Top-Down Network Design

Third Edition

A systems analysis approach to enterprise network design

ciscopress.com

Priscilla Oppenheimer

Top-Down Network Design

Third Edition

Priscilla Oppenheimer

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

Top-Down Network Design, Third Edition

Priscilla Oppenheimer

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America

Third Printing: May 2012

Library of Congress Cataloging-in-Publication data is on file.

ISBN-13: 978-1-58720-283-4

ISBN-10: 1-58720-283-2

Warning and Disclaimer

This book is designed to provide information about top-down network design. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an "as is" basis. The author, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact:
U.S. Corporate and Government Sales 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States please contact: International Sales international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Executive Editor: Mary Beth Ray

Managing Editor: Sandra Schroeder

Senior Development Editor: Christopher Cleveland

Senior Project Editor: Tonya Simpson

Editorial Assistant: Vanessa Evans

Composition: Mark Shirar

Indexer: Tim Wright

Manager, Global Certification: Erik Ullanderson

Business Operation Manager, Cisco Press: Anand Sundaram

Technical Editors: Keith Nabozny, Joe Wilson

Copy Editor: Bill McManus

Book Designer: Louisa Adair

Proofreader: Apostrophe Editing Services

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

About the Author

Priscilla Oppenheimer has been developing data communications and networking systems since 1980 when she earned her master's degree in information science from the University of Michigan. After many years as a software developer, she became a technical instructor and training developer and has taught more than 3000 network engineers from most of the Fortune 500 companies. Her employment at such companies as Apple Computer, Network General, and Cisco gave her a chance to troubleshoot real-world network design problems and the opportunity to develop a practical methodology for enterprise network design. Priscilla was one of the developers of the Cisco Internetwork Design course and the creator of the Designing Cisco Networks course. Priscilla teaches network design, configuration, and troubleshooting around the world and practices what she preaches in her network consulting business.

About the Technical Reviewers

Keith Nabozny is a technology consultant with HP, an adjunct professor at Macomb Community College, and a graduate of Oakland University in Rochester, Michigan. He has three Cisco professional certifications and is a Certified Information Systems Security Professional (CISSP). Keith has supported large corporate clients for the past 14 years in operations, implementation, and engineering roles. He is currently supporting the firewalls of a major manufacturer with locations around the world. Most recently he taught network design and troubleshooting classes at Macomb Community College. Keith and his family live in Southeast Michigan.

Joe Wilson, MSCS, PMC, CISSP No. 100304, is a senior network design engineer for TelcoCapital Systems, LLC. TelcoCapital is a leading provider of Cisco Unified Communications solutions for small and medium-sized enterprises. Joe is completing his dissertation toward a PhD in information technology at Capella University (Minneapolis, MN), with specializations in college teaching and IT security and assurance. Joe has worked in information technology for the past 20 years and is a retired systems engineer from The Boeing Company in Seattle, Washington, where he designed airborne NMS solutions for commercial aircraft. While working for AT&T Broadband Network Solutions as a broadband systems engineer, Joe designed commercial broadband networks using advanced communications technologies such as ATM, SONET, DWDM, and Gigabit Ethernet. Joe has been a CISSP since 2006 and has distinguished himself as a trusted partner in providing secure communications solutions and services to public and private organizations. Joe teaches courses in the Cisco Networking Academy program at DeVry University in Federal Way, Washington.

Dedication

To my parents, Dr. Stephen T. Worland, PhD, and Mrs. Roberta Worland, MS. They gave me an appreciation for knowledge, logic, and analysis, and taught me that "where there's a will, there's a way."

Acknowledgments

I would like to thank Mary Beth Ray, executive editor at Cisco Press, for giving me the opportunity to update this book and for marshaling the people and resources needed to complete the project. I would especially like to thank Christopher Cleveland, Tonya Simpson, and Bill McManus for their hard work on the book. I am also grateful for the work of the technical editors, Keith Nabozny and Joe Wilson. In many ways, updating a book is even harder than writing it in the first place, and I couldn't have done it without the help of Chris, Tonya, Bill, Keith, and Joe.

I also wish to thank the technical editors for the first two editions, Matthew Birkner, Blair Buchanan, Dr. Peter Welcher, Dr. Alex Cannara, David Jansson, and Hank Mauldin. Their terrific contributions are still evident in the third edition.

I would like to thank other networking professionals who have inspired me over the years, including Joseph Bardwell and Anita Lenk from Connect802, Laura Chappell and her terrific Wireshark University, Howard Berkowitz, Paul Borghese, John Neiberger, Leigh Anne Chisholm, Marty Adkins, Matthias David Moore, Tom Lisa, Scott Vermillion, and many more.

I am grateful for my colleagues and students in Ashland, Oregon, who have inspired and entertained me, including Dr. Lynn Ackler, Jeff McJunkin, Andrew Krug, Brandon Kester, Stephen Perkins, Daniel DeFreeze, Christina Kaiserman, Nicole Colbert, Corey Smith, Stefan Hutchison, Jesse Williamson, Jonathan McCoy, Jennifer Comstock, Linda Sturgeon, Kathleen Marrs, Vinnie Moscaritolo, Louis Kowolowski, and Robert Luaders for his ideas regarding the design scenarios.

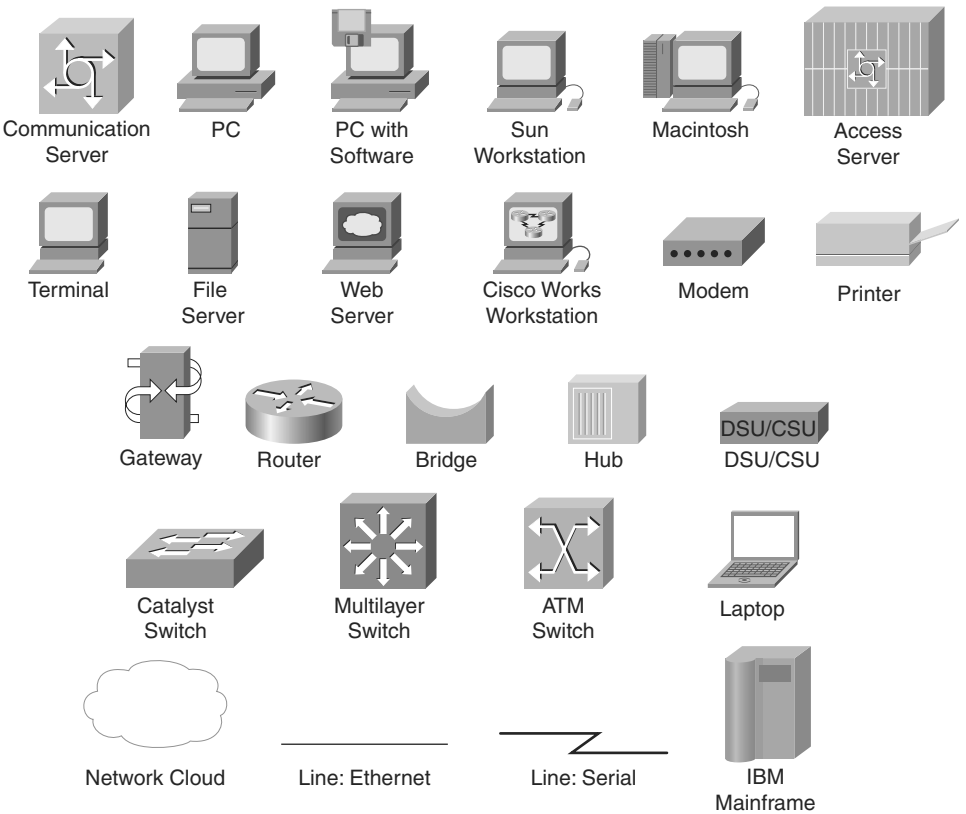
I'd like to thank Gary Rubin, Rob Stump, and Kip Peterson from Advanced Network Information for the many opportunities they've given me over the years, in particular the terrific opportunity to work at Cisco. To my colleagues at Cisco, Patrick Stark, our manager, Lisa Bacani, Walt Sacharok, Dax Mickelson, David Daverso, and Paul Azzi; you are terrific!

Finally, I would like to thank Alan Oppenheimer, who throughout this project acted as my technical advisor, therapist, chef, and best friend. I'm glad he doesn't mind that it was finally time to remove AppleTalk.

Contents at a Glance

Contents

Icons Used in This Book



Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the Cisco IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

New business practices are driving changes in enterprise networks. The transition from an industrial to an information economy has changed how employees do their jobs, and the emergence of a global economy of unprecedented competitiveness has accelerated the speed at which companies must adapt to technological and financial changes.

To reduce the time to develop and market products, companies are empowering employees to make strategic decisions that require access to sales, marketing, financial, and engineering data. Employees at corporate headquarters and in worldwide field offices, and telecommuters in home offices, need immediate access to data, regardless of whether the data is on centralized or departmental servers.

To develop, sell, and distribute products into domestic and foreign markets, businesses are forming alliances with local and international partners. Businesses are carefully planning their network designs to meet security goals while also offering network access to resellers, vendors, customers, prospective customers, and contract workers located all over the world.

To accommodate increasing requirements for remote access, security, bandwidth, scalability, and reliability, vendors and standards bodies introduce new protocols and technologies at a rapid rate. Network designers are challenged to develop state-of-the-art networks even though the state of the art is continually changing.

Whether you are a novice network designer or a seasoned network architect, you probably have concerns about how to design a network that can keep pace with the accelerating changes in the internetworking industry. The goal of this book is to teach a systematic design methodology that can help you meet an organization's requirements, regardless of the newness or complexity of applications and technologies.

Objectives

The purpose of *Top-Down Network Design*, Third Edition, is to help you design networks that meet a customer's business and technical goals. Whether your customer is another department within your own company or an external client, this book provides you with tested processes and tools to help you understand traffic flow, protocol behavior, and internetworking technologies. After completing this book, you will be equipped to design enterprise networks that meet a customer's requirements for functionality, capacity, performance, availability, scalability, affordability, security, and manageability.

Audience

This book is for you if you are an internetworking professional responsible for designing and maintaining medium- to large-sized enterprise networks. If you are a network engineer, architect, or technician who has a working knowledge of network protocols and

technologies, this book will provide you with practical advice on applying your knowledge to internetwork design.

This book also includes useful information for consultants, systems engineers, and sales engineers who design corporate networks for clients. In the fast-paced presales environment of many systems engineers, it often is difficult to slow down and insist on a top-down, structured systems analysis approach. Wherever possible, this book includes shortcuts and assumptions that can be made to speed up the network design process.

Finally, this book is useful for undergraduate and graduate students in computer science and information technology disciplines. Students who have taken one or two courses in networking theory will find *Top-Down Network Design*, Third Edition, an approachable introduction to the engineering and business issues related to developing real-world networks that solve typical business problems.

Changes for the Third Edition

Networks have changed in many ways since the second edition was published. Many legacy technologies have disappeared and are no longer covered in the book. In addition, modern networks have become multifaceted, providing support for numerous bandwidth-hungry applications and a variety of devices, ranging from smart phones to tablet PCs to high-end servers.

Modern users expect the network to be available all the time, from any device, and to let them securely collaborate with coworkers, friends, and family. Networks today support voice, video, high-definition TV, desktop sharing, virtual meetings, online training, virtual reality, and applications that we can't even imagine that brilliant college students are busily creating in their dorm rooms.

As applications rapidly change and put more demand on networks, the need to teach a systematic approach to network design is even more important than ever. With that need in mind, the third edition has been retooled to make it an ideal textbook for college students. The third edition features review questions and design scenarios at the end of each chapter to help students learn top-down network design.

To address new demands on modern networks, the third edition of *Top-Down Network Design* also has updated material on the following topics:

- Network redundancy
- Modularity in network designs
- The Cisco SAFE security reference architecture
- The Rapid Spanning Tree Protocol (RSTP)
- Internet Protocol version 6 (IPv6)
- Ethernet scalability options, including 10-Gbps Ethernet and Metro Ethernet
- Network design and management tools

Organization

This book is built around the steps for top-down network design. It is organized into four parts that correspond to the major phases of network design.

Part I: Identifying Your Customer's Needs and Goals

Part I covers the requirements-analysis phase. This phase starts with identifying business goals and technical requirements. The task of characterizing the existing network, including the architecture and performance of major network segments and devices, follows. The last step in this phase is to analyze network traffic, including traffic flow and load, protocol behavior, and quality of service (QoS) requirements.

Part II: Logical Network Design

During the logical network design phase, the network designer develops a network topology. Depending on the size of the network and traffic characteristics, the topology can range from simple to complex, requiring hierarchy and modularity. During this phase, the network designer also devises a network layer addressing model and selects switching and routing protocols. Logical design also includes security planning, network management design, and the initial investigation into which service providers can meet WAN and remote-access requirements.

Part III: Physical Network Design

During the physical design phase, specific technologies and products that realize the logical design are selected. Physical network design starts with the selection of technologies and devices for campus networks, including cabling, Ethernet switches, wireless access points, wireless bridges, and routers. Selecting technologies and devices for remote-access and WAN needs follows. Also, the investigation into service providers, which began during the logical design phase, must be completed during this phase.

Part IV: Testing, Optimizing, and Documenting Your Network Design

The final steps in top-down network design are to write and implement a test plan, build a prototype or pilot, optimize the network design, and document your work with a network design proposal. If your test results indicate any performance problems, during this phase you should update your design to include such optimization features as traffic shaping and advanced router queuing and switching mechanisms. A glossary of networking terms concludes the book.

Companion Website

Top-Down Network Design, Third Edition, has a companion website at www.topdownbook.com. The companion website includes updates to the book, links to white papers, and supplemental information about design resources.

Chapter 8

Developing Network Security Strategies

Developing security strategies that can protect all parts of a complicated network while having a limited effect on ease of use and performance is one of the most important and difficult tasks related to network design. Security design is challenged by the complexity and porous nature of modern networks that include public servers for electronic commerce, extranet connections for business partners, and remote-access services for users reaching the network from home, customer sites, hotel rooms, Internet cafes, and so on. To help you handle the difficulties inherent in designing network security for complex networks, this chapter teaches a systematic, top-down approach that focuses on planning and policy development before the selection of security products.

The goal of this chapter is to help you work with your network design customers in the development of effective security strategies, and to help you select the right techniques to implement the strategies. The chapter describes the steps for developing a security strategy and covers some basic security principles. The chapter presents a modular approach to security design that will let you apply layered solutions that protect a network in many ways. The final sections describe methods for securing the components of a typical enterprise network that are most at risk, including Internet connections, remote-access networks, network and user services, and wireless networks.

Security should be considered during many steps of the top-down network design process. This isn't the only chapter that covers security. Chapter 2, "Analyzing Technical Goals and Tradeoffs," discussed identifying network assets, analyzing security risks, and developing security requirements. Chapter 5, "Designing a Network Topology," covered secure network topologies. This chapter focuses on security strategies and mechanisms.

Network Security Design

Following a structured set of steps when developing and implementing network security will help you address the varied concerns that play a part in security design. Many security strategies have been developed in a haphazard way and have failed to actually secure assets and to meet a customer's primary goals for security. Breaking down the process of

security design into the following steps will help you effectively plan and execute a security strategy:

1. Identify network assets.
2. Analyze security risks.
3. Analyze security requirements and tradeoffs.
4. Develop a security plan.
5. Define a security policy.
6. Develop procedures for applying security policies.
7. Develop a technical implementation strategy.
8. Achieve buy-in from users, managers, and technical staff.
9. Train users, managers, and technical staff.
10. Implement the technical strategy and security procedures.
11. Test the security and update it if any problems are found.
12. Maintain security.

Chapter 2 covered steps 1 through 3 in detail. This chapter quickly revisits steps 1 through 3 and also addresses steps 4, 5, 6, and 12. Steps 7 through 10 are outside the scope of this book. Chapter 12, "Testing Your Network Design," addresses Step 11.

Identifying Network Assets

Chapter 2 discussed gathering information on a customer's goals for network security. As discussed in Chapter 2, analyzing goals involves identifying network assets and the risk that those assets could be sabotaged or inappropriately accessed. It also involves analyzing the consequences of risks.

Network assets can include network hosts (including the hosts' operating systems, applications, and data), internetworking devices (such as routers and switches), and network data that traverses the network. Less obvious, but still important, assets include intellectual property, trade secrets, and a company's reputation.

Analyzing Security Risks

Risks can range from hostile intruders to untrained users who download Internet applications that have viruses. Hostile intruders can steal data, change data, and cause service to be denied to legitimate users. *Denial-of-service (DoS)* attacks have become increasingly common in the past few years. See Chapter 2 for more details on risk analysis.

Analyzing Security Requirements and Tradeoffs

Chapter 2 covers security requirements analysis in more detail. Although many customers have more specific goals, in general, security requirements boil down to the need to protect the following assets:

- The confidentiality of data, so that only authorized users can view sensitive information
- The integrity of data, so that only authorized users can change sensitive information
- System and data availability, so that users have uninterrupted access to important computing resources

According to RFC 2196, "Site Security Handbook:"

> One old truism in security is that the cost of protecting yourself against a threat should be less than the cost of recovering if the threat were to strike you. Cost in this context should be remembered to include losses expressed in real currency, reputation, trustworthiness, and other less obvious measures.

As is the case with most technical design requirements, achieving security goals means making tradeoffs. Tradeoffs must be made between security goals and goals for affordability, usability, performance, and availability. Also, security adds to the amount of management work because user login IDs, passwords, and audit logs must be maintained.

Security also affects network performance. Security features such as packet filters and data encryption consume CPU power and memory on hosts, routers, and servers. Encryption can use upward of 15 percent of available CPU power on a router or server. Encryption can be implemented on dedicated appliances instead of on shared routers or servers, but there is still an effect on network performance because of the delay that packets experience while they are being encrypted or decrypted.

Another tradeoff is that security can reduce network redundancy. If all traffic must go through an encryption device, for example, the device becomes a single point of failure. This makes it hard to meet availability goals.

Security can also make it harder to offer load balancing. Some security mechanisms require traffic to always take the same path so that security mechanisms can be applied uniformly. For example, a mechanism that randomizes TCP sequence numbers (so that hackers can't guess the numbers) won't work if some TCP segments for a session take a path that bypasses the randomizing function due to load balancing.

Developing a Security Plan

One of the first steps in security design is developing a security plan. A *security plan* is a high-level document that proposes what an organization is going to do to meet security requirements. The plan specifies the time, people, and other resources that will be required to develop a security policy and achieve technical implementation of the policy. As the network designer, you can help your customer develop a plan that is practical and

pertinent. The plan should be based on the customer's goals and the analysis of network assets and risks.

A security plan should reference the network topology and include a list of network services that will be provided (for example, FTP, web, email, and so on). This list should specify who provides the services, who has access to the services, how access is provided, and who administers the services.

As the network designer, you can help the customer evaluate which services are definitely needed, based on the customer's business and technical goals. Sometimes new services are added unnecessarily, simply because they are the latest trend. Adding services might require new packet filters on routers and firewalls to protect the services, or additional user-authentication processes to limit access to the services, adding complexity to the security strategy. Overly complex security strategies should be avoided because they can be self-defeating. Complicated security strategies are hard to implement correctly without introducing unexpected security holes.

One of the most important aspects of the security plan is a specification of the people who must be involved in implementing network security:

- Will specialized security administrators be hired?
- How will end users and their managers get involved?
- How will end users, managers, and technical staff be trained on security policies and procedures?

For a security plan to be useful, it needs to have the support of all levels of employees within the organization. It is especially important that corporate management fully support the security plan. Technical staff at headquarters and remote sites should buy into the plan, as should end users.

Developing a Security Policy

According to RFC 2196, "Site Security Handbook:"

> A security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide.

A *security policy* informs users, managers, and technical staff of their obligations for protecting technology and information assets. The policy should specify the mechanisms by which these obligations can be met. As was the case with the security plan, the security policy should have buy-in from employees, managers, executives, and technical personnel.

Developing a security policy is the job of senior management, with help from security and network administrators. The administrators get input from managers, users, network designers and engineers, and possibly legal counsel. As a network designer, you should work closely with the security administrators to understand how policies might affect the network design.

After a security policy has been developed, with the engagement of users, staff, and management, it should be explained to all by top management. Many enterprises require personnel to sign a statement indicating that they have read, understood, and agreed to abide by a policy.

A security policy is a living document. Because organizations constantly change, security policies should be regularly updated to reflect new business directions and technological shifts. Risks change over time also and affect the security policy.

Components of a Security Policy

In general, a policy should include at least the following items:

- An *access policy* that defines access rights and privileges. The access policy should provide guidelines for connecting external networks, connecting devices to a network, and adding new software to systems. An access policy might also address how data is categorized (for example, confidential, internal, and top secret).
- An *accountability policy* that defines the responsibilities of users, operations staff, and management. The accountability policy should specify an audit capability and provide incident-handling guidelines that specify what to do and whom to contact if a possible intrusion is detected.
- An *authentication policy* that establishes trust through an effective password policy and sets up guidelines for remote-location authentication.
- A *privacy policy* that defines reasonable expectations of privacy regarding the monitoring of electronic mail, logging of keystrokes, and access to users' files.
- *Computer-technology purchasing guidelines* that specify the requirements for acquiring, configuring, and auditing computer systems and networks for compliance with the policy.

Developing Security Procedures

Security procedures implement security policies. Procedures define configuration, login, audit, and maintenance processes. Security procedures should be written for end users, network administrators, and security administrators. Security procedures should specify how to handle incidents (that is, what to do and who to contact if an intrusion is detected). Security procedures can be communicated to users and administrators in instructor-led and self-paced training classes.

Maintaining Security

Security must be maintained by scheduling periodic independent audits, reading audit logs, responding to incidents, reading current literature and agency alerts, performing security testing, training security administrators, and updating the security plan and policy. Network security should be a perpetual process. Risks change over time, and so should security. Cisco security experts use the term *security wheel* to illustrate that

implementing, monitoring, testing, and improving security is a never-ending process. Many overworked security engineers might relate to the wheel concept. Continually updating security mechanisms to keep up with the latest attacks can sometimes make an administrator feel a bit like a hamster on a training wheel.

Security Mechanisms

This section describes some typical ingredients of secure network designs. You can select from these ingredients when designing solutions for common security challenges, which are described in the "Modularizing Security Design" section later in this chapter.

Physical Security

Physical security refers to limiting access to key network resources by keeping the resources behind a locked door and protected from natural and human-made disasters. Physical security can protect a network from inadvertent misuses of network equipment by untrained employees and contractors. It can also protect the network from hackers, competitors, and terrorists walking in off the street and changing equipment configurations.

Depending on the level of protection, physical security can protect a network from terrorist and biohazard events, including bombs, radioactive spills, and so on. Physical security can also protect resources from natural disasters such as floods, fires, storms, and earthquakes.

Depending on your particular network design customer, physical security should be installed to protect core routers, demarcation points, cabling, modems, servers, hosts, backup storage, and so on. Work with your customer during the early stages of the network design project to make sure equipment will be placed in computer rooms that have card key access and/or security guards. Computer rooms should also be equipped with uninterruptible power supplies, fire alarms, fire-abatement mechanisms, and water-removal systems. To protect equipment from earthquakes and high winds during storms, equipment should be installed in racks that attach to the floor or wall.

Because physical security is such an obvious requirement, it is easy to forget to plan for it, but it should never be overlooked or considered less important than other security mechanisms. As mentioned in the "Secure Network Design Topologies" section of Chapter 5, you should start working with your design customer at the beginning of the design project to make sure that critical equipment will be protected. Planning for physical security should start during the early phases of the top-down design process in case there are lead times to build or install security mechanisms.

Authentication

Authentication identifies who is requesting network services. The term *authentication* usually refers to authenticating users but can also refer to authenticating devices or software processes. For example, some routing protocols support *route authentication*, whereby a router must pass some criteria before another router accepts its routing updates.

Most security policies state that to access a network and its services, a user must enter a login ID and password that are authenticated by a security server. To maximize security, one-time (dynamic) passwords can be used. With one-time password systems, a user's password always changes. This is often accomplished with a security card, also called a *Smartcard*. A *security card* is a physical device about the size of a credit card. The user types a personal identification number (PIN) into the card. The *PIN* is an initial level of security that simply gives the user permission to use the card. The card provides a one-time password that is used to access the corporate network for a limited time. The password is synchronized with a central security card server that resides on the network. Security cards are commonly used by telecommuters and mobile users. They are not usually used for LAN access.

Authentication is traditionally based on one of three proofs:

- **Something the user knows:** This usually involves knowledge of a unique secret that is shared by the authenticating parties. To a user, this secret appears as a classic password, a PIN, or a private cryptographic key.
- **Something the user has:** This usually involves physical possession of an item that is unique to the user. Examples include password token cards, security cards, and hardware keys.
- **Something the user is:** This involves verification of a unique physical characteristic of the user, such as a fingerprint, retina pattern, voice, or face.

Many systems use *two-factor authentication*, which requires a user to have two proofs of identity. An example is an access control system that requires a security card and a password. With two-factor authentication, a compromise of one factor does not lead to a compromise of the system. An attacker could learn a password, but the password is useless without the security card. Conversely, if the security card is stolen, it cannot be used without the password.

Authorization

Whereas authentication controls who can access network resources, *authorization* says what they can do after they have accessed the resources. Authorization grants privileges to processes and users. Authorization lets a security administrator control parts of a network (for example, directories and files on servers).

Authorization varies from user to user, partly depending on a user's department or job function. For example, a policy might state that only Human Resources employees should see salary records for people they don't manage.

Security experts recommend use of the *principle of least privilege* in the implementation of authorization. This principle is based on the idea that each user should be given only the minimal necessary rights to perform a certain task. Therefore, an authorization mechanism should give a user only the minimum access permissions that are necessary. Explicitly listing the authorized activities of each user with respect to every resource is difficult, so techniques are used to simplify the process. For example, a network manager can create user groups for users with the same privileges.

Accounting (Auditing)

To effectively analyze the security of a network and to respond to security incidents, procedures should be established for collecting network activity data. Collecting data is called *accounting* or *auditing*.

For networks with strict security policies, audit data should include all attempts to achieve authentication and authorization by any person. It is especially important to log "anonymous" or "guest" access to public servers. The data should also log all attempts by users to change their access rights.

The collected data should include user- and hostnames for login and logout attempts, and previous and new access rights for a change of access rights. Each entry in the audit log should be timestamped.

The audit process should not collect passwords. Collecting passwords creates a potential for a security breach if the audit records are improperly accessed. Neither correct nor incorrect passwords should be collected. An incorrect password often differs from the valid password by only a single character or transposition of characters.

A further extension of auditing is the concept of security assessment. With *security assessment*, the network is examined from within by professionals, trained in the vulnerabilities exploited by network invaders. Part of any security policy and audit procedure should be periodic assessments of the vulnerabilities in a network. The result should be a specific plan for correcting deficiencies, which might be as simple as retraining staff.

Data Encryption

Encryption is a process that scrambles data to protect it from being read by anyone but the intended receiver. An *encryption device* encrypts data before placing it on a network. A *decryption device* decrypts the data before passing it to an application. A router, server, end system, or dedicated device can act as an encryption or decryption device. Data that is encrypted is called *ciphered data* (or simply *encrypted data*). Data that is not encrypted is called *plain text* or *clear text*.

Encryption is a useful security feature for providing data confidentiality. It can also be used to identify the sender of data. Although authentication and authorization should also protect the confidentiality of data and identify senders, encryption is a good security feature to implement in case the other types of security fail.

There are performance tradeoffs associated with encryption, however, as mentioned in the "Analyzing Security Tradeoffs" section earlier in the chapter. Encryption should be used when a customer has analyzed security risks and identified severe consequences if data is not kept confidential and the identity of senders of data is not guaranteed. On internal networks and networks that use the Internet simply for web browsing, email, and file transfer, encryption is usually not necessary. For organizations that connect private sites via the Internet, using virtual private networking (VPN), encryption is recommended to protect the confidentiality of the organization's data.

Encryption has two parts:

- An *encryption algorithm* is a set of instructions to scramble and unscramble data.
- An *encryption key* is a code used by an algorithm to scramble and unscramble data.

Children sometimes play with encryption by using a simple algorithm such as "find the letter on the top row and use the letter on the bottom row instead," and a key that might look something like the following table:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
I	N	B	Y	G	L	S	P	T	A	R	W	Q	H	X	M	D	K	F	U	O	C	Z	V	E	J

In this example, LISA is encrypted as WTFI. The key shows only uppercase letters, but there are many other possibilities also, including lowercase letters, digits, and so on. Most algorithms are more complex than the one in the children's example to avoid having to maintain a key that includes a value for each possible character.

The goal of encryption is that even if the algorithm is known, without the appropriate key, an intruder cannot interpret the message. This type of key is called a *secret key*. When both the sender and receiver use the same secret key, it is called a *symmetric key*. The Data Encryption Standard (DES) is the best known example of a symmetric key system. DES encryption is available for most routers and many server implementations.

Although secret keys are reasonably simple to implement between two devices, as the number of devices increases, the number of secret keys increases, which can be hard to manage. For example, a session between Station A and Station B uses a different key than a session between Station A and Station C, or a session between Station B and Station C, and so on. Asymmetric keys can solve this problem.

Public/Private Key Encryption

Public/private key encryption is the best known example of an asymmetric key system. With public/private key systems, each secure station on a network has a public key that is openly published or easily determined. All devices can use a station's public key to encrypt data to send to the station.

The receiving station decrypts the data using its own private key. Because no other device has the station's private key, no other device can decrypt the data, so data

confidentiality is maintained. Mathematicians and computer scientists have written computer programs that identify special numbers to use for the keys so that the same algorithm can be used by both the sender and receiver, even though different keys are used. Figure 8-1 shows a public/private key system for data confidentiality.

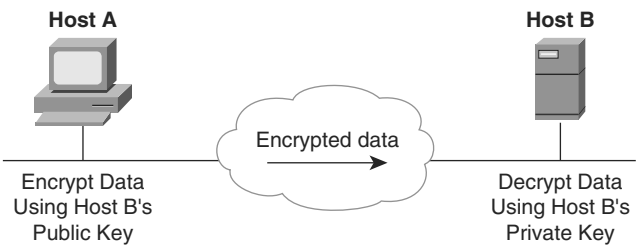


Figure 8-1 *Public/Private Key System for Ensuring Data Confidentiality*

Public/private key systems provide both confidentiality and authentication features. Using asymmetric keys, a recipient can verify that a document really came from the user or host that it appears to have come from. For example, suppose you are sending your tax returns to the Internal Revenue Service (IRS). The IRS needs to know that the returns came from you and not from a hostile third party that wants to make it look like you owe more than you do.

You can encrypt your document or a part of your document with your private key, resulting in what is known as a *digital signature*. The IRS can decrypt the document, using your public key, as shown in Figure 8-2. If the decryption is successful, the document came from you because nobody else should have your private key.

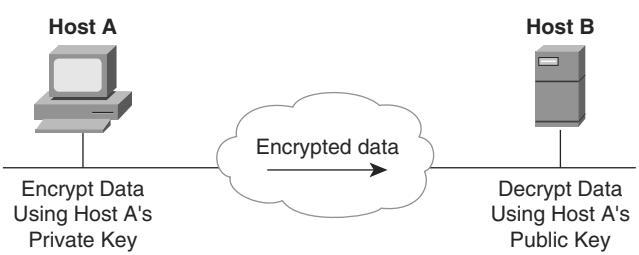


Figure 8-2 *Public/Private Key System for Sending a Digital Signature*

The digital signature feature of asymmetric keys can be used with the feature for data confidentiality. After encrypting your document with your private key, you can also encrypt the document with the IRS's public key. The IRS decrypts the document twice. If the result is plain-text data, the IRS knows that the document came from you and that you meant for the document to go to the IRS and not anyone else.

Some examples of asymmetric key systems include the Rivest, Shamir, and Adleman (RSA) standard, the Diffie-Hellman public key algorithm, and the Digital Signature Standard (DSS). Cisco uses the DSS standard to authenticate peer routers during the setup of an encrypted session. The peer routers use the Diffie-Hellman algorithm to send information on a secret key to use to encrypt data. The actual data is encrypted using the DES algorithm and the secret key.

Packet Filters

Packet filters can be set up on routers, firewalls, and servers to accept or deny packets from particular addresses or services. Packet filters augment authentication and authorization mechanisms. They help protect network resources from unauthorized use, theft, destruction, and DoS attacks.

A security policy should state whether packet filters implement one or the other of the following policies:

- Deny specific types of packets and accept all else
- Accept specific types of packets and deny all else

The first policy requires a thorough understanding of specific security threats and can be hard to implement. The second policy is easier to implement and more secure because the security administrator does not have to predict future attacks for which packets should be denied. The second policy is also easier to test because there is a finite set of accepted uses of the network. To do a good job implementing the second policy requires a good understanding of network requirements. The network designer should work with the security administrator to determine what types of packets should be accepted.

Cisco implements the second policy in its packet filters, which Cisco calls *access control lists (ACL)*. An ACL on a router or switch running Cisco IOS Software always has an implicit deny-all statement at the end. Specific accept statements are processed before the implicit deny-all statement. (The statement is implicit because the administrator does not have to actually enter it, although it is a good idea to enter it to make the behavior of the list more obvious.)

ACLs let you control whether network traffic is forwarded or blocked at interfaces on a router or switch. ACL definitions provide criteria that are applied to packets that enter or exit an interface. Typical criteria are the packet source address, the packet destination address, or the upper-layer protocol in the packet.

Because Cisco IOS Software tests a packet against each criteria statement in the list until a match is found, ACLs should be designed with care to provide good performance. By studying traffic flow, you can design the list so that most packets match the earliest conditions. Fewer conditions to check per packet means better throughput. Good advice for designing ACLs is to order the list with the most general statements at the top and the most specific statements at the bottom, with the last statement being the general, implicit deny-all statement.

Firewalls

As discussed in Chapter 5, a *firewall* is a device that enforces security policies at the boundary between two or more networks. A firewall can be a router with ACLs, a dedicated hardware appliance, or software running on a PC or UNIX system. Firewalls are especially important at the boundary between the enterprise network and the Internet.

A firewall has a set of rules that specifies which traffic should be allowed or denied. A *static stateless packet-filter firewall* looks at individual packets and is optimized for speed and configuration simplicity. A *stateful firewall* can track communication sessions and more intelligently allow or deny traffic. For example, a stateful firewall can remember that a protected client initiated a request to download data from an Internet server and allow data back in for that connection. A stateful firewall can also work with protocols, such as active (port-mode) FTP, that require the server to also open a connection to the client.

Another type of firewall is a *proxy firewall*. Proxy firewalls are the most advanced type of firewall but also the least common. A proxy firewall acts as an intermediary between hosts, intercepting some or all application traffic between local clients and outside servers. Proxy firewalls examine packets and support stateful tracking of sessions. These types of firewalls can block malicious traffic and content that is deemed unacceptable.

Intrusion Detection and Prevention Systems

An intrusion detection system (IDS) detects malicious events and notifies an administrator, using email, paging, or logging of the occurrence. An IDS can also perform statistical and anomaly analysis. Some IDS devices can report to a central database that correlates information from multiple sensors to give an administrator an overall view of the real-time security of a network. An intrusion prevention system (IPS) can dynamically block traffic by adding rules to a firewall or by being configured to inspect (and deny or allow) traffic as it enters a firewall. An IPS is an IDS that can detect and prevent attacks.

There are two types of IDS devices:

- **Host IDS:** Resides on an individual host and monitors that host.
- **Network IDS:** Monitors all network traffic that it can see, watching for predefined signatures of malicious events. A network IDS is often placed on a subnet that is directly connected to a firewall so that it can monitor the traffic that has been allowed and look for suspicious activity.

In the past a major concern with both IDS and IPS devices was the volume of false alarms that they tended to generate. A false alarm occurs when an IDS or IPS reports a network event as a serious problem when it actually isn't a problem. This false-alarm problem has been ameliorated by sophisticated software and services on modern IPS devices. Cisco IPS solutions, for example, include anomaly detection that learns about typical actual network traffic on a customer's network and alarms only upon deviation from that traffic.

Cisco also supports reputation filtering and global correlation services so that an IPS can keep up-to-date on global security trends and more accurately deny traffic from networks known to be currently associated with botnets, spam, and other malware.

Modularizing Security Design

Security experts promote the *security defense in depth* principle. This principle states that network security should be multilayered, with many different techniques used to protect the network. No security mechanism can be guaranteed to withstand every attack. Therefore, each mechanism should have a backup mechanism. This is sometimes called the *belt-and-suspenders approach*. Both a belt and suspenders ensure that trousers stay up. A networking example is to use a dedicated firewall to limit access to resources and a packet-filtering router that adds another line of defense.

As part of implementing security defense in depth, security design should be modular. Multiple methods should be designed and applied to different parts of the network, whether it be the Internet connection, the wireless infrastructure, or the remote-access component. Cisco provides a modular approach with its SAFE security reference architecture (described in Chapter 5).

In general, using a modular approach to security design is a good way to gain an understanding of the types of solutions that must be selected to implement security defense in depth. The next few sections cover security for the following modules or components of an enterprise network:

- Internet connections
- Remote-access and virtual private networks (VPN)
- Network services and management
- Server farms
- User services
- Wireless networks

Securing Internet Connections

Internet connections should be secured with a set of overlapping security mechanisms, including firewalls, packet filters, physical security, audit logs, authentication, and authorization. Internet routers should be equipped with packet filters to prevent DoS and other attacks. These filters should be backed up with additional filters placed on firewall devices. The Internet connection should be carefully monitored. Network and host IDS devices should monitor subnets, routers, and Internet-accessible servers to detect signs of attack or malicious network activity and identify successful breaches into the protected network.

A good rule for enterprise networks is that the network should have well-defined exit and entry points. An organization that has only one Internet connection can manage Internet

security problems more easily than an organization that has many Internet connections. Some large organizations require more than one Internet connection for performance and redundancy reasons, however. This is fine as long as the connections are managed and monitored. Departments or users who add Internet connections without coordination from corporate network engineers should not be tolerated.

A common risk associated with the Internet connection is reconnaissance threats from the Internet, whereby an attacker attempts to probe the network and its hosts to discover reachable networks, hosts, and services running on exposed hosts, and to develop a network map. To manage the risk of reconnaissance attempts, routers and first-line firewall devices should block all incoming connections, except those necessary to reach specific services on public servers or to complete a transaction started by a trusted client. The routers and firewalls should also block packets typically used for reconnaissance threats, such as pings.

When selecting routing protocols for the Internet connection and for routers that inject Internet routes into the interior network, you should select a protocol that offers route authentication such as Routing Information Protocol version 2 (RIPv2), Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), or Border Gateway Protocol, version 4 (BGP4). Static and default routing is also a good option because with static and default routing there are no routing updates that could be compromised.

When securing the Internet connection, Network Address Translation (NAT) can be used to protect internal network addressing schemes. As discussed in Chapter 6, "Designing Models for Addressing and Naming," NAT hides internal network numbers from outside networks. NAT translates internal network numbers when outside access is required.

Securing Public Servers

Most companies have a need for public servers that are accessible from the Internet. These include World Wide Web, File Transfer Protocol (FTP), Domain Name System (DNS), email, and e-commerce servers. Public servers should be placed on a demilitarized zone (DMZ) network that is protected from other networks via firewalls. DMZ networks were discussed in more detail in Chapter 5.

To protect public servers from DoS attacks, server administrators should use reliable operating systems and applications that have been patched with the most recent security fixes. Adding Common Gateway Interface (CGI) or other types of scripts to servers should be done with great care. Scripts should be thoroughly tested for security leaks.

Public servers should run firewall software and be configured for DoS protection. For example, the server should be configured to limit the number of connection establishments that can occur in a particular timeframe. Servers should also run software that can examine the content carried by application protocols so that the software can scan, and possibly eliminate, dangerous content such as viruses or mobile code. (*Mobile code* is software that can be transmitted across a network and executed on another device.)

If a customer can afford two separate servers, security experts recommend that FTP services not run on the same server as web services. FTP users have more opportunities for

reading and possibly changing files than web users do. A hacker could use FTP to damage a company's web pages, thus damaging the company's image and possibly compromising web-based electronic commerce and other applications. Security experts recommend never allowing Internet access to Trivial File Transfer Protocol (TFTP) servers, because TFTP offers no authentication features.

Email servers have long been a source for intruder break-ins, probably because email protocols and implementations have been around a long time and hackers can easily understand them. Also, by its very nature, an email server must allow outsider access. To secure email servers, network administrators should keep current on well-known bugs and security leaks by subscribing to mailing lists dedicated to security information.

DNS servers should be carefully controlled and monitored. Name-to-address resolution is critical to the operation of any network. An attacker who can successfully control or impersonate a DNS server can wreak havoc on a network. DNS servers should be protected from security attacks by packet filters on routers and versions of DNS software that incorporate security features.

Traditionally, DNS had no security capabilities. In particular, there was no way to verify information returned in a DNS response to a query. A hacker could hijack the query and return a counterfeit name-to-address mapping. Digital signatures and other security features are being added to the protocol to address this issue and other security concerns. Refer to RFC 4033, "DNS Security Introduction and Requirements," and its companion documents, RFC 4034 and RFC 4035, for more information.

Securing E-Commerce Servers

E-commerce servers are vulnerable to the same attacks that threaten all public servers, but a compromise of an e-commerce server results in more substantial loss because these servers hold highly confidential and sensitive customer and financial data. E-commerce servers are often targets of DoS attacks, directed at their operating systems or applications. E-commerce servers must be protected from DoS attacks with packet-filtering rules and rules that deny successive connection attempts in a short period of time. They should also be protected from attackers who want to compromise them to launch an attack on other servers, including other e-commerce servers.

In some network designs, e-commerce applications run on multiple servers. For example, an e-commerce application front-end web server accepts encrypted sessions from Internet clients, processes the requests, and queries a database server, which holds sensitive customer and financial data. For optimum protection of sensitive data, and to avoid a compromised server attacking another server, you can separate the servers into their own DMZ networks. For example, design the topology so that there is a firewall that protects the database server from the front-end web server, in case the web server is compromised. Servers on the same segment can also be separated by LAN switch access control

mechanisms (such as private VLANs). Network and host IDS devices should monitor subnets and individual servers to detect signs of attacks and confirm successful breaches.

Securing Remote-Access and VPNs

To support mobile users, many enterprise networks include remote-access technologies, VPN concentrators, and site-to-site VPN gateways. The users' data is sent over public networks, such as the Public Switched Telephone Network (PSTN) and the Internet, so protecting the data from eavesdropping is important. Protecting from identity spoofing of remote clients or sites is also important, to avoid an attacker impersonating a legitimate client and logging in to the network. This can happen if an attacker steals a legitimate user's credentials (such as a username and password pair) or learns the authentication keys used on a VPN connection.

Securing Remote-Access Technologies

Security is critical for remote-access technologies and should consist of firewall technologies, physical security, authentication and authorization mechanisms, auditing, and possibly encryption. Authentication and authorization are the most important features and can be implemented with the Challenge Handshake Authentication Protocol (CHAP) and the Remote Authentication Dial-In User Service (RADIUS) protocol.

Remote users and remote routers that use the Point-to-Point Protocol (PPP) should be authenticated with CHAP. The Password Authentication Protocol (PAP), which offers less security than CHAP, is not recommended. The "Remote-Access Technologies" section of Chapter 11, "Selecting Technologies and Devices for Enterprise Networks," covers PPP, CHAP, and PAP in more detail.

Another option for authentication, authorization, and accounting is *RADIUS*. Livingston, Inc., developed RADIUS, which has become an industry standard and is documented in RFC 2865. RADIUS gives an administrator the option of having a centralized database of user information. The database includes authentication and configuration information and specifies the type of service permitted by a user (for example, PPP, Telnet, rlogin, and so on). RADIUS is a client/server protocol. An access server acts as a client of a RADIUS server.

Dialup services should be strictly controlled. Users should not be allowed to attach modems and analog lines to their own workstations or servers. (Some companies actually fire employees who do this.) If some remote users still need to dial in to the network using a modem and analog telephone line, it's helpful to have a single dial-in point (for example, a single modem pool or access server) so that all users are authenticated in the same way. A different set of modems should be used for any dial-out services. Both dial-in and dial-out services should be authenticated.

There are many operational security considerations with dialup networks, and if possible, dialup networks should be eliminated from modern networks. If that is not possible,

modems and access servers should be carefully configured and protected from hackers reconfiguring them. Modems should be programmed to reset to the standard configuration at the start and end of each call, and modems and access servers should terminate calls cleanly. Servers should force a logout if the user hangs up unexpectedly.

If the modems and access servers support callback (which most do), callback should be used. With *callback*, when a user dials in and is authenticated, the system disconnects the call and calls back on a specified number. Callback is useful because the system calls back the actual user, not a hacker who might be masquerading as the user. Callback can easily be compromised, however, and should not be the only security mechanism used.

Securing VPNs

Organizations that use VPNs to connect private sites and end users via a public network such as the Internet should use NAT, firewalls, strong authentication, and data encryption. The client operating systems that connect via the VPN should use personal firewall and virus protection software. It is important to protect against a compromise of a client or remote site that allows an attacker to successfully attack the enterprise network over the VPN. An example is a VPN client that has been compromised by a Trojan horse that turns the client system into a relay. Such an attack could mean that when the client is connected to the enterprise network via an Internet remote-access VPN, the attacker can connect to the client over the Internet, and then from the client connect to the protected enterprise network.

In VPN topologies, private data travels across a public network, so encryption is a must. The most common solution for encryption is to use the IP Security Protocol (IPsec), which is an Internet Engineering Task Force (IETF) standard that provides data confidentiality, data integrity, and authentication between participating peers at the IP layer. IPsec provides a secure path between remote users and a VPN concentrator, and between remote sites and a VPN site-to-site gateway.

Numerous RFCs deal with Ipsec, and many Internet drafts. To learn IPsec better, the main RFCs you should read are as follows:

- RFC 4301, “Security Architecture for the Internet Protocol”
- RFC 4302, “IP Authentication Header”
- RFC 4303, “IP Encapsulating Security Payload (ESP)”
- RFC 4306, “Internet Security Association and Key Management Protocol (ISAKMP)”

IPsec enables a system to select security protocols and algorithms, and establish cryptographic keys. The Internet Key Exchange (IKE) protocol provides authentication of IPsec peers. It also negotiates IPsec keys and security associations. IKE uses the following technologies:

- **DES:** Encrypts packet data.
- **Diffie-Hellman:** Establishes a shared, secret, session key.
- **Message Digest 5 (MD5):** A hash algorithm that authenticates packet data.
- **Secure Hash Algorithm (SHA):** A hash algorithm that authenticates packet data.
- **RSA encrypted nonces:** Provides repudiation.
- **RSA signatures:** Provides nonrepudiation.

Securing Network Services and Network Management

To protect internal network services, it is important to protect internal internetworking devices, such as routers and switches. You should treat each network device as a high-value host and harden (strengthen) it against possible intrusions. This involves common practices such as running only the minimal necessary services and establishing trust only with authentic partners. For example, a router should not accept routing updates from a router that has not been authenticated. Routing protocols that support authentication should be selected, including RIPv2, OSPF, EIGRP, and BGP4. Static and default routes are also a good choice because they eliminate the need to accept routing updates.

Login IDs and passwords should be required for accessing routers and switches, whether the user accesses the device via a console port or via the network. A first-level password can be used for administrators that simply need to check the status of the devices. A second-level password should be used for administrators who have permission to view or change configurations. Avoid using a nonsecure protocol such as Telnet to access routers and switches over a network. A better choice is Secure Shell (SSH).

When administrators (or hackers posing as administrators) connect to a router or switch, they should not see the typical connect message, which often says something simple, such as Welcome to This Router. Instead, a router or switch should display warnings about authorized usage and the monitoring of all activity on the device. Many security experts recommend getting help from a lawyer when writing the connect message.

If modem access to the console ports of internetworking devices is allowed, the modems must be secured just as standard dial-in user modems are, and the phone numbers should be unlisted and unrelated to the organization's main number(s). The phone numbers should also be changed when there is staff turnover.

For customers with numerous routers and switches, a protocol such as the *Terminal Access Controller Access Control System (TACACS)* can be used to manage large numbers of router and switch user IDs and passwords in a centralized database. TACACS also offers auditing features, which can be helpful when an inexperienced network administrator tries to avoid responsibility for a misconfiguration that led to a security incident.

To protect against the misconfiguration of devices by hackers (or inexperienced network administrators), you can enforce authorization on specific configuration commands. TACACS and other authorization methods can be configured to permit only specific administrators to enter risky commands, such as commands to change IP

addresses or ACLs. The use of a well-managed, centralized change-control process is also recommended.

Limiting use of the Simple Network Management Protocol (SNMP) should be considered on enterprise networks for which security goals outweigh manageability goals. One of the main issues with SNMP is the **set** operation, which allows a remote station to change management and configuration data. If SNMPv3 is used, this is not as big a concern, because SNMPv3 supports authentication for use with the **set** operation and other SNMP operations.

Network management systems should be especially protected because they host extremely sensitive data about network and security device configuration. Moreover, network management systems are sometimes connected to other devices over a separate (out-of-band) management network, which, without careful design, could provide a path around security mechanisms such as firewalls.

To minimize risk, network management systems should be placed in their own DMZ behind a firewall. They should run a hardened operating system that has been patched with the latest security fixes. All unnecessary services should be disabled.

As is the case with routers and switches, network management systems must be protected from the impersonation of administrators, where an attacker steals the credentials (usernames or passwords) of an administrator. To manage the risk of administrator impersonation, provide the administrator with strong authentication mechanisms. A good example is a two-factor, one-time password system based on security cards.

Securing Server Farms

Server farms host file, print, database, and application servers inside campus networks and branch offices. These servers often contain an enterprise's most sensitive information, so they must be protected. Because servers are accessed by a large number of users, network performance is usually a critical issue, which can limit the choice of protection mechanisms. Nonetheless, methods should be deployed to protect against the compromise of exposed applications and unauthorized access to data. Network and host IDS devices should be deployed to monitor subnets and individual servers to detect signs of attacks and confirm successful breaches.

When servers in a server farm are compromised, attackers can use those servers to attack other servers. To manage this risk, configure network filters that limit connectivity from the server. In many cases, a server has no need to initiate connections. Connection establishments generally come from the client. There are numerous exceptions, however, which can be programmed into filters. For example, with active (port-mode) FTP, the server initiates a connection. Also, various network management, naming, resource-location, and authentication and authorization protocols might require the server to initiate a connection. As part of the top-down network design process, you should have analyzed the protocols present in server farm locations (see Chapter 3, "Characterizing the Existing Internetwork" and Chapter 4, "Characterizing Network Traffic" for more information). The data you gathered can help you determine which protocols a server will need to allow.

To maximize security, both server and end-user software should be carefully selected and maintained. Server and desktop administrators should be required to keep current as to the latest hacker tricks and viruses. Known security bugs in operating systems should be identified and fixed. In addition, application software should be selected based partly on its adherence to modern, secure programming practices. With the creation of safer high-level programming languages and increasing programmer awareness of security issues, many applications are available that are reasonably secure. Most stock software, which is still used by many businesses, is vulnerable to simple attacks to defeat its security, however.

For customers with stringent security requirements, server applications might incorporate encryption. This is in addition to any client/server encryption used to protect data traveling across a network. To protect against the unauthorized use of data, cryptographic methods can protect data on a disk drive. For example, the data on disk drives can be encrypted so that it can be read only by the proper application.

File and other servers should provide authentication and authorization features. Security policies and procedures should specify accepted practices regarding passwords: when they should be used, how they should be formatted, and how they can be changed. In general, passwords should include both letters and numbers, be at least six characters, not be a common word, and be changed often.

On servers, root password knowledge (or the non-UNIX equivalent) should be limited to a few people. Guest accounts should be avoided if possible. Protocols that support the concept of *trust* in other hosts should be used with caution (examples include rlogin and rsh on UNIX systems). Hosts that permit guest accounts and support trusted hosts should be isolated from other hosts if possible.

Kerberos is an authentication system that provides user-to-host security for application-level protocols such as FTP and Telnet. If requested by the application, Kerberos can also provide encryption. Kerberos relies on a symmetric key database that uses a key distribution center (KDC) on a Kerberos server.

Securing User Services

A security policy should specify which applications are allowed to run on networked PCs and restrict the downloading of unknown applications from the Internet or other sites. The security policy should also require that PCs have personal firewall and antivirus software installed. Security procedures should specify how this software is installed and kept current.

Users should be encouraged to log out of their sessions with servers when leaving their desks for long periods of time and to turn off their machines when leaving work, to protect against unauthorized people walking up to a system and accessing services and applications. Automatic logouts can also be deployed to automatically log out a session that has had no activity for a period of time.

One other aspect of securing the end-user part of a network is ensuring that users connect only permitted computers or other devices to the LAN interfaces in their offices. In particular, one area of concern is users who connect wireless access points that are not properly secured. These unauthorized access points are sometimes called *rogue access points*. Security for wireless networks, which is discussed in more detail in the next section, should not be left to end users. It should be carefully planned and implemented and not compromised by users installing their own wireless access points.

Cisco and other vendors support an IEEE standard called 802.1X, which provides port-based security on switch ports. With 802.1X enabled on a switch port, no device can connect to the network without first using 802.1X to authenticate. This is one method for ensuring that a user doesn't install an unknown device, such as a wireless access point. With this use of 802.1X, it is the access point that is authenticated. Another use of 802.1X is to authenticate wireless client devices, such as laptops. When a legitimate wireless infrastructure is in place, 802.1X is no longer needed on the ports that connect known access points, but it can be used to authenticate wireless users, as discussed later in the "802.1X with Extensible Authentication Protocol" section of this chapter.

Securing Wireless Networks

Wireless networks are gaining widespread popularity in enterprise campus networks, at branch offices, and in home offices. Most organizations support the increases in productivity and employee satisfaction that wireless networking offers but at the same time are concerned about the security risks, as they should be. In recent years, glaring holes have been discovered in the typical methods used for wireless security, resulting in the development of new methods and models for providing security on wireless networks. This section covers some overall design guidelines first and then includes information on the following two topics:

- Authentication in wireless networks
- Data privacy in wireless networks

As mentioned in Chapter 5, it is best to place wireless LANs (WLAN) in their own subnet and their own VLAN. This simplifies addressing for stations that roam and also improves management and security. Keeping all wireless clients in their own subnet makes it easier to set up traffic filters to protect wired clients from an attack launched on the wireless network. To maximize roaming flexibility, all WLANs can be a single VLAN and IP subnet, so that there is no need to retrieve a new IP address when moving from one area to another. To maximize security, however, it might be wiser to subdivide the WLAN into multiple VLANs and IP subnets.

Keep in mind that security requirements for wireless users vary with the type of user. Guests who visit an enterprise might need easy access to the Internet but should be prevented from accessing the enterprise network. These guests cannot be expected to know an encryption key or to have VPN software installed. This is different from the employ-

ees who want wireless access while having lunch in the cafeteria or while meeting in private conference rooms. Those users could be expected to know a key or to have the corporate-approved VPN software installed. The use of VLANs comes in handy here. When you understand the different user types and where they might roam, you can divide the WLAN into multiple VLANs and apply security policies separately for each VLAN.

You should implement ACLs on wireless access points and on wired switches and routers that carry traffic that originated on a wireless network. The ACLs should allow only specific protocols, in accordance with security policies.

All wireless (and wired) laptop computers should be required to run antivirus and personal firewall software. They should also be regularly updated with the most recent operating system security patches. Depending on security requirements, you might also want to require corporate wireless laptop users to use VPN software to access the enterprise network. The final section in this chapter, "Using VPN Software on Wireless Clients," discusses using IPsec VPN software as a security option for wireless networks.

Authentication in Wireless Networks

In a wired Ethernet LAN, a device must physically plug into the network to communicate. This fundamental feature of a wired Ethernet is not present in the realm of wireless networking, however. There is nothing to plug in. The IEEE 802.11 standard provides a method for devices to authenticate to a wireless access point, thus emulating the basic security provided by a wired network where a user must have physical access to a port to communicate.

Authentication takes place after a wireless client has located an access point with a sufficiently strong signal and selected a channel. The 802.11 client initialization process consists of the following steps:

Step 1. The client broadcasts a Probe Request frame on every channel.

Step 2. Access points within range respond with a Probe Response frame.

Step 3. The client decides which access point is the best for access and sends an Authentication Request frame.

Step 4. The access point sends an Authentication Response frame.

Step 5. Upon successful authentication, the client sends an Association Request frame to the access point.

Step 6. The access point replies with an Association Response frame. The client can now pass traffic to the access point.

IEEE 802.11 specifies two forms of authentication: *open* and *shared key*. With open authentication, the client is always authenticated as long as the access point has been configured to allow open authentication. This is the default mode for most systems. Open authentication can be thought of as null authentication. The client asks to be authenticated

and the access point permits the authentication. It might sound pointless to use such an algorithm, but open authentication has its place in 802.11 networks. Open authentication is often used for guest access, where it would be impractical to provide users with a key. Also, many 802.11-compliant devices are handheld data-acquisition units, such as bar-code readers. They do not have the CPU capabilities required for complex authentication algorithms.

With shared key authentication, a Wired Equivalent Privacy (WEP) static key must be properly configured in both the client and the access point. The steps for shared key authentication are as follows:

Step 1. The client sends an Authentication Request to the access point requesting shared key authentication.

Step 2. The access point responds with an Authentication Response containing challenge text.

Step 3. The client uses its locally configured WEP key to encrypt the challenge text and replies with another Authentication Request.

Step 4. If the access point can decrypt the Authentication Request and retrieve the original challenge text, the client must be using the correct WEP key, so the access point responds with an Authentication Response that grants the client access.

In August 2001, cryptanalysts Fluhrer, Mantin, and Shamir determined that a WEP key can be derived by passively collecting particular frames from a wireless LAN. Researchers at AT&T and Rice University and the developers of the AirSnort application implemented the vulnerability and verified that either 64- or 128-bit WEP keys can be derived after as few as 4 million frames. For high-usage wireless LANs, this translates to roughly 4 hours until a 128-bit WEP key can be derived.

In addition to WEP's vulnerability to passive attacks, WEP is also vulnerable to inductive key derivation, which is the process of deriving a key by coercing information from the wireless LAN. Man-in-the-middle attacks, a form of inductive key derivation, are effective in 802.11 networks because of the lack of effective message integrity. The receiver of a frame cannot verify that the frame was not tampered with during its transmission.

The shared WEP key, as specified by IEEE 802.11, is a static key. If the key is discovered by an unauthorized user, it must be changed on access points and every individual client. Attackers can discover the key in many ways, including eavesdropping on numerous packets, but also by using simpler methods, such as asking naive users for the key or stealing users' laptop computers where the key is configured.

The 802.11 specification stipulates only the two mechanisms for authenticating wireless devices that have already been discussed: open authentication and shared key authentication. Other mechanisms that are also commonly used include setting an unpublished Service Set Identifier (SSID), authenticating devices by their client Media Access Control

(MAC) address, and using 802.1X with the Extensible Authentication Protocol (EAP). These are described in the next three sections.

Using an Unpublished Service Set Identifier

Every WLAN has an SSID that identifies it. To gain access to a wireless LAN, a client must know the correct SSID. Some network administrators rely on this as a method for security even though it doesn't truly authenticate the client and doesn't provide any data privacy. Also, an eavesdropper can easily determine the SSID with the use of a wireless protocol analyzer. The SSID is advertised in plain text in beacon messages that the access point sends.

Some access point vendors, including Cisco, offer the option to disable SSID broadcasts in beacon messages, but this does not offer much protection. The SSID can still be determined by analyzing Probe Response frames from an access point. Also, disabling SSID broadcasts might have an adverse effect on wireless interoperability for mixed-vendor deployments. Therefore, most experts do not recommend using the SSID as a mode of security.

MAC Address Authentication

MAC address authentication verifies a client's MAC address against a configured list of allowed addresses. MAC address authentication is used to augment the open and shared key authentications provided by 802.11, further reducing the likelihood of unauthorized devices accessing the network. Depending on the access point, the list of MAC addresses might be locally configured on the access point, or the access point might use an authentication protocol such as RADIUS and an external authentication server. A server is helpful for large installations where configuring individual access points would be difficult. If a server is used, redundancy must be considered so that the server does not become a single point of failure.

MAC addresses are sent as clear text per the 802.11 specification. As a result, in wireless LANs that use MAC address authentication, a network attacker might be able to subvert the MAC authentication process by spoofing a valid MAC address. Network attackers can use a protocol analyzer to determine valid MAC addresses that are being used in the network and change their own wireless NICs to use that address (on NICs that support changing the MAC address).

MAC address authentication is labor-intensive. A network administrator must know the address of every allowed NIC and configure this into the access point or server. Also, as mentioned, hackers can get around MAC address authentication by changing their own address to match an allowed address. Therefore, most experts do not recommend relying on MAC address authentication as the only mode of security.

802.1X with Extensible Authentication Protocol

IEEE 802.1X specifies a method for authenticating and authorizing a device attached to a LAN port. It is used on both wired switches and on wireless access points (where the "attachment" is not physical). 802.1X provides optional support for use of an authentication server, such as a RADIUS server, which is recommended for larger installations.

802.1X is extensible and supports a variety of authentication algorithms. The most common are varieties of EAP, which is an IETF standard, documented in RFC 2284. With 802.1X and EAP, devices take on one of three roles:

- The supplicant resides on the wireless LAN client.
- The authenticator resides on the access point.
- An authentication server resides on a RADIUS server.

When 802.1X and EAP are implemented, a client that associates with an access point cannot use the network until the user is authenticated. After association, the client and the network (access point or RADIUS server) exchange EAP messages to perform authentication. An EAP supplicant on the client obtains credentials from the user, which could be a user ID and password, a user ID and one-time password, or a digital certificate. The credentials are passed to the authenticator or server and a session key is developed.

With 802.1X and EAP, session timeouts force a client to reauthenticate to maintain network connectivity. Although reauthentication is transparent to the client, the process of reauthentication generates new WEP keys at every reauthentication interval. This is important for mitigating statistical key derivation attacks and is a critical WEP enhancement. One disadvantage of 802.1X with EAP, however, is that reauthentication can cause some delay, when compared to using a static WEP key. This might cause a problem for users that roam with delay-sensitive devices, such as 802.11 phones.

Note that EAP authenticates users. Whereas 802.11 authentication is device-based, EAP is based on authenticating a user rather than a wireless LAN device. This avoids the problems caused by theft of a laptop computer using a static WEP key, which would allow the thief access to the network and would probably result in a network administrator needing to change the WEP key on the affected access points and all clients. EAP generates unique keying material for each user. This relieves network administrators from the burden of managing static keys. EAP also supports mutual authentication, which allows a client to be certain that it is communicating with the intended authentication server.

Selecting the right EAP implementation can be a challenging process due to the large number of options. The funny-sounding names, such as LEAP and PEAP, don't help matters. You must get this right though. The supplicant, authenticator, and authentication server must all support the same variety of EAP, which is mostly likely one of the following:

- **Lightweight EAP (LEAP):** Developed by Cisco and is sometimes called *EAP-Cisco*. Cisco licenses LEAP to other vendors, including Apple Computer and Intel. LEAP supports user-based authentication and dynamic WEP keys that are generated after authentication and when session timeouts occur. User authentication is based on a user's Windows logon, which means the user does not have to supply additional logon information to access the wireless network, which makes LEAP easy to use. LEAP supports mutual authentication, which means that the client authenticates the server and the server authenticates the client. This is important for ensuring that the client talks to an authorized server and not a hacker posing as a server.

- **EAP-Transport Layer Security (EAP-TLS):** Developed by Microsoft and is documented in RFC 2716. Microsoft supports EAP-TLS in all versions of Windows XP and has released a free Windows 2000 client. Like LEAP, EAP-TLS supports mutual authentication, dynamic keys, and session timeouts. EAP-TLS requires certificates for clients and servers. Because of this, some users consider Microsoft's EAP to be more secure than other EAPs. However, the certificate requirement also means EAP-TLS needs certificate management, such as the use of a trusted certificate authority and the ability to quickly revoke certificates.
- **EAP-Tunneled TLS (EAP-TTLS):** Developed by Funk and Certicom and then turned over to the IETF, where it is currently (as of this writing) a standards-based Internet draft. EAP-TTLS is an enhancement of EAP-TLS, with support for advanced authentication methods such as token cards. A variety of vendors have signed on to support EAP-TTLS.
- **Protected EAP (PEAP):** Supported by Cisco, Microsoft, and RSA Security. Like LEAP and EAP-TLS, PEAP supports mutual authentication, dynamic keys, and session timeouts. PEAP uses a certificate for the client to authenticate the RADIUS server. The server uses a one-time password or a username and password to authenticate the client. When the client validates the server's certificate, it builds an encrypted tunnel and then uses EAP in the tunnel to authenticate. PEAP is more manageable and scalable than EAP-TLS. Organizations can avoid installing digital certificates on every client machine, as required by EAP-TLS, and select the method of client authentication that best suits them.
- **EAP-MD5:** Has no key management features or dynamic key generation. Although EAP-MD5 is supported on many platforms, it will probably be phased out of most wireless networks because it has few benefits over WEP.

Data Privacy in Wireless Networks

Previous sections discussed methods for authenticating a wireless device (or the user of a wireless device). Another important requirement for wireless networks is data privacy. The original IEEE 802.11 standard specified WEP as the method for encrypting data to meet privacy requirements. Unfortunately, WEP has been shown to be ineffective as a data-privacy mechanism because of the many ways of compromising it. Cisco and other vendors implemented many enhancements to WEP, which IEEE standardized as part of its IEEE 802.11i standard.

One set of enhancements that addresses the shortcomings with WEP is known as the Temporal Key Integrity Protocol (TKIP). TKIP provides the following:

- A message integrity check (MIC), which provides effective frame authenticity to mitigate man-in-the-middle vulnerabilities
- Per-packet keying, which provides every frame with a new and unique WEP key that mitigates WEP key derivation attacks

In addition to TKIP, the IEEE recognized the need for stronger encryption mechanisms and adopted the use of the Advanced Encryption Standard (AES) for the data-privacy section of the 802.11i standard. The development of AES was facilitated by the National Institute of Standards and Technology (NIST), which solicited the cryptography community for new encryption algorithms. The algorithms had to be fully disclosed and available royalty free. The NIST judged candidates on cryptographic strength as well as practical implementation. The finalist, and adopted method, is known as the Rijndael algorithm. The Rijndael algorithm provides for a variety of key sizes, including 128, 192, and 256 bits.

Wi-Fi Protected Access

Another development that is related to 802.11i and wireless security is Wi-Fi Protected Access (WPA). WPA is a subset of the 802.11i standard that was adopted by the Wi-Fi Alliance. The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless products based on IEEE 802.11 specifications.

The Wi-Fi Alliance introduced WPA because 802.11i was not ratified yet and also because 802.11i was expected to include specifications that would eventually require hardware upgrades for some devices. The Wi-Fi Alliance decided to introduce a subset of the specification that was stable and could be achieved via software upgrades.

WPA uses 802.1X with EAP for authentication and TKIP for data encryption. For enterprise networks, WPA should be used with an authentication server, such as a RADIUS server, to provide centralized access control and management. In small and home offices, WPA allows the use of manually entered keys or passwords. The small or home office user enters a password (also called a *master key* or a *preshared key*) in the access point and each client, and WPA takes over from there. The password ensures that only devices with a matching password can join the network. Entering a correct password also starts the TKIP encryption process.

In some configurations, a WPA1 option is distinguished from a WPA2 option. WPA1 uses TKIP and predates 802.11i. WPA2 uses AES and is compatible with 802.11i. Another distinction is WPA Personal versus WPA Enterprise. WPA Personal uses preshared keys and is appropriate for home or small office networks. WPA Enterprise uses a RADIUS server and is appropriate for larger business networks.

Using VPN Software on Wireless Clients

Although EAP and WPA solve many of the problems with WEP, they can be difficult to implement, especially in multivendor environments. Another option for customers with a strong need to protect data confidentiality is to use VPN software on the wireless clients. With this solution, the clients reach the campus network by connecting to a VPN concentrator. VPN software that uses IPsec has many advantages, including Triple Data Encryption Standard (3DES) encryption, one-time password support, and support for per-user policies.

When VPN software is installed, WLAN clients still associate with a wireless access point to establish connectivity at Layer 2. The clients then establish connectivity at Layer 3 using DHCP and DNS. The clients establish a VPN tunnel to a VPN concentrator to securely communicate with the campus network.

The wireless network should be considered an untrusted network, suitable only as a transit network for IPsec traffic once a VPN tunnel has been established. To isolate the untrusted wireless network, administrators should place the WLAN users in their own VLAN. The wireless clients should also run personal firewall software to protect them while they are connected to the untrusted WLAN network without the protection of IPsec.

Another protection mechanism is a feature called *Publicly Secure Packet Forwarding (PSPF)*, which prevents WLAN clients on the same access point from communicating with each other (or attacking each other). PSPF provides Internet access to clients without providing other typical LAN services, such as the capability to share files.

To minimize security threats, you should configure the wireless access point to allow only the protocols required for establishing a secure tunnel to a VPN concentrator. These protocols include DHCP for initial client configuration, DNS for name resolution, and IPsec VPN-specific protocols—IP protocol 50 for ESP and UDP port 500 for IKE. (The DNS traffic is necessary only if the VPN client accesses the VPN gateway by name.)

Despite the assurance of data privacy that IPsec provides, an IPsec VPN solution for wireless security has some disadvantages. For example, some VPN software requires the user to start the software and provide additional logon information before accessing the campus network. Roaming from one area to another might require the acquisition of a new IP address or a mobile IP solution. Also, when 3DES encryption is provided in software, users may notice a performance degradation.

In general, IPsec VPN in a wireless network has the same disadvantages that it has in wired networks, including diminished ease of use and performance, configuration complexity, the need for local software to be installed on the client computers, interoperability problems with various applications, the lack of support for multicast applications, and the fact that IPsec is an IP-only solution. Also, handheld devices, including 802.11 phones, might not support IPsec.

Understanding the needs of the various user communities and their applications will help you decide whether IPsec should be required instead of (or in addition to) the wireless security measures discussed in the previous sections. Determining the size of wireless user communities and the traffic volume they will generate is also important. Many VPN solutions were designed to handle a small number of remote users rather than a large number of transient wireless users. An analysis of traffic flow and volume may be necessary to determine if a VPN solution will scale to support your wireless users.

Summary

This chapter provided information to help you select methods for meeting a customer's goals for network security. Security is a major concern for most customers because of the increase in Internet connectivity and Internet applications, and because more users are accessing enterprise networks from remote sites and wireless devices. Also, at the same time that enterprises have become more dependent on their networks, the number of attacks on networks has increased.

The tasks involved with security design parallel the tasks involved with overall network design. It is important to analyze requirements, develop policies, and consider tradeoffs before selecting actual technologies and products to meet the security needs of the various users of an enterprise network. The network should be considered a modular system that requires security for many components, including Internet connections, remote-access networks, network services, end-user services, and wireless networks. To protect the network, you should develop multilayered strategies, procedures, and implementations that provide security defense in depth.

Review Questions

1. What is the difference between a security plan and a security policy? How do these two relate to each other?
2. People who are new to security often assume that security simply means encryption. Why is this a naive assumption? What are some other aspects of security that are just as important as encryption?
3. List and briefly describe four tradeoffs that often must be made in order to achieve good network security.
4. Research a case that has been in the news in the last few years where a major security breach occurred on a wireless network. Find a case where attackers got in via the wireless network but then penetrated farther into the network, resulting in severe economic or political damage to the victim organization. Write two or three paragraphs about what you found.

Design Scenario

In previous chapters you have been asked to do some design work for ElectroMyCycle. Throughout this process you have kept security requirements in mind, of course, but now the time has come to focus on security.

1. What are ElectroMyCycle's most important assets that must be protected with security mechanisms?
2. What are the biggest security risks that ElectroMyCycle faces?
3. Design a high-level security policy for ElectroMyCycle.
4. Describe how you will achieve buy-in from the major stakeholders for your security policy.

Index

Numerics

A

B

C

D

E

F

G

H

I

J-K-L

M

N

O

P

Q

R

S

T

U

V

W

X-Y-Z