a way that renders it non-retrievable.

Detective control a control that is used to detect specific types of activity.

Deterrent control a control used to deter unwanted activity.

Device driver a program that permits the operating system and other programs to communicate with a specific hardware device or type of device.

Diameter an authentication, authorization, and accounting protocol that is a replacement for RADIUS.

Diffie-Hellman (D-H) key exchange a secure mechanism for two parties with no prior knowledge of each other to jointly establish a shared symmetric encryption key.

Digital certificate an electronic document that utilizes a digital signature and an identity, used to reliably identify a person or system.

Digital Encryption Algorithm (DEA) the data encryption algorithm chosen in 1976 as the new Digital Encryption Standard (DES).

Digital Encryption Standard (DES) the data encryption standard established in 1976 by the U.S. government. DES uses the Digital Encryption Algorithm (DEA) algorithm.

Digital signature the result of cryptographic functions used to verify the integrity and authenticity of a message.

Digital Subscriber Line (DSL) a group of telecommunications technologies used to deliver digital data services (such as Internet connectivity) over telephone wires.

Digital Subscriber Line Access Multiplexer (DSLAM) a multiplexer node on a DSL service provider network that connects individual DSL subscribers to data networks such as the Internet.

Director of Central intelligence Directive 6/3 (DCID 6/3) the process for protecting sensitive compartmented information within information systems at the U.S. Central Intelligence Agency (CIA).

Disaster any event that that disrupts the operations of a business in such a significant way that a considerable and coordinated effort is required to achieve a recovery.

Disaster Recovery Planning (DRP) the activities concerned with the assessment, salvage, repair, and restoration of damaged facilities and assets.

Discretionary access control (DAC) an access control model where the owner of an object may grant access rights to subjects based upon the owner's discretion.

Distributed application an application in which its components reside on many systems.

Distributed database a database that is logically or physically distributed among several systems.

Distributed Denial of Service (DDoS) a Denial of Service attack that originates from many systems. *See also* Denial of Service.

Diverse network routing a network design strategy where two or more separate circuits to a given location will be located in different areas. If a mishap severs one of the circuits, communication will continue via the other circuit(s).

Document review a review of a business continuity or disaster recovery procedure in which a single individual reviews procedures.

Documentation processes, procedures, and even records, whether in paper or electronic form.

Domain Name Service (DNS) a TCP/IP layer 4 protocol used to translate (via lookup) host and domain names into IP addresses.

DS-0 a single 64kbit/s voice or data channel on a DS-1 circuit.

DS-1 the base North American telecommunications carrier protocol used to carry up to 24 64 kbit/s voice or data channels.

Dumpster diving an attack where an attacker rummages through refuse bins ("dumpsters") in an attempt to discover sensitive discarded information.

Dynamic Host Configuration Protocol (DHCP) a TCP/IP layer 4 protocol used to assign IP addresses and other configuration settings to nodes on a network.

Dynamic Random Access Memory (DRAM) a random access memory (RAM) technology used in computer main storage.

E1 the base European telecommunications carrier protocol used to carry up to 32 64 kbit/s voice or data channels. *See also* DS-1.

Eavesdropping an attack where an attacker attempts to intercept communications.

EEPROM (Electrically Erasable Programmable Read Only Memory) a form of erasable semiconductor memory used to store firmware.

Electric generator *See* generator.

Electronic codebook (ECB) a block cipher mode wherein each plaintext block is encrypted separately.

Elevation of privileges an attack where an attacker is able to perform some manipulation in order to raise his privileges, enabling him to perform unauthorized functions.

Emanations typically RF emissions from a computer or conductor that permits eavesdroppers to eavesdrop on computer activity.

Embezzlement the act of dishonestly or illegally appropriating wealth from another party, often an employer or service provider.

Employee handbook a formal document that defines terms and conditions of employment.

Employment agreement a legal agreement that specifies terms and conditions of employment for an individual employee or group of employees.

Encapsulation a design attribute that permits the hiding of internal details about an object in an OO system.

Encipher another word for encrypt.

Encryption a means of transforming plaintext info ciphertext to make it unreadable except by parties who possess a key.

Enhanced Data rates for GSM Evolution (EDGE) a wireless telecommunications standard that is a successor to GPRS that provides bandwidth up to 1 Mbit/s.

Enhanced GPRS (EGPRS) a wireless telecommunications standard that is a successor to GPRS that provides bandwidth up to 1 Mbit/s.

Enhanced Interior Gateway Routing Protocol (EIGRP) a Cisco proprietary routing protocol that is an enhancement of its earlier IGRP protocol. *See also* IGRP.

EPROM (Erasable Programmable Read Only Memory) a form of erasable semiconductor memory used to store firmware.

Espionage the process of obtaining secret or confidential information without the permission of the holder of the information.

Ethernet a family of frame-based wired network technologies used to connect computers in a local area network (LAN).

Ethics the discipline of dealing with a code of professional behavior.

Evaluation Assurance Level (EAL) the seven levels of evaluation in the Common Criteria.

Expert system a software system that accumulates knowledge on a particular subject and is able to predict outcomes based upon historical knowledge.

Explicitly Parallel Instruction Computing (EPIC) a microprocessor design that permits parallel execution in a single CPU.

Exposure factor (EF) the proportion of an asset's value that is likely to be lost through the realization of a particular threat.

Extensible Authentication Protocol (EAP) an authentication framework of protocols used to authenticate users to system or network resources. Several variants exist, including EAP-PSK, EAP-IKEv2, EAP-AKA, and EAP-SIM.

Extortion the act of obtaining money or other valuables from a person or organization through coercion, intimidation, or threat.

Facilities the buildings and other structures that house the space where people work and the equipment that they use.

Fail closed the characteristic of a security control – upon failure, it will deny all access.

Fail open the characteristic of a security control – upon failure, it will permit all access.

Fail safe *See* Fail closed.

Fail soft the process of shutting down non-essential components on a system, thereby freeing up resources so that critical components can continue operating.

Failover an event in a server cluster where production workload is transferred from one server to another.

False Accept Rate (FAR) how often a biometric system accepts an invalid user.

False Reject Rate (FRR) how often a biometric system rejects valid users.

Fault tolerance the design of a device or system where failure-prone components are duplicated, so that the failure of one component will not result in the failure of the entire device or system.

Federal Information Security Management Act (FISMA) a U.S. law that requires the evaluation of all systems used by the U.S. federal government.

Fiber Distributed Data Interface (FDDI) a token network technology transmitted over fiber optic cable.

Fibre Channel a gigabit network protocol usually used in storage area networks (SANs), and transported over fiber optic or copper cable.

File system a logical collection of files that resides on a storage medium.

File Transfer Protocol (FTP) a TCP/IP layer 4 protocol used to transfer files between computers.

Financial attack an attack against a computer or network that is intended to provide financial gain for the attacker.

Finger a TCP/IP layer 4 protocol used to make queries about users on network-attached computers.

Fire alarm an alarm system that warns human occupants of the presence of a nearby fire.

Fire extinguisher a portable fire suppression device that sprays liquid or foam onto a fire.

Firewall a hardware device or software program that controls the passage of traffic at a network boundary according to a predefined set of rules.

FireWire *See* IEEE1394.

Firmware computer instructions that are stored on a non-volatile memory device such as a PROM or EPROM.

Flash memory a form of erasable semiconductor memory used to store firmware.

Forensics the application of scientific knowledge to solve legal problems, especially the analysis of evidence from a crime scene.

Frame a data packet at the data link layer in a network.

Frame Relay an early packet switched telecommunications network technology used to connect together entities for data communications.

Fraud an act of deception made for personal gain.

Frequency analysis a cryptanalysis attack where the frequency of occurrence of the characters in ciphertext are examined.

FTP (File Transfer Protocol) a protocol used to transfer files from one system to another.

FTPS File transfer protocol (FTP) protected with SSL

Fun attack an attack against a computer or network that is usually performed for the thrill alone.

Gaseous fire suppression an installed system of pipes and nozzles that sprays a fire-retardant gaseous substance into a room.

Gateway a device or system on a network that translates various types of network communications.

General Packet Radio Service (GPRS) the data-centric mobile radio technology used in GSM (Global System for Mobile Communications) network.

Generator a device consisting of an internal combustion engine and an electric generator.

Geographic cluster a cluster whose members are dispersed over a wide geographic area.

Global System for Mobile Communications (GSM) one of the prevalent standards for wireless mobile voice and data telecommunications.

Governance the entire scope of activities related to the management of policies, procedures, and standards.

GPG (Gnu Privacy Guard) an open source software program that implements the PGP (Pretty Good Privacy) encryption standard.

Grudge attack an attack against a computer or network that is carried out as an act of revenge against its owner.

Guard *See* Security guard.

Guard dog a dog that is employed to guard against or detect unwanted or unexpected personnel.

Guideline information that describes how a policy may be implemented.

Hardening the process of configuring a system to make it more robust and resistant to attack.

Hardware computers and ancillary equipment that support information processing and storage.

Hash a computational transformation that receives a variable sized data input and returns a unique fixed-length string. Hashing is considered irreversible – it is not possible to obtain an original plaintext from a known hash.

Header the portion of a network frame or packet that includes information such as the source address, destination address, and type of message.

Heap overflow an attack that attempts to corrupt a program's heap (the dynamically allocated memory space created by a program for storage of variables).

Heating, ventilation, and air conditioning (HVAC) a system that is used to control the temperature and humidity in a building or a part of a building.

Hierarchical database a database model that is built on a tree structure.

High Speed Serial Interface (HSSI) a high speed serial communications protocol, usually used to connect nearby WAN devices together.

HMAC (Hashed Message Authentication Code) a message digest (hashing) algorithm.

Hook *See* maintenance hook.

Host based Intrusion Detection System (HIDS) an Intrusion Detection System (IDS) that is a part of a host computer. *See also* Intrusion Detection System.

Host based Intrusion Prevention System (HIPS) an Intrusion Prevention System (IDS) that is a part of a host computer. *See also* Intrusion Prevention System.

Hosts file a file on a workstation or server that associates host names and IP addresses.

Hub a device used to connect multiple computers together to form a network. A hub sends all packets on the network to all nodes. *See also* Switch.

Humidity a measurement of the amount of water vapor in the air.

Hypertext Transfer Protocol (HTTP) a TCP/IP layer 4 protocol used to transmit HTML and XML content from World Wide Web servers to client browsers.

Hypertext Transfer Protocol over Secure Socket Layer (HTTPS) a TCP/IP layer 4 protocol used to transmit HTML and XML content from World Wide Web servers to client browsers that is protected with SSL/TLS encryption.

Identification the act of claiming identity to an information system.

Identity theft a crime that involves the illegal use of some other person's identity.

IEEE 802.1a/b/g/n a family of wireless network standards. *See also* Wi-Fi.

IEEE 802.1X a network based device authentication protocol that is based on EAP.

IEEE1394 an external bus architecture used to connect high speed external devices such as video cameras.

Incident an unexpected event that results in an interruption of normal operations. *See also* Security incident.

Information flow a security model that describes permitted and forbidden flows of information rather than access controls.

Information Technology Security Evaluation Criteria (ITSEC) the European framework for system security evaluation now superseded by the Common Criteria.

Information warfare the use of information or information systems in the pursuit of an advantage over an opponent.

International Information Systems Security Certification Consortium (ISC)^2 the organization that created and manages the CISSP and other security certifications.

Infrared Data Association (IrDA) the governing body that has developed a number of line-of-sight optical protocols known as IrDA. Largely superseded by Bluetooth.

Inheritance the characteristics of a subclass that inherits attributes from its parent class.

Initialization vector (IV) a random block of data that is used by some cryptographic functions.

Injection attack an attack on a system where some scripting or procedural language is inserted into a data stream with the intention that the scripting will be performed.

Input attack any attack on a system where specially coded data is provided in an input field with the intention of causing a malfunction or failure of the system.

Integrated Services Digital Network (ISDN) a digital voice and data telecommunications service over copper wires.

Integrity the concept of asserting that information may be changed only by authorized persons and means.

Intellectual property (IP) a product of creation such as information, architecture, invention, music, image, and design.

Intellectual property agreement a legal agreement between an employee and an organization that defines ownership of intellectual property (IP) that the employee may develop during employment.

Intellectual property law the branch of law that protects created works and includes such safeguards as copyrights, trademarks, service marks, and patents.

Interframe gap a pause between transmitted frame on an Ethernet network.

Interior Gateway Routing Protocol (IGRP) a Cisco proprietary TCP/IP routing protocol that utilizes bandwidth, delay, load, MTU, and reliability metrics for determining the best path between endpoints.

Intermediate system to intermediate system (IS-IS) a TCP/IP routing protocol used by ISPs and other network service providers.

Internal audit the activity of self evaluation of controls and policies to measure their effectiveness.

Internet the global network of interconnected TCP/IP networks.

Internet Control Message Protocol (ICMP) a TCP/IP protocol used primarily for error messages and utility functions such as PING and TRACEROUTE.

Internet Group Management Protocol (IGMP) a TCP/IP protocol used to manage multicast groups. Analogous to ICMP.

Internet layer layer 3 of the OSI and TCP/IP network models.

Intrusion Detection System (IDS) a program or device that generates alerts when unwanted network traffic is detected. *See also* Intrusion Prevention System.

Intrusion Prevention System (IPS) a program or device that blocks unwanted traffic when it is detected. *See also* Intrusion Detection System.

IP Camera A video surveillance camera that sends its video signal over a TCP/IP data network.

IPSec a tunneling protocol used to protect communications between two systems.

IPSec (IP security) a suite of protocols for securing IP communications with authentication and encryption.

IPv4 (Internet Protocol version 4) the original Internet Protocol (IP) that is layer 3 in the TCP/IP network model.

IPv6 (Internet Protocol version 6) the extended Internet Protocol, layer 3 in the TCP/IP network model that included extended addressing and security features.

ISO 15408 *See* Common Criteria.

ISO17799:2005 an international standard that defines a framework of controls for information security management.

IT service continuity the process of ensuring the continuity of IT-provided services and systems.

Job description a formal document that defines a particular job title, responsibilities, duties, and required experience.

Job rotation the practice of rotating personnel through a variety of roles in order to reduce the risk of unauthorized activities.

Jump-to-register a type of buffer overflow attack where a function's return pointer is overwritten, in order to alter the behavior of a program.

Kerberos an authentication service that utilizes a centralized authentication server.

Kernel the part of an operating system that actively manages processes and access to resources.

Key a block of information that is used in an encryption algorithm.

Key card a credit card-sized plastic card with a magnetic stripe or embedded electronic circuit encoded with data that uniquely identifies the cardholder, and generally used to access restricted areas in a facility.

Key logger a hardware or software component that records keystrokes on a computer.

Key management processes and procedures used to create, protect, and destroy encryption keys.

Knowledge based system a system that is used to make predictions or decisions based upon input data.

Known plaintext attack (KPA) a cryptanalysis attack where the attacker has samples of plaintext and corresponding ciphertext messages.

Labeling the process of affixing a sensitivity identifiers to a document or data file.

Layer 2 Tunneling Protocol (L2TP) a TCP/IP layer 2 tunneling protocol used to encapsulate network traffic.

Least privilege the access control principle that states that an individual should have only the accesses required to perform their official duties.

Lightweight Directory Access Protocol (LDAP) a TCP/IP layer 4 protocol used to query and modify directory services. LDAP is often used for authentication.

Line conditioner a device that filters or removes some of the undesirable anomalies in an incoming power feed.

Link layer layer 1 in the TCP/IP network model.

Local Area Network (LAN) a computer network covering a small geographic area such as a residence, building, or group of buildings.

Logic bomb computer code placed in a system that is intended to perform some harmful event when certain conditions are met – usually a specific day or time in the future.

Logical controls *See* technical controls.

Main storage the primary, but usually volatile, high-speed storage used by a computer.

Maintenance hook a feature in a program that permits easy maintenance or access to information that bypasses security controls.

Malicious code computer instructions that are intended to disrupt or control a target system.

Malware *See* Malicious code.

Man in the middle attack (MITM) a cryptanalysis attack in which the attacker is able to read, insert, and modify messages passing between two parties' without their knowledge.

Mandatory access control (MAC) an access control model where subjects are permitted to access objects based upon specific security policies.

Man-made disaster a disaster caused by people or organizations.

Mantrap a set of interconnected double doors used to control the entrance or exit of personnel.

Marking *See* Labeling.

Master boot record (MBR) a place on a mass storage device (such as a hard drive) that contains computer instructions that can be read into memory when a computer is powered up or restarted.

Maximum Tolerable Downtime (MTD) the period of time after which the organization would suffer considerable pain were the process unavailable for that period of time.

MD5 a message digest (hashing) algorithm.

Media Access Control (MAC) address a notation for uniquely identifying nodes on a network, usually expressed as six octets.

Media Access Control (MAC) layer a sublayer of the data link layer that provides channel access on a network.

Memory *See* Main storage.

Memory interface the portion of a CPU that facilitates access to the computer's main memory.

Message digest a fixed length block of data that is the result of a hash function. *See also* Hash.

Method a function or calculation that an object is capable of performing.

Metropolitan Area Network (MAN) a computer network covering a geographic area the size of a city or region.

Microchannel an internal bus architecture used by IBM in PS/2 systems as a replacement for the slower ISA bus.

Military attack (in the context of information security) an attack against a computer or network used by a military organization.

MIME Object Security Services (MOSS) a protocol that provides confidentiality, authentication, and non-repudiation

Mobile code computer code that is downloaded or transferred from one system for execution on another system.

Monoalphabetic cipher a cipher in which plaintext characters are substituted for ciphertext characters according to a single alphabetic table.

Multicast a method for efficiently transmitting network packets to groups of destination nodes. *See also* unicast.

Multi-Level a security model consisting of several clearance levels for subjects and objects.

Multilevel security mode one of the security modes of operation where users can access data based upon their need to know, formal access approval, and security clearance.

Multiprotocol Label Switching (MPLS) a packet switched telecommunications network technology used to transport voice and data.

National Information Assurance Certification and Accreditation Process (NIACAP) the process used to certify and accredit systems that handle U.S. national security information.

Natural disaster a disaster caused by a natural event such as an earthquake or flood.

Near Field Communication (NFC) a short-range (10cm) network technology generally used by mobile phones and other hand-held devices for mobile payment and other applications.

Need-to-know the access control concept where individual personnel should have access to only the information that they require in order to perform their stated duties.

Network a computer network covering any size geographic area from a few inches to International. *See also* PAN, LAN, MAN, and WAN.

Network based Intrusion Detection System (NIDS) an Intrusion Detection System (IDS) that is connected to a network. *See also* Intrusion Detection System.

Network based Intrusion Prevention System (NIPS) an Intrusion Prevention System (IDS) that is connected to a network. *See also* Intrusion Prevention System.

Network database a database model based upon the hierarchical model, but with the ability for records to be related to other records in the database.

Network File Service (NFS) a TCP/IP layer 4 protocol that is used to share file systems over a network.

Network Information Service (NIS) a TCP/IP layer 4 protocol that is used to centralize authentication and system configuration information for computers on a network.

Network interface card (NIC) a computer hardware component that connects the computer's bus to a communication channel or network.

Network layer layer 3 of the OSI network model that consists of low level protocols used to transport data from computer to computer.

Network Time Protocol (NTP) a TCP/IP layer 4 protocol that is used to synchronize the time clocks on computers.

Neural network a software system that simulates the human reasoning process and is able to make predictions and decisions based on prior results.

Non-compete agreement a legal agreement that stipulates terms and conditions regarding whether the employee may accept employment with a competing organization in the future.

Non-disclosure agreement (NDA) a legal agreement that requires one or both parties to maintain confidentiality.

Non-interference an abstract security model that states that subjects with low clearance levels cannot learn anything about information at higher clearance levels on account of activities performed by subjects at higher clearance levels.

Non-repudiation the concept of ensuring that a person cannot later deny having performed some action.

NOP sled a type of stack overflow attack where the attacker floods the stack with NOP (no-operation) instructions in an attempt to take control of the program.

Object an instance of an OO class.

Object orientation (OO) a methodology for organizing information and software programs that supports objects, methods, and object reuse.

Object oriented database (OODB) a database that is organized and stored as objects.

Object oriented programming (OOP) a programming language methodology that consists of code contained in reusable objects.

Object reuse an attack on a system where one user or program is able to read residual information belonging to some other process, as a means for exploiting the other process through a weakness that can be discovered in the residual data.

Offer letter a formal letter from an organization to an employment candidate that offers employment under a basic set of terms.

Off-site storage the storage of storage media or paper documents at an off-site storage facility, to prevent against irrecoverable loss of information in the event of a disaster.

One-time pad an encryption algorithm where the key is the same size as the message and is used only once.

One-way hash *See* Message digest.

Open Database Connectivity (ODBC) a TCP/IP based client-server communications protocol used to facilitate database transactions over a network.

Open Shortest Path First (OSPF) a TCP/IP routing protocol used in large enterprise networks.

Open Systems Interconnect (OSI) the seven layer network model whose layers are: Physical, Data link, Network, Transport, Session, Presentation, and Application.

Optical fiber a cable type used to carry high-speed communications signals in the form of light over a glass-like fiber.

Organizationally Unique Identifier (OUI) the first three octets of a MAC address that is assigned to an equipment manufacturer, in order to guarantee uniqueness of MAC addresses.

Output feedback (OFB) a block cipher mode where the results of the previous plaintext block are used in the encryption of the next block.

Packet filter a router with an Access Control List (ACL) or an early generation firewall. *See also* Access Control List, Firewall.

Page fault an event where a process attempts to access data in a memory location that has been moved to secondary storage.

Paging the memory management technique of moving inactive memory pages between main storage and secondary storage.

Parallel test a test of a disaster recovery or business continuity plan in which backup or recovery systems or processes are operated alongside normal business operations.

Partition a separate division of storage, usually on a hard disk drive.

Password a secret word or phrase entered by a user to authenticate to a system.

Password Authentication Protocol (PAP) an authentication protocol used by PPP to authenticate users. PAP is unsafe because login credentials are not encrypted.

Password cracking an attack where the attacker uses tools to methodically guess passwords in order to gain access to a system.

Password guessing an attack where the attacker guesses likely passwords in an attempt to gain access to a system.

Patch management the process of managing the installation of patches on target systems.

Patent a means of legal protection for exclusive rights to an invention or process.

Payload the data that is contained in a network packet or frame.

PC card an external bus architecture used for the connection of compact peripheral devices to laptop computers.

PCI (Peripheral Component Interconnect) an internal bus architecture used in modern PCs.

Penetration testing an activity that consists of transmitting network packets to a target system in order to discover unprotected, misconfigured, or unsecure services on a target system.

Permutation cipher *See* Transposition cipher.

Personal Area Network (PAN) a computer network that spans a distance close to one person.

Personal Identification Number (PIN) a numeric password. *See also* Password.

Personally identifiable information (PII) items associated with an individual such as name, passport number, driver's license number, and social insurance number.

Pharming an attack where the attacker poisons DNS or hosts information to redirect communications intended for a legitimate system instead to an imposter system, as a means for harvesting sensitive information.

Phishing fraudulent e-mail messages that attempt to lure an unsuspecting user to provide private information via a fraudulent web site (usually) or in an e-mail reply (less often).

Physical controls mechanisms that control or monitor physical access and environmental systems.

Physical layer layer 1 of the OSI and TCP/IP network models that consists of a network's physical medium.

PIN pad a numeric keypad that is typically used in connection with an access control system.

PING a tool used to send an ICMP Echo Request to a specific node on a network.

Ping of Death (PoD) an attack where an attacker sends PING packets of length 65,535 bytes to the target system in hopes that the target system will crash.

Plaintext data that is not encrypted.

Point to Point Protocol (PPP) a TCP/IP layer 2 protocol that is usually used for dial-up Internet access.

Point to Point Tunneling Protocol (PPTP) an early TCP/IP tunneling protocol that has been largely replaced by L2TP and IPsec.

Policy an official statement that establishes plans, boundaries, and constraints on the behavior of information systems and employees.

Polyalphabetic cipher a cipher in which plaintext characters are substituted for ciphertext characters according to a multiple alphabet table.

Polymorphism the ability for an object to respond to a call differently, depending upon the object's type.

Port number a numbering scheme in which messages of various types are distinguished.

Presentation layer layer 6 of the OSI network model that provides various methods for presenting data, for instance in different character sets or encryption algorithms.

Pretexting an act of deception intended to persuade a targeted individual into providing information under false pretenses.

Pretty Good Privacy (PGP) a popular computer program that is used to encrypt and decrypt data.

Preventive control a control that blocks unauthorized or undesired activity.

Primary storage *See* Main storage.

Privacy the protection of sensitive information associated with individuals.

Privacy Enhanced Mail (PEM) a standard for encrypting e-mail that depends upon a global PKI.

Private key an encryption key used in public key cryptography that is kept private by its owner.

Privilege level an operating system protection scheme where users are assigned levels of permissions that dictates the resources and data that they are permitted to access.

Procedure step-by-step instructions for performing a task.

Program a set of computer instructions that usually resides in a file and is used to perform a specific task.

Program counter a CPU register that tracks the current instruction in a program.

PROM (Programmable Read Only Memory) a form of semiconductor memory used to store firmware.

Protected Extensible Authentication Protocol (Protected EAP or PEAP) a wireless network protocol used to authenticate users.

Protection ring a hierarchical operating system protection scheme used to protect resources based upon levels of privilege.

Public key an encryption key used in public key cryptography that can be widely distributed to users.

Public key cryptography a class of cryptographic algorithms that utilize public-private encryption keys.

Public Key Infrastructure (PKI) a network based service in which public encryption keys or certificates are stored and available for retrieval.

Public Switched Telephone Network (PSTN) the well known public telephone network. Also known as POTS (plain old telephone service).

Pull station a manually operated device that is used to trigger a building fire alarm.

Race condition *See* Time of check to time of use (tocttou) bug.

Random Access Memory (RAM) *See* main storage.

RC4 a common stream cipher.

Records retention the determination of the minimum and/or maximum period of time that specific business records must be retained.

Recovery the process of restoring a system to its pre-incident condition.

Recovery control a control that is used to restore conditions to normal.

Recovery Point Objective (RPO) the maximum acceptable amount of data loss or work loss for a given process.

Recovery Time Objective (RTO) the maximum period of time that a business process or IT system will be unavailable during a disaster.

Reduced Instruction Set Computer (RISC) a newer microprocessor design where the CPU has a smaller (reduced) instruction set which permits it to be more efficient.

Reduced sign-on a type of authentication where users have a limited set of userids and passwords that are used to access systems and applications.

Redundant Array of Independent Discs (RAID) a disc storage technology that allows for greater reliability and performance in a disc-based storage system.

Reference monitor a hardware or software component in a system that mediates access to objects according to their security level or clearance.

Register a storage location within a CPU.

Relational database a database model based upon tables of data and the relationships between them.

Relative humidity the amount of water vapor in a sample of air compared to the maximum amount of water vapor that the air can hold.

Remote access any means used to connect to a target network from a remote location.

Remote Authentication Dial In User Service (RADIUS) an authentication protocol used to authenticate a user, control access rights through authorization, and provide accounting (usage) information for billing.

Remote login (Rlogin) a TCP/IP layer 4 network protocol that is used to log in to another computer over a network.

Remote Procedure Call (RPC) a TCP/IP layer 4 protocol used to permit a computer to execute a subroutine or procedure on another computer.

Remote Shell (Rsh) a TCP/IP layer 4 protocol used to execute commands on other computers on a network.

Repeater a network device used to receive and re-transmit a network signal, usually to extend the physical length of a network connection.

Replay attack a cryptanalysis attack where the attacker records transmissions and replays them at a later time, usually to masquerade as one of the parties whose transmissions were recorded.

Replication an operation concerning the data on a storage system, where additions and changes to the data are transmitted to a counterpart storage system where the same additions and changes take place.

Requirements statements of necessary characteristics of an information system.

Residual risk the risk that remains after countermeasures are applied.

Resource protection controls and procedures enacted to protect business resources including facilities, hardware, software, documentation, and records.

Restore the process of copying data from backup media to a system.

Reverse Address Resolution Protocol (RARP) a TCP/IP protocol that is used to translate a known MAC address into an IP address. Superseded by DHCP.

RFC Request for Comments; the formalized documents that describe the Internet's technical and procedural standards.

Rijndael the data encryption algorithm chosen in 2001 as the new Advanced Encryption Standard.

Ring a network topology where each node is connected to exactly two other nodes in a circular pathway.

Risk acceptance a form of risk treatment where an identified risk is accepted as-is.

Risk analysis the process of identifying risks, their probability of occurrence, impact, and mitigating steps to reduce probability or impact.

Risk assessment the process of examining a system or process to identify potential risks.

Risk avoidance a form of risk treatment where the activity associated with an identified risk is discontinued, thereby avoiding the risk.

Risk management the strategic activities related to the identification of risks through risk assessment and the subsequent treatment of identified risks.

Risk mitigation *See* Risk reduction

Risk reduction a form of risk treatment where an identified risk is reduced through countermeasures.

Risk transfer a form of risk treatment where an identified risk is transferred to another party, typically through an insurance policy.

Role-based access control (RBAC) an access control method where access permissions are granted to roles, and users are assigned to those roles.

Rootkit malicious code that is designed to avoid detection by hiding itself by some means.

Router a network device that connects two or more networks together logically, and can also control the flow of traffic between networks according to a set of rules known as an Access Control List (ACL).

Routing Information Protocol (RIP) an early TCP/IP routing protocol that uses hop count as the primary metric for determining the lowest cost of a route between endpoints.

RS-232 a serial communications technology used to connect computers to low speed peripherals such as mice, printers, modems, and terminals. Superseded by USB.

RS-449 a serial communications standard that is similar to RS-232 and with a maximum bandwidth of 2Mbit/s.

rsh (remote shell) an unsecure protocol used to establish a command line session on another system over a network.

Running key cipher a cryptography technique used when plaintext is longer than the key.

SATA (Serial ATA) an external bus architecture used primarily for communications with disk storage.

SBus an internal bus architecture used in SPARC based computers including those made by Sun Microsystems.

Script Injection an attack on a system where script language accompanies input data in an attempt to execute the script on the target system.

Script kiddie an individual with relatively low skills who breaks into computer systems using tools written by others.

SCSI (Small Computer Systems Interface) an external bus architecture used to connect a computer to disk storage devices.

Secondary storage the slower, but persistent, form of storage used by a computer.

Secure / Multipurpose Internet Mail Extensions (S/MIME) a protocol used for protecting e-mail message through encryption and digital signatures.

Secure Electronic Transaction (SET) a protocol used to protect electronic transactions. SET is not widely used, and has been replaced by SSL and TLS.

Secure Shell (SSH) a TCP/IP layer 4 tunneling protocol used for secure remote management of systems. Supersedes Rsh, Rcp, Rlogin, and Telnet.

Secure siting locating a business at a site that is reasonably free from hazards.

Secure Sockets Layer (SSL) a TCP/IP layer 4 tunneling protocol used to protect network traffic through encryption. Superseded by TLS. *See also* TLS.

Security awareness training a formal education program that teaches security principles and expected behavior to employees.

Security guard a trained person who is responsible for protecting building assets and controlling access to the building.

Security incident an event in which some aspect of an organization's security policy has been violated.

Security incident response the procedures followed in the event of a security incident.

Security management activities related to the development and implementation of security policies and controls.

Security modes of operation the security classifications for systems that determine the types of permissions necessary for users to access data.

Security policy a branch of organizational policy that defines security-related controls and behaviors

Segregation of duties *See* separation of duties.

SEI CMMI (Software Engineering Institute Capability Maturity Model Integration) a framework for evaluating the maturity of an organization's systems engineering practices.

Sensitivity level a category of information sensitivity in an information classification scheme.

Separation of duties the work practice where high risk tasks are structured to be carried out by two or more persons.

Sequence number attack an attack in which an attacker injects packets with guessed sequence numbers that pretend to originate from one of the two computers in the session.

Serial Line Interface Protocol (SLIP) an early implementation for transporting TCP/IP over serial connections.

Service Level Agreement (SLA) formal statements that specify levels of service provided by a service organization.

Service set identifier (SSID) a name that is used to identify a specific Wi-Fi wireless network.

Session Initiation Protocol (SIP) a TCP/IP layer 4 protocol that is used to establish and tear down voice and video communications sessions.

Session layer layer 5 of the OSI network model that controls connections between computers.

SHA-1 (Secure Hash Algorithm) a message digest (hashing) algorithm.

Shredding the process of cutting paper, magnetic, or optical media into small pieces for the purpose of secure destruction.

S-HTTP (Secure Hyper-Text Transfer Protocol) a connectionless protocol used to encrypt and authenticate data being sent from a server to a client.

Side-channel attack an attack on a system where a subject can observe the physical characteristics of a system in order to make inferences on its internal operation.

Simple Mail Transport Protocol (SMTP) a TCP/IP layer 4 protocol used to transmit e-mail messages from one e-mail server to another.

Simple Network Management Protocol (SNMP) a TCP/IP layer 4 protocol used to remotely monitor and manage network devices and systems over a network.

Simulation a review of a disaster recovery or business continuity procedure that is performed in a pretend disaster scenario.

Single Loss Expectancy (SLE) the cost of a single loss through the realization of a particular threat. This is a result of the calculation, SLE = asset value x exposure factor (EF).

Single point of failure a component in a system that lacks a redundant or backup counterpart; the failure of the component will cause the failure of the entire system.

Single Sign-On an access control method where users can authenticate once and be able to access other systems and applications without being required to re-authenticate to each one.

Smart card a credit-card sized memory device used for authentication.

Smoke detector a device that detects the presence of combustion-related smoke and contains or is connected to an audible warning alarm.

Smurf an attack that consists of a large number of forged ICMP echo requests, which are sent to a network's broadcast address with a forged "source" address. Systems that receive the attack packets send large numbers of "reply" packets to the target.

Sniffer a device or program used to record communications on a network.

Sniffing the act of eavesdropping on a network by capturing traffic.

Social engineering an attack on an organization where the attacker is attempting to gain secrets from staff members, usually for gaining unauthorized access to the organization's systems.

Software computer instructions that fulfill a stated purpose.

Software development life cycle (SDLC) the overall process used to design, create, and maintain software over its lifetime.

Source code review a review of a program's source code in order to ensure that recent changes were applied correctly and that the program contains no unwanted code.

Spam unwanted e-mail that usually contains unsolicited commercial advertisements, pornography, or attempts to lure recipients into opening malicious attachments or visiting malicious web sites.

Spear phishing a specially targeted phishing attack. *See also* phishing.

Split custody a control safeguard in which an important secret (such as a password) is broken into two or more parts, each of which is kept by different individuals.

Spoofing an attack where the attacker forges the origin of a message as an attempt to disrupt or control a system.

Sprinkler system an installed system of piping and nozzles used to spray water or foam onto a fire.

Spyware usually unwanted and sometimes malicious software that is used to harvest Internet usage information from a user's workstation.

SQL injection an attack where SQL statements are injected into an input stream in the hopes that the SQL commands will be executed by the application's database server.

SQLNet a TCP/IP based client-server communications protocol used to facilitate database transactions over a network.

Standard a statement that specifies the brand, model, protocol, technology, or configuration of a system.

Star a network topology where all nodes are connected to a central device such as a hub or switch.

Statement of impact a document that describes the impact that an interrupted business process would have on an organization.

Static random access memory (SRAM) a random access memory (RAM) technology used in computer main memory.

Steganography the practice of hiding a message in another medium.

Stream cipher an encryption algorithm that operates on a continuous stream of data, such as a video or audio feed.

Strong authentication a means of authenticating to a system using a means strong than userid and password, such as a hardware token, smart card, or biometric. Also known as two-factor authentication.

Structured language a hierarchical computer language methodology that consists of main programs and called subroutines or functions.

Subnet a range of a network addresses in a network.

Subnet mask a numeric value, expressed in the same manner as an IP address, that is used to determine the network and host portions of an IP address.

Substitution cipher an encryption algorithm where characters are substituted for others.

Swapping the memory management technique of moving an entire process's memory contents between main storage and secondary storage.

Switch a network device used to connect multiple computers to form a network. A switch sends packets only to destination nodes. *See also* Hub.

Symmetric cryptography a method of cryptography where each party is in possession of an encryption key.

Symmetric multiprocessing (SMP) a computer architecture where two or more CPUs are connected to the computer's main memory in a symmetrical arrangement.

SYN flood a denial of service (DoS) attack where the attacker sends large numbers of TCP SYN packets to the target system, hoping to overwhelm it and exhaust its resources.

Synchronous Digital Hierarchy (SDH) the prevalent standard for voice and data communications over fiber networks outside of North America. *See also* SONET.

Synchronous optical networking (SONET) the standard in North America for transporting voice and data over optical fiber.

System high security mode one of the security modes of operation where all users can access some data based upon their need to know.

Systems Security Engineering Capability Maturity Model (SSE CMM) a framework for evaluating the maturity of an organization's security implementation practices.

T1 *See* DS-1.

Target of evaluation (TOE) a system being evaluated with the Common Criteria.

Teardrop an attack in which an attacker sends mangled packet fragments with overlapping and oversized payloads to a target system in an attempt to crash the target system.

Technical controls programs and mechanisms that control user access system behavior.

TELNET a TCP/IP layer 4 protocol that is used to establish a raw TCP session over a network to a service on another computer.

TEMPEST U.S. DoD research in the fields of unwanted emanations and the resulting standards for shielding equipment.

Terminal Access Controller Access-Control System (TACACS) a remote authentication protocol used to authenticate user access to a computer or network based resource. Superseded by TACACS+ and RADIUS.

Termination the cessation of employment for an employee.

Terrorist attack *See* cyberterrorism.

Threat a potential activity that would, if it occurred, exploit a vulnerability in a system.

Threat analysis the process of identifying potential threats, their probability of occurrence, impact, and mitigating steps to reduce probability or impact.

Threat risk modeling a process where threats in an environment are identified and ranked, and mitigating controls introduced to counter the identified threats. Also known as threat modeling.

Three tier application an application that consists of three logically separate layers, usually a user interface front end, business logic middle tier, and database management third tier.

Time bomb *See* Logic bomb.

Time of check to time of use (tocttou) bug a resource allocation vulnerability where a period of time elapses between the time when a resource's availability is confirmed and the resource is assigned or used.

Token a hardware device used for authentication.

Token Ring a network technology consisting of a logical ring and the passing of a logical 'token' from node to node over the network. Only a node in possession of a token may transmit data.

Tools separate programs that are included with an Operating System that are used to change system configurations, edit files, create directories, and install other programs.

Traceroute a tool used to determine the network path to a specific destination.

Trade secret a formula, design, process, or method used by an organization to gain competitive advantage over others.

Trademark a means of legal protection for exclusive rights to a name or symbol.

Transaction an event where data is updated within a database.

Transmission Control Protocol (TCP) a connection-oriented TCP/IP transport protocol used to carry messages within a session between two nodes. TCP guarantees delivery, order of delivery, and flow control.

Transport layer layer 4 of the OSI model and layer 3 in the TCP/IP network models that provides reliable data transfer.

Transport Layer Security (TLS) a TCP/IP layer 4 tunneling protocol that protects network traffic through encryption. TLS supersedes SSL.

Transposition cipher an encryption method where characters in plaintext are rearranged to form ciphertext.

Trap door *See* back door.

Trivial File Transfer Protocol (TFTP) a TCP/IP layer 4 protocol used to transfer files over a network.

Trojan horse malicious computer code that claims to perform some benign function while actually performing some additional, malicious function.

Trusted Computer Security Evaluation Criteria (TCSEC) the U.S. DoD framework for system security evaluation now superseded by the Common Criteria.

Trusted Computing Base (TCB) the hardware, firmware, operating system, and software that effectively supports security policy.

Trusted Network Interpretation (TNI) the evaluation criteria for evaluating the confidentiality and integrity of communications networks.

Trusted Platform Module (TPM) a secure cryptoprocessor used to store cryptographic keys and perform some crypto functions.

Tunnel any of several network protocols that use packet encapsulation to deliver packets to an endpoint.

Twisted pair a type of cable that utilizes pairs of twisted copper conductors.

Two tier application an application that consists of two logically separate layers, usually a user interface and business logic front end and a data management back end.

Two-factor authentication *See* Strong authentication.

Unibus an internal bus architecture used by Digital Equipment Corp. PDP-11 and VAX computers.

Unicast a type of network communications where packets are sent to a single node. See also multicast.

Unified Threat Management (UTM) a security device or appliance that performs many security functions such as firewall, IDS, IPS, anti-virus, anti-spam, or Web content filtering.

Uninterruptible Power Supply (UPS) a short-term backup power source that derives its power from storage batteries.

United States Code (U.S.C.) the body of published criminal laws in the United States.

Universal Mobile Telecommunications System (UMTS) a wireless telecommunications protocol for data communications.

Universal Serial Bus (USB) a serial bus communications standard, used for the connection of peripheral devices to a computer including keyboards, mice, storage device, and network adaptors.

Unsolicited Commercial E-mail (UCE) *See* Spam.

U.S. Code of Federal Regulations (C.F.R.) the code of administrative law in the United States.

User Datagram Protocol (UDP) a connectionless TCP/IP transport protocol used to carry messages within a session between two nodes. UDP does not guarantee delivery, order of delivery, or flow control.

Vernam cipher *See* One-time pad.

Video surveillance system a system that consists of monitors and/or recording equipment plus one or more video cameras, which together are used to observe and/or record activities such as personnel movement.

View a virtual table in a relational database.

Virtual memory a memory management technique whereby the operating system can permit a process's memory to become fragment and even overflow onto secondary storage.

Virtual Private Network (VPN) an encrypted communications channel that is used for secure remote access or for protecting the traffic between two networks.

Virus malicious code that attaches to a file, document, or master boot record (MBR).

Voice over Internet Protocol (VoIP) a TCP/IP layer 4 protocol used to transport voice traffic over a network.

Vulnerability a weakness in a system that may permit the realization of a threat.

Vulnerability management the process of identifying vulnerabilities in a system and then acting to mitigate those vulnerabilities.

Walkthrough a review of a business continuity or disaster recovery procedure in which a group of individuals review and discuss procedures.

Watermarking the process of placing in image or mark in a file for identification purposes.

Web application an application that utilizes a Web browser as the client software.

Web server a software component used to accept and process incoming requests for information sent from end users who are using Web browsers.

Whaling a specially targeted phishing attack that targets executives in an organization.

Whois a TCP/IP layer 4 protocol that is used to query a whois server, usually to determine the owner of a domain name or IP address.

Wide Area Network (WAN) a computer network covering large geographic areas spanning metropolitan, regional, national, or international.

Wi-Fi a family of wireless data link standards for connecting computers together to form networks.

Wi-Fi Protected Access (WPA and WPA2) protocol standards that replace the Wired Equivalent Privacy (WEP) protocol.

Wi-Fi Protected Access (WPA) a wireless network encryption protocol.

Wiping the process of destroying data stored on magnetic media by overwriting the media several times.

Wired Equivalent Privacy (WEP) a standard for encrypting packets on a Wi-Fi wireless network. Superseded by WPA and WPA2.

Wireless USB (WUSB) a wireless protocol designed for wireless connectivity of various computer peripherals such as printers, digital cameras, hard disks, and other high-throughput devices.

Wireline any of the telecommunications services that is transported over copper or optical fiber.

Worldwide Interoperability for Microwave Access (WiMAX) a wireless telecommunications standard for fixed-base and mobile voice and data communications.

Worm malicious code that has the ability to self-propagate and spread rapidly from system to system.

X.25 a packet-switched telecommunications network.

x.509 the prevailing digital certificate standard. *See also* Digital Certificate.

X11 the GUI based window system that is used in UNIX and Linux operating systems.

xDSL *See* Digital Subscriber Line (DSL).

XOR a logical operation on two operands, where the return value is TRUE only if one of the two operands (but not both) is TRUE.

Index

Page references in **bold** denote pages on which terms are defined.

B

C

D

E

F

G

H

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X