CISSP Study Group

Communications and Network Security

Presented by Duane Harrington CISSP #27890

OSI Model

7	**Application**	FTP, Browser, Directory Services, WEB services
6	**Presentation**	View of the data, either Human or Application
5	**Session**	Directory and Access services
4	**Transport**	Technology and Implementations
3	**Network**	Concepts and Architecture, WAN Technologies
2	**Data-Link**	Ethernet, Concepts and Technologies, Encryption
1	**Physical**	Cable, Wire, Fiber Optics, Wi-Fi, Cellular

Layer 1

1 **Physical,**
Wire, Cable, Fiber Optics, Wi-Fi, Cellular

Network Topology

Star Wired, Today's Ethernet

Serial Coaxial Cable (Cable TV)

Fiber Optics, High Speed long distance media

Wi-Fi, Nearly Ubiquitous Wireless Computer network Technology

Cellular

Star Wired, Today's Ethernet

Standardized By IEEE

Category 3, 5 & 6 Unshielded Twisted Pair (UTP)

The standards establish the distance and achievable bandwidth of wired LAN connections

Category 1	Less than 1Mbps	Analog phone cable
Category 2	<4Mbps	4Mbps IBM Token Ring
Category 3	16Mbps	10 Base T Ethernet
Category 4	20Mbps	16Mbps Token Ring
Category 5	100 Mbps	100 Base TX & Asynchronous Transfer Mode
Category 5e	1,000 Mbps	100 Base T Ethernet
Category 6	1,000 Mbps	100 Base T Ethernet

Can be Eavesdropped on, it is Unshielded

Serial Coaxial Cable (Cable TV)

Shielded COAX is available in many cities and localities in the US

High speeds can be achieved by Bonding the Channels together.

Each TV channel uses a 2Mbps space in the available frequencies. This is established by the Head End. The Head End can establish a huge number of frequency combinations for many uses.

Closed Circuit TV, Internet Access, and a multitude of entertainment uses.

Very Robust, operates over long distances
Difficult and expensive to install
Shielded more difficult to eavesdrop on

Fiber Optics, High Speed long distance media

Fiber optics Today take 2 basic Forms.

Multi-Mode, 50 to 100 microns in diameter
- Relatively short fiber runs
- Light Emitting Diode (LED) driven

Great for use on campuses and Multi floor Buildings.

Single-Mode, 10 Microns in diameter
- Long runs, 25 Miles before regeneration
- Laser Driven

Used for Network trunking world wide

Can’t be eavesdropped on without breaking into the cable

Wi-Fi, Nearly Ubiquitous Wireless Computer Network Technology

Many evolving transmission technologies and standards

This Wi-Fi technology space is changing at a phenomenal pace.

There are constantly more data centric capabilities in this technology.

Each new version of Smartphone has significantly more data usage.

There is an inherent security vulnerability with this technology.
It is broadcast publically.

Any determined attacker could intercept the broadcast and then decode it later
Many of the standards have increasing encryption and privacy capabilities.

Cellular

There is increasing use of cellular for data communications.

I use a Hotspot myself.

Global Service for Mobile Communications (GSM) is the most popular Cellular signaling Technology in the world.

Each channel supports 8 callers using Time Division Multiplexing.

Many of the same vulnerabilities that Wi-Fi has Cellular shares.

It is broadcast

Cell SIM cards can be cloned and then easily intercepted.

The instructions are available over the Internet.

General Layer 1 Technology

All Physical Layer 1 equipment uses Patch panels for connections, terminations And media Conversions. i.e. Copper to Fiber for trunking.

- Patching is how an Ethernet Connection arrives at your desk.
- Your desk's data jack is run with many others to an equipment room, often called a closet.
- Inside the closet are many connections that are Patched together in a very organized manner to provide various capabilities to a desk.
- This also applies to Fiber Optics

There are also many devices that extend or amplify layer 1 Cabling.
Repeaters, Multiplexors(MUX) or media boosters.

Layer 2

2 **Data-Link**
Ethernet, Concepts and Technologies, Encryption

Ethernet, as we know it today, is an IEEE standard. 802.3
There are several other Data Link technologies that have lost favor.
Token Ring, Token Bus, FDDI, ATM etc.

Ethernet is a Collision Sensed Multiple Access/Collision Detected (CSMA/CD) Network signaling architecture. Yes, current LAN switches operate in Full Duplex Mode. This means that one host and one network device are the only things on a given segment. There aren't any collisions because there are only 2 possible nodes.

Layer 2 Communications

At Layer 2, there is only one network. The only network is the one that the node is Physically connected to.

At Layer 2, each device that is on the network broadcasts it's address.

An Ethernet Address looks like this;
08:00:20:0d:52:54 48 bits, hexadecimal, Identifies the manufacturer.

You will see this address format in Wi-Fi, Fiber Optics and others.

Either directly or via the LAN switches each Host is said to learn its neighbors addresses. This process builds an Address Resolution Protocol (ARP) table for use by higher Layer activities.

Layer 2 Encryption

There are several hardware encryption solutions that occur at Layer 2.

Extensible Authentication Protocol has several variants, these are used for authentication.

EAP-TLS (Transport Layer Security)
EAP-TTLS (Tunneled Transport Layer Security) No Certificates
EAP-PEAP (Protected EAP) No client Certificate

Point to Point Protocol (PPP) This is for serial line connectivity.

Password Authentication Protocol (PAP) Transmits in Plaintext

Challenge Handshake Authentication Protocol (CHAP) MD5

Layer 2 Wi-Fi

There are several IEEE standards that deal exclusively with Wi-Fi

IEEE 802.11b, ratified 1999 CSMA/CD & DSSS 2.4Gb band
IEEE 802.11a, ratified 1999 5Gb band
IEEE 802.11g, ratified 2003 Combined the 2 frequency bands
IEEE 802.15.1, Bluetooth Short range communication Blue jacking

Wired Equivalent Privacy (WEP) This uses a CRC-32 checksum Transmission for encryption with a shared secret and initialization Vector then it's encrypted using RC4. Due to flaws in RC4 this is easily decrypted by an attacker.

Wi-Fi Protected Access (WPA) This is an improved release of RC4 with 128 bit key. WEP's 32 bit checksum was replaced a Message Integrity Check 'Michael'

Wi-Fi Protected Access 2 (WPA2) This included Advanced Encryption Standard (AES)

Layer 2 Risks

The Layer 2 vulnerabilities are mostly Physical.

Unauthorized LAN Insertion
Unauthorized Closet changes
Power

Layer 3 Network

LAN, Local Area Network Geographically small network *i.e.* Your home, a single office Building a Local Campus.

This where the concept of multiple networks 1st appears.

LAN connectivity is confined to the length of the cables or local Fiber Optics.
All LAN connectivity requires Layer 2 underlying protocols
VLAN, Virtual Local Area Networks, A group of like users defined by software
From the perspective of the higher Layers LAN and VLAN are the same
LAN connectivity requires human presence. It has to be plugged in.
VLAN can be administered from anywhere. It is software.

Today's Ethernet Switches are very powerful. They can work at Layer2 or 3
A switch is required to establish VLANs

Layer 3 Network

Wide Area Network (WAN)

Public Switched Telephone Networks (PSTN) This was originally designed for switched Analog Voice communication.

When a call is made, the callers seem to be on dedicated lines to each other. In fact they are talking across a very complex network.

To accommodate the vast number of simultaneous call, the calls are trunked via the toll office, the toll offices are connected via fiber optic trunks.

Early Long Distance data communications utilized the PSTN and modems. The modems interfaced the data equipment to the analog network. As more bandwidth was required the analog phone lines were combined into Data Service Circuits, DS0 is 64Kb, DS1 is 1.544Mb (T1) CSU\DSU's replaced modems on these Data Service Circuits. 24 DS0's combine to be a DS1.

A fractional T1 is a group of DS0's aggregated. Less than 24

Digital Subscriber Loops (DSL) are used were they can be provisioned.

12,000 ft to 18,000 ft depending

Layer 3 Network

We have established LANs, High speed, small geographic area, many hosts.
WANS, Lower speeds, long distance capable, limited connections.

Layer 3 is where the different types of networks can be connected to form an internetwork.

Layer 3 requires the use of a device called a router. A router's job is to forward data traffic between multiple dissimilar networks.

In today's world the router uses software to do many tasks around the Job of forwarding data traffic. Yes I know VOIP too.

TCP\IP

Transmission Control Protocol\Internet Protocol.

TCP is said to be a reliable transport protocol. This means that every transmitted packet is sequenced and acknowledged by the destination.
Packet 2 doesn't leave if packet 1 hasn't been acknowledged.
Highly reliable, less performance.

IP is a high speed, unreliable protocol. IP transmits data with no Acknowledgements. User Datagram Protocol is the most widely used IP protocol.

Why would you ever employ one of these over the other?

IP Addressing

This is called dotted decimal notation. Decimal numbers separated by dots.

Class A 1-127.0.0.0 Network # 1 Octet, 16,777,216 addressable hosts
i.e. 14.0.0.0
Class B 128-191.xxx.0.0 Network # 2 Octets 65,536 addressable hosts
i.e. 135.1.0.0
Class C 192-223.xxx.xxx.0 Network # 3 Octets 256 addressable hosts
i.e. 200.100.22.0
Class D 224.239.0.0.0 Multicast
Class E 240-255.0.0.0 Reserved

This is IP Version 4, (IPV4) It is governed by
American Registry for Internet Numbers (ARIN)

IPV6

IPV6 is available and organizations are implementing it, mostly in Europe.

Cisco talks about The **Internet of Things (IOT)** every street lamp, traffic light, automobile, home appliance and electronic device will have an IPV6 address.

IPV6 uses 128 bit address space, 4 orders of magnitude more than V4.
1 to 128th is said to be enough to address every grain of sand.

Improved Security IPSec must be implemented in V6. This will help to ensure integrity and confidentiality.

A more concise packet header will require less processor time.

Improved Quality of Service

Intranet

Intranet is a network of interconnected internal Networks.

Layer 3 allows members of the intranet to work almost as if they are on the network.

An Intranet can extend from A city or Metro area to internationally.

Extranet

Extranet allows the sharing of Data Resources with business Partners.

There are many Security issues with Extranets. Target

DHCP, DDNS & Active Directory

Dynamic Host Configuration Protocol reaches full potential only with Layer 3

Dynamic Domain Name Services combined with Microsoft's Active Directory

These 3 Technologies are the foundation of the nearly seamless connectivity that we all enjoy today.

I can undock my Laptop from my desk and walk around the building. My IP address changes to a WiFi address, the DNS entry changes and Active Directory manages it all.

I don't drop a session and rarely have any issues at all.

Routers

Routers forward packets to other neighboring networks

They read the destination address and based on the Routers view of the network it forwards the packet to the next hop.

Routers can be used to interconnect different technologies, *i.e. Token Ring*

Routers keep track of their neighboring networks via a routing protocol.

RIP and RIP2

OSPF and OSPFv3

EIGRP and EIGRP IPV6

Firewalls

Firewalls enforce administrative security policies.

This is done by filtering all traffic based on a set of rules.

Firewalls should be placed between entities that have different trust domains.

Between the Internet and the DMZ as well as between the DMZ and the Rest of the enterprise.

Firewalls can be fiendishly complex to administer and manage.

It's not uncommon for this management to be outsourced.

Security Services

Network Address Translation (NAT) Firewalls can change the source address of An outgoing packet (From Trusted to Untrusted) or non-routable to Routable RFC1918

Also some organizations prefer to hide their enterprise behind translated addresses.

Port Address Translation (PAT) an extension of NAT, translates all addresses to a single IP Address uses the port number to keep track of the session.

Static Packet Filtering; this means that every packet is compared against the set of rules
i.e. Block all packets with port 69 (ICMP) High performance not dynamic.

Stateful Inspection; the packets are examined in the context of the current session
i.e. FTP, port 21 might be blocked but the FTP client requests a port above 1023.

Proxies; A proxy is used to provide services while hiding the network details behind it.
To a user it appears that they are communicating with an untrusted service

Layer 3 Risks and Attacks

The best Layer 3 defense is to keep current on all the patches and versions.
Let the vendors help you.

Virtual Private Networks (VPN) is an encrypted tunnel between to hosts. This allows For encrypted secure communications over untrusted networks. NAT has issues

Authentication Headers is used to prove the identity of the sender and ensure integrity. Replay attacks are prevented by the sequence number. You can't replay a previous number.

Encapsulating Security Payload (ESP) Plain text headers, encrypted data payload.

SSLVPN has advantages over IPSec, it's easier to implement. Used with any browser.

Tunneling has come under much scrutiny recently

Internet control Message Protocol (ICMP) aka Ping many different attacks

Scanning, Port scanning is the act of probing for available TCP/IP services.

Layer 4 Transport

Layer 4 provides data communications between hosts.
It is concerned with the Payload.

All addressing to layer 3, all data processes to Layer 5 and above.

Transmission Control Protocol (TCP) is mapped by port numbers.

Internet Assigned Number Authority (IANA) has assigned a total of 65,536 IP ports. 0/TCP…65536/TCP

Well known ports 0-1023 are assigned by IANA

Registered Ports, By Application 1024-49151 by application developers

Dynamic ports 49152-65535 are freely available.

Layer 4 Risks

IP port scanning is done to provoke a SYN response.
If any numbered port responds with a SYN the attacker knows it is available.

TCP Sequence Number Attacks; To detect and correct loss of data packets
TCP numbers transmitted packets sequentially. Any packet not in sequence will be Re-transmitted. It is not difficult to guess the next sequence number.

Session Hijacking; IP Spoofing and Man in the Middle replacing legitimate packets with the attackers own.

Denial of Service (DOS), or Distributed Denial of Service (DDOS). Typically this done by An attack against the initial TCP handshake. Either a single source SYN Flood or In today's world an attack from many BOTS with a single target.

Layer 5 Session

Layer 5 provides logical persistent connection between peer hosts.
Directory Services which identify objects between hosts.

Remote Procedure Call (RPC) the way to execute objects across hosts.
NFS Sun's implementation Mapped or Mounted Drives
Common Object Request Broker Architecture CORBA
Microsoft's Distributed Component Object Model DCOM
RPC has many vulnerabilities Mostly weak authentication

Domain Name Service (DNS) Many vulnerabilities have been addressed over time.
DNS remains a very key and visible entity. IPV6 makes DNS more robust.

Layer 6 Presentation

Data presentation both to applications and humans may seem less relevant from a security perspective.

The Presentation Layer is pertinent to compression and encryption.

Transport Layer Security (TLS) lives at Layer 6

SSL encryption for HTTP connections, Server Authentication and key exchange.

Many RFC's

Layer 7 Application

Simple Mail Transfer Protocol (SMTP)
Post Office Protocol (POP & POP3)
Network News Transfer Protocol (NNTP)
Instant Messaging
Extensible Messaging and Presence Protocol (XMPP)
Internet Relay Chat (IRC)
All kinds of vulnerabilities

Data Exchange and Transfer Services
File Transfer Protocol (FTP) secure reliable file applications uses TCP
Trivial File Transfer Protocol (TFTP) uses UDP
HyperText Transfer Protocol (HTTP) port 80 Changed the World
Secure HyperText Transfer Protocol (HTTPS) port 443
Peer to Peer Applications and Services; usually tunneled

Communications and Network Security

Converged Protocols

What is IP Convergence?

- Network and Security practitioners have long wanted a Network capable of transferring Data and Voice seamlessly and securely.
  - The core aspects are that; It should be up to date

    With the capacity and capabilities today's Enterprises require.

    Security is vital to success

1. Support and connectivity for multi-media tasks
2. Single platform, Desktops, networks, routers, access control & Firewalls.
3. Simple management, uniform setup and user training.
4. The flexibility to dynamically collaborate and make decisions.
5. IP networks have proven to be remarkably scalable
6. Service differentiation and QoS based routing, with redundancy.
7. Fewer manageable components for the elimination of parallel networks.
8. Business applications have varying tolerance for network delay, QoS reflects these requirements.
9. Standard device integration has the potential to simplify end to end management and security.
10. Cost savings at every level, Space and power utilization, increases in mobility and productivity.

Implementation

A converged IP network provides capacity and scalability.
i.e. VOIP and Fax

Not only Phone services but technology also, WiFi, Cellular, Blue Tooth and legacy WAN and ATM.

Data Center Convergence, Virtualization, Network Storage and remote management.

Fibre Channel Protocols carry IP
Fibre channel over IP (FCIP) Internet Fibre Channel Protocol (iFCP)

InifiniBand (IB) SCSI Remote Direct Memory Access Protocol and iSCSI
iSCSI is apealling because small and medium businesses can afford it.

Data Center Bridging Protocols

Priority Based Flow Control (PFC) 802.1Qbb allows the network to pause by class

Enhanced Transmission Selection (ETS) 802.1Qaz Scheduling and priorities

Quantized Congestion Notification (QCN) End to end Flow control (read Congestion)

Data Center Bridging Exchange Protocol (DCBX) 802.1Qaz protocol support All above

Fibre Channel over Ethernet (FCoE)

Layer 2 non routable Uber reliable, IT Won't drop packets.
Requires DCB-Enabled Ethernet. Lossless Traffic.

Fibre Channel and Ethernet in the same converged network equipment.

iSCSI Internet Small Computer System Interface

Encapsulated request protocol. Encrypted if required.

Data Center **Overlay** (OTP) networks at Layer 2 make this all work to geographically diverse remote data centers. Cloud services also.

Multi-Protocol Label Switching (MPLS)

Instead of each router hop making the next decision The label finds the destination via a predetermined path.

The advantage is that the routing paths are determined by lower cost edge routers instead of core backbone routers.

Why do we Security Pro's care?

The ability to control traffic
Data Transport over Multi-Service networks
Resiliency with MPLS Fast Reroute **Page 498**

Voice over Internet Protocol (VoIP)

All VoIP systems convert voice to digital Packets. Then transfer them over the network to be converted back for the listener.

This is said to be Isochronous data. It has to be delivered within strict timing constraints. Otherwise the call sounds odd.

IP telephony Full suite of VoIP Services.

IP communications Business applications that enable such technologies as messaging, contact centers, Multi-media conferencing

Unified Communications Session Initiation Protocol (SIP) unifies and simplifies all forms of communication.

Voice over Internet (VoIP) 2

Issues:

Packet loss: Packet Loss Concealment (PLC) Several design techniques

Jitter: QoS issue, signal shaping timing algorithms and stuff

Sequence Errors: Packet delivery timing, design and Routing techniques (MPLS for example)

Codec Quality: ADSL and Cable network providers often limit upstream bandwidth. They weren't originally designed to be bi-directional.

Wireless

Convenience-Access from anywhere, almost.

Mobility-Users are not tied to their desks.

Productivity-Efficiently accomplish work and encourage collaboration.

Easy set up-A few minutes and no network people stringing wire.

Expandable-Relatively easy compared to running multiple wired runs.

Costs-Minimal wiring costs.

One wired antenna/access point can service many connections

It is a radio broadcast, available to anyone with the right equipment.

Types of Wireless Technologies

Wi-Fi IEEE 802.11 Each new version is faster than the last.

Bluetooth Low power, a maximum range of 50 feet. This is basically used to replace short run cables, phones, remote controls, Keyboard/mouse.

WiMax Wireless Broadband. This is fast becoming the realm of the cellular providers. More than 30 Mbits per sec. Distance matters

Types of Wireless Networks

Wireless PAN Personal Area Network (WPAN) Blue tooth and infrared

Wireless LAN Local Area Network (WLAN) 802.11, Microwave and Modulated Lasers

Wireless Mesh Network A mesh or grid of Wireless nodes, self healing.

Cont=>

Types of Wireless Networks

Wireless MAN Metropolitan Area Networks IEEE 802.16, WiMax

Wireless WAN Wide Area Network Covers a large area typically between neighboring towns and cities. 2.4 Gbit bandwidth with the use of solar or wind power they can be stand alone systems.

Cellular Network A mobile network that is distributed over land areas called cells. Each cell has at least one fixed location tranceiver. Neighboring cells use different radio frequencies. When joined together these can service a wide area. Constantly improving service for data applications.

Spread Spectrum Methodology to spread data transmissions into manageable units that can be applied to about 70 different channels and then re-combined at the receiving end. Data integrity requires node redundancy

Direct-Sequence Spread Spectrum (DSSS)

Frequency-Hopping Spread Spectrum (FHSS0

Other Signaling: Orthogonal Frequency Division Multiplexing (OFDM) Vectored OFDM FDMA and TDMA

Wireless Security Issues

Open System Authentication Default for 802.11 used with WEP, NO AUTHENTICATION

Shared Key Authentication Encrypted WEP challenge between to user and the access point.

Ad-Hoc Mode User to user, can not scale.

Infrastructure Mode This network topology can form large and complex networks.

Wired Equivalent Privacy Protocol (WEP) 802.11 standard Insecure, cracked in 5 min.

Wi-Fi Protected Access (WPA) and WPA2 is based on 802.11i that uses
Advanced Encryption Standard (AES) uses stronger encryption.
Extensible Authentication Protocol is stronger authentication, key management, replay attack protection and data integrity.

This is a radio broadcast, a well equipped attacker can easily eavesdrop or tamper.
"Parking Lot Attack"

Cryptography

Is a discipline that uses principles, means and methods to hide Information content.

- Confidentiality
- Authenticity
- Undetected Modification
- Non-Repudiation
- Unauthorized use

Cryptography is widely used by governments and enterprises that require all the characteristics noted above.

Cryptography is also increasingly used by less law abiding entities.

Due to the increasing availability of CPU power Cryptography, while critical is becoming more easily compromised.

Pressure from all facets to increase the effectivity of Cryptography exists.

Continue=>

Public Key

Digital Signatures Authentication, Integrity, Non-Repudiation

Electronic Payments Payment Card Industry (PCI) standards

Certifying Public Key relationships “Web of Trust”

Issues for consideration with Cryptography

- Users have to believe
- Users have to choose different types and levels of Cryptography
- Standardized use means interoperability
- Interoperability means the ability of different levels of cryptography to work seamlessly
- Mobility means use by different infrastructures
- Portability means it must work on multiple platforms. i.e. Mac and PC

TCP/IP allows a third party to interfere with communications;

Eavesdropping Credit card Info

Tampering Alter someone's financial transaction

Impersonation

Spoofing - pretending to be another

Misrepresentation – Pretends to be a valid store

But just funnels CC info for fraudulent use.

Public Key Cryptography Facilitates;

Encrytion and de-encryption between sender and receiver

Tamper detection - allows recipient verification

Authentication allows the recipient to determine the senders Identity

Non-Repudiation The sender can't later claim Info wasn't sent.

Encryption and Decryption

Symmetric Key Sender and receiver have the same Key

Public-Key also called Asymmetric encryption This requires a published Public Key and a Private Key two way communications requires both,
Transmit with Public, receive with Private.

Key Length and Encryption strength. Usually longer is better.
RSA only uses a subset of the possible combinations (Effectively easier to Break)

Digital Signature Detection and authentication rely on a one way hash.
The value of the hash is unique to the data.
The data cannot be deduced from the hash (One Way)

The data and the signature are 2 different items from the network perspective.

Certificates and Authentication

A certificate is an electronic document used for identification.

Public Key cryptography uses certificates to prevent impersonization

A certificate is issued and managed by a Certificate Authority (CA)
It binds a public key to an identifier i.e. User ID or Emp #

Password-Based Authentication Almost universal, User-id and Password.

Certificate-Based Authentication SSL Public Key, Certificate and Signature.

How Certificates are Used

Client SSL Identifies the Clients to the Server
Server SSL Identifies the Server to the Clients

The Client Software maintains the Private Keys that correspond to the Servers Public Keys.

S/MIME Used for encrypted e-mail SSL certificate.

Object-Signing certificates. Often used to identify original software.

Certificate Authority (CA) Certificates. Limits the use of licensed software copies.

Secure Socket Layer SSL certificate is used during Handshake to authorize use.

Signed and Encrypted Email Validates and provides non-repudiation.
Form Signing is persistent.

Continue=>

Certificates – More

Single sign-on Using a single User-ID and password to access all network resources.

Requires a “Directory Service” as well as SSL and S/MINE certificates (AD)

Object Signing is about authorized use and licensing of software.

Distinguished Names X.509 v3 Often Contain:

- Uid – User ID
- e – email address
- cn – User’s common name
- o – Organization
- c- Country

And a signature

Certificate Authorities and Trust

CA Hierarchies Root is the top level, each subsequent CA must be signed or Authorized by the CA above it.

Certificate chains Each CA in the chain is only "Authoritative" between itself and the issuer of the key.

Verifying a Certification Chain

The certificate is validated against current time
The issuers certificate is located
The cert. signature verified with the public key of the issuer

Managing Certificates

Issuing Certificates Depends on Enterprise policy and procedure

Certificates and LDAP directory The CA can leverage Directory information to pre-populate access certificates. User info

Key Management The public key and the corresponding Private Key are generated, Stored, backed-up and managed. Key Recovery mechanism.

Renewing and revoking Certificates All certificates have a validity timer. Online Certificate Status Protocol (OCSP) is used in X509 management.

Registration Authorities Used across organizations as the registration, retrieval, renewal, revocation and Back-up and recovery master.

Securing Network Components

Domains of Trust

Secure Routing/Deterministic Routing Anytime the Internet is used as an Enterprise Network deterministic routing must be used. Only traffic with predetermined routes is allowed. The Internet can't come in and most Enterprise traffic can't leave.

Boundary Routers these primarily advertise routes that external hosts can access. Boundary routers block many types of inbound and outbound attacks.

Non-Blind Spoofing This type of attack occurs when the attacker and the victim are on the same network. They can see the SEQ and ACK packets.

Bind Spoofing A more sophisticated attack, the SEQ and ACK aren't attainable.

Man in The Middle A malicious party intercepts and acts like each party to the other Capturing all the data.

Security Perimeter This is the first line of defense between the trusted and un-trusted networks. Firewalls and Intrusion Prevention Systems (IPS) are used here. The first line, shouldn't be the only one. Content Filter etc.

Network Partitioning Network should be separated into domains of trust; Internal, DMZ, External. Goes along way. Department segmentation?

Dual Homed Hosts This is a computer with 2 NIC cards on separate networks. These should be prevented from forwarding. No RouteD or RIP.

Bastion Host A bastion is a Dual Homed special purpose computer that only allows certain transactions to the unsecured side. PCI uses this arrangement.

Demilitarized Zone (DMZ) Also known as a screened Subnet. This where an organization puts limited public access resources without allowing access to internal resources.

Hardware

Modems Modulator/demodulator, Digital to analog and vice versa. Does anyone use these anymore? Telephony firewalls stop dialing intrusions.

Concentrators Multiplex connected devices into one higher speed signal. FDDI

Front-End Processors Service I/O requests freeing up larger processors.

Multiplexers Overlays multiple signals into one higher speed signal. LAN Hubs to Dense-Wave Division Multiplexers (DWDM) that combine Optical signals into one strand of fiber

Hubs and Repeaters Hubs implement Star topology networks, repeaters are used to double the distance spec of LANs. All connected devices see all of each others traffic. If the hub breaks, all connected devices lose connectivity.

Bridges and Switches

Bridges work at Layer 2. The send and receive traffic by “learning” the MAC address on either side. Typically a bridge doubles the length of the LAN.

The bridge learns which MAC addresses are on the right. It won’t forward to left any MAC destination on the right.

Bridges don’t filter broadcasts. ASIC’s were the key. Spanning Tree

Wireless 802.11 bridges are efficient but have huge security issues. Access Control Lists (ACL) Just like a Firewall must be employed.

Switches create the Star wired networks in use today. They are bridges except; all of the LAN traffic is between the switch and the host only, there are only 2 ports that participate in the LAN. This is aid to be full wire speed. Each port registers it’s MAC and the Switch only sends traffic to that source or destination

Routers forward packets to other networks. Layer 3, The IP address. The router builds a routing table. The routing table has the details of each next hop.

Transmission Media

Wired Nothing works without cables, even WiFi has to hit wires to get to the internet.

Throughput The rate that data will be transmitted.

Distance Between Devices The degradation of signal (Attenuation) is a limitation of all wired media. Frequency and propagation delay are factors.

Data Sensitivity What is the risk of the data being intercepted? Fiber makes this very difficult.

Environment It is a Cable unfriendly world. Temperature, Interference, Ultra violet and did I mention Rodents?

Twisted Pair Pairs of same gauge wire twisted together with Teflon insulation. Multiple pairs, 4 in Ethernet, are twisted inside an outer jacket. The quality of the resulting cable is determined by the gauge of the conductor wire, the number of twists and type of jacket.

Page 542, Table 4.11 Illustrates the different Cable Categories

Continue=>

Unshielded Twisted Pair (UTP)

UTP is limited to 100 meters and throughput by the Category Category 5 or 6 today. (Cat5) RFI is also a consideration.

Shielded Twisted Pair (STP) STP is less susceptible to RFI than UTP. It also bulkier and more expensive.

Coaxial Cable Instead of being twisted, Coax uses a center conductor sheathed in Teflon insulation and surrounded by braided conductor for grounding.

The center conductor is much thicker than Twisted Pair. Coax has much longer distance capability and RFI protection than UTP. This cable is harder to bend and expensive.

Limited to Cable TV, CCTV and other RF applications

Patch Panels

Even modest Data Centers have the need for easily understood and implemented patch panels. This true for Cat 5, and Fiber. Each work area is connected to the wall jack, the wall jack is connected to a Closet patch panel. The LAN switch is connected via patch cables to the patch panel.

The closet patch panel is connected to a Main distribution panel, With either fiber or UTP patch cables. The LAN Switch Trunks data at a higher rate to the next level equipment. Another patch panel and a bigger switch.

Fiber Optic

Fiber Optics are handled much the same way as UTP. There is a patch panel and patched connections. Fiber Optics employ light pulses to transmit data.

At one end there is a transmitter. The transmitter takes electrical pulses and changes them to light pulses. The other end has a receiver. It changes light pulses to electrical pulses. There is always a pair, each strand transmits in one direction.

Continue=>

Fiber Optics, more

There are 3 types of Fiber Optic cable commonly used.

- Single Mode
- Multi-mode
- Plastic Optical Fiber

The cable acts as the light guide by guiding the light introduced at one end to the other end. The light source pulses on and off, the receiver at the other end converts the light pulses back into electrical pulses.

Even a Laser shining through a Fiber optic cable will lose strength over long distances. It has to be regenerated or Repeated.

Page 544, Fiber Optic specifications table.

Network Access Control Devices

Firewalls Administer security policies by filtering incoming traffic based on the rules.

Often Firewalls are thought of as the protectors of the Internet Gateway only

There are internal network considerations also, such as Zoning.

Additionally Firewalls are employed as threat management appliances, with other security services embedded. Intrusion Prevention Systems, (IPS) and proxy services are often employed.

Firewalls should used between entities that have different trust domains. Firewalls will do little out of the box, they require a good deal of work to configure properly for your enterprise. Firewalls are complex and require a lot of care and feeding. They have to be patched, have their logs monitored, and their rules altered on frequently. Outsourcing the management of Firewalls has become a significant industry.

Continue=>

Filtering

Filtering traffic is based on a rule set. Each rule instructs the firewall to block or Allow packets based on one or more conditions

By Address Packets can be filtered by source or destination address. Or range of addresses. i.e. Only this host can access that host, source and destination. Or this range can access that range.

By Service Packets can be filtered by service. i.e. Only HTTPS is allowed, all other packets are dropped. Port 443

Packets can be filtered based on address and port simultaneously i.e. Only allow HostA to get to Host27 using HTTPS. All others are dropped.

Any packets that don't meet one of the rules criteria will be dropped at the end of the rule list. It's a Table like lookup.

Network Address Translation (NAT)

Firewalls can change the source address of outgoing packets.
Hosts with an RFC1918 private address has to be changed to a forwardable address. NAT greatly extends the life of IPV4

Port Address Translation (PAT) An extension of NAT , PAT allows the use of One routable address by manipulating the port number, Like a session number.

Static Packet Filtering with this on the firewall examines each packet in turn without regard for the context of the packet.

Stateful Inspection or Dynamic Packet Filtering inspects every packet in the context of a session. This allows for adjustment of filtering in response to a perceived malicious traffic pattern.

Proxies

A proxy Firewall or server mediates traffic between two untrusted endpoints.

In a proxy situation the originator talks to the proxy. The proxy talks to the server. Usually out a second interface. The server responds to the Proxy as if it is the originator. The proxy talks to the originator as if it is the server.

The Man in the Middle.

Circuit -Level Proxy creates a conduit trusted host can talk to an untrusted one. No application awareness.

Application Level Proxy relays information from a trusted host to an untrusted host For a specific application only. These Proxies may require authentication.

WEB Content filters and other WEB services.

Personal Firewalls protect a single host from unwanted or untrusted access.

End Point Security

Users pose the biggest risk to security. This is very difficult to prevent.

Security Policies, management, Monitoring and Enforcement are the best defense.

Hardened Workstation configurations with the Notion of ‘Least Privilege’

Mobile devices are another facet.

Content Distribution Networks

Amazon Cloud Front
CNN
The Weather Channel
Netflix

The Security Professional needs to understand the potential risks from Content Distribution Networks