Network and Security Foundations Study Guide

By Christy Twilight ctwili1@wgu.edu

5/8/2024

Note that the Information from the Study Guide 2021 has very different questions than the current guide. The current guide questions seem to be based on the videos that were made a couple of years ago and do not follow the same material patten as the recent cohort videos.

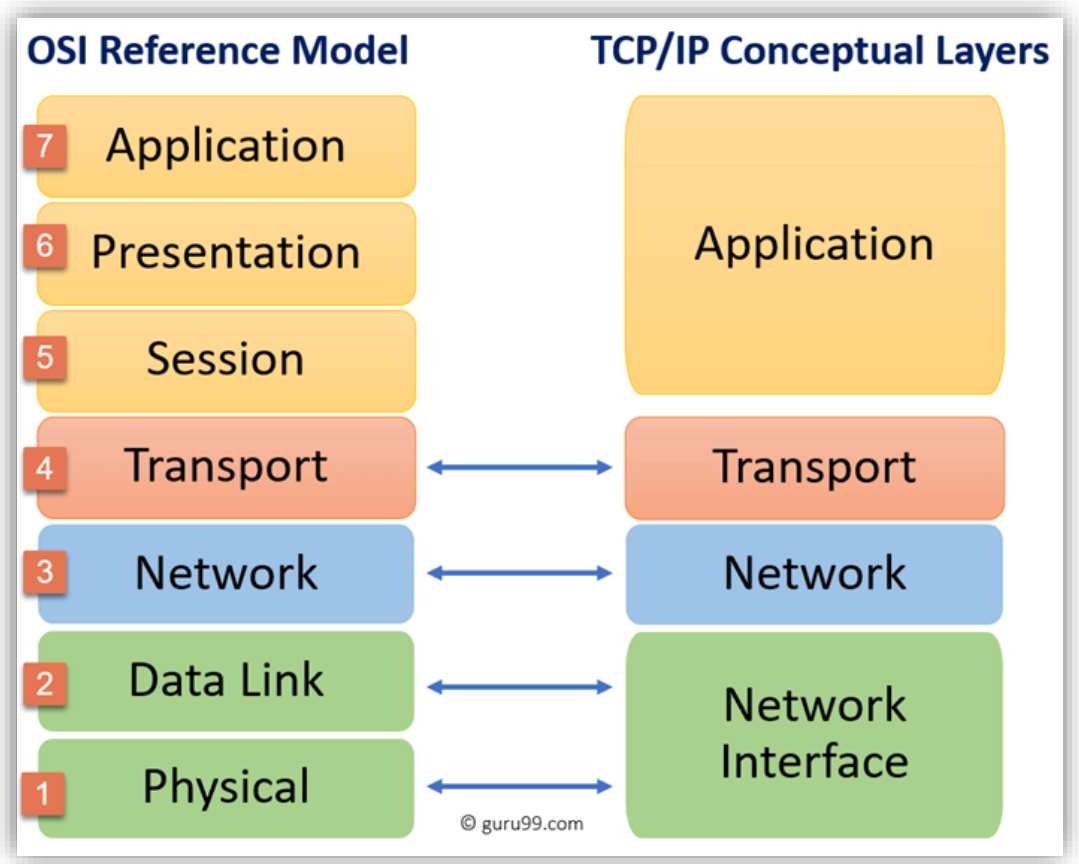
Section 1 was almost identical in path to the questions posted on this study guide but Section 2 and 3 were utter chaos. There is A LOT of material that is in section 2 and 3 that are not in the guide and had no questions. There is also a lot of questions in the guide that were nowhere to be found in any video or textbook reference. I Summarized every single video and textbook before making this guide and it still was not enough. I then referenced two study guides (Feb 2021 updated C172 and Mike's Notes) to fill in any additional gaps that I did not grab directly from Comptia.

Section 3 Lesson 5 Security Governance is not in any questions. If there are material known to be on the OA. Please let me know and I will add them to the study guide. I will not remove material because the OA's are random pool and material I may not see, you may.

Unit 1: Introduction to Networking Concepts

OSI Model & TCP/IP Model

OSI 7 Layer Network Reference Model				
Layer Number	**Layer Name**	**Devices**	**Functions**	**Protocols**
7	**Application Layer**	Gateways Proxies	Serves as the window for users and application processes to access network services.	HTTP FTP SMTP DNS DHCP TELNET
6	**Presentation Layer**	Software-based - • OS • Applications	Translates data between the application layer and the network format; data encryption and compression.	SSL TLS JPEG MPEG
5	**Session Layer**	Software-based - • OS • Applications	Manages sessions between applications; establishes, manages, and terminates connections between applications.	NetBIOS PPTP SMB NFS
4	**Transport Layer**	Software-based - • OS • Applications	Provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control.	TCP UDP
3	**Network Layer**	Routers Layer 3 switches Firewalls	Determines how data is sent to the receiving devices; routing and forwarding of packets.	IP ICMP IPSec IGMP IPX
2	**Data Link Layer**	Switches Bridges NICs	Provides node-to-node data transfer—a link between two directly connected nodes; packages data into frames.	Ethernet PPP HDLC ARP
1	**Physical Layer**	Hubs Cables Repeaters NICs	Transmits raw bit streams over physical medium, defines electrical and physical specifications.	Hardware-based No Protocols



How does the OSI model match to the TCP/IP model?

TCP/IP 4 Layer Conceptual Model				
Layer Number	**Layer Name**	**Devices**	**Functions**	**Protocols**
4	**Application Layer**	End-user software applications.	Closest to the end user. Both end-user and application-layer processes interact with the transport layer to send and receive data. This layer provides application services for file transfers, e-mail, and other network software services.	HTTP FTP SMTP DNS DHCP SNMP
3	**Transport Layer**	Primarily managed by software within operating systems.	Responsible for end-to-end communication services for applications. It provides services such as connection-oriented communication, reliability, flow control, and multiplexing.	TCP UDP
2	**Internet Layer (Network)**	Routers Layer 3 switches	Provides internetworking, addressing, and routing. This layer is responsible for sending packets from any network, and they can pass through multiple routers to reach any other network.	IP ICMP IPSec IGMP
1	**Link Layer (Network Interface)**	NICs Switches Other networking hardware	Handles the physical and logical connections to the hardware. This layer is responsible for how data is physically transmitted over the network, including defining the electrical, mechanical, procedural, and functional specifications for activating, maintaining, and deactivating the physical link between communicating network systems.	Ethernet ARP PPP

Help remember what occurs at each level:

PHYSICALLY HOP to the HOST to get SERVICE with COOKIES BITe carefully I

COMMAND you

Layer 1 – Physical -Bit - (TCP/IP 1)
Layer 2 – Hop to Hop (Mac Address) – Frame - (TCP/IP 1)
Layer 3 – Host to Host (aka End to End) IP address (IPV4, IPV6, ICMP) – Packet - (TCP/IP 2) – routes data between networks
Layer 4 – Service to Service (TCP/UDP) -Segment - (TCP/IP 3) - Ensures that packets are delivered with no loss or duplication
Layer 5 – User Sessions (Cookies) (TCP/IP 4)
Layer 6 - Used to interpret the bits for presentation; encryption/decryption (TCP/IP 4)
Layer 7 – Application command (TCP/IP 4)

I think this is more important than memorizing the layer names as it lets you know what that layer does which will help for attacks and security

Network Media Devices

Device	Layer	What does device do?
Hub	1	Connects router to the network. Takes data packets from router and sends them to devices in the network. By connecting a USB hub to a PC, data packets can be transferred to multiple devices connected to your computer, but each device only looks at traffic destined for it and ignores the rest.
Modem	2	Sends and receives data. Allows computers to transport digital info over analog lines, such as phone and cable.
Repeater	1	Repeaters take in the signal being sent, process it and then send out the signal stronger than before to the next waypoint (either another repeater or the end user). Another method is signal boosters, which are common with wireless signals. (comptia)

Switch	2	Connect devices in a specific network and allow them to communicate within network. Like a hub but more complex, has capability to add security measures and function more intelligently, sending traffic directly from sender to receiver without other devices aware of communication. Most internet routers include a switch in the form of wired and wireless ethernet connections.
Bridge	2	Connects two or more networks. Different from a router because a router analyzes data packets to determine where to send, whereas a bridge forwards the data to next network without analysis. Fast data transfer but lacks versatility. Not widely used today as routers and switches are favored. Repeater: Used to strengthen, replicate, and regenerate signals that are weakened. A range extender is a form of repeater.
Router	3	Point of connection between two or more networks, and forwards data packets between the networks. Connects networks on internet to networks at home. Provides ethernet port or wi-fi. Responsible for implementing Network Address Translation (NAT)

Additional Media Mentioned on videos and in Textbooks

- Edge Router- This is at the end of the network backbone to connect to other core routers. It is meant to distribute packets to other networks than its own. (Layer 3 OSI)
- Core Router- Internal; does not distribute packets out of its network. (Layer 3 OSI)
- Subscriber Edge Router – tele com networks to connect individual subscribers to the wider infrastructure. (Layer 3 OSI)
- Inter-provider Border Router - typically is ISP to ISP, really the core or the backbone of the Internet itself. (Layer 3 OSI)
- Access point – is used to interconnect wireless devices and provide a connection to the wired devices and provide a connection to the wire LAN. The data transfer speeds, for access points, are dictated by the choice of wireless technology for the clients but this device will support Wireless-N (Layer 2 OSI)

Cables

Unshielded Twisted Pair (UTP) vs Shielded Twisted Pair

Both Cables are with wires that are twisted together. The STP uses a foil or mesh shield to reduce noise and crosstalk. It also requires the use of an electrical ground. STP provides higher data rates but more challenging due to the shielding. STP is ideal for underground installation. It tends to be used in environments that are susceptible to EMI such as Airports, Industrial, and Medical centers

UTP are more flexible, smaller, and lighter but have slower data rates.

NAME	MAXIMUM DATA RATE	BANDWIDTH	APPLICATION
Category 1	1 Mbps	0.4 MHz	Analog phone, modem, or fax line
Category 2	4 Mbps	4 MHz	Async terminals
Category 3	10 Mbps	16 MHz	10BaseT Ethernet
Category 5	100 Mbps	100 MHz	100BaseTX and 1000BaseT Ethernet
Category 5e	1 Gbps	100 MHz	100BaseTX and 1000BaseT Ethernet
Category 6	10 Gbps	250 MHz	10GBaseT Ethernet
Category 6a	10 Gbps	500 MHz	10GBaseT Ethernet (higher bandwidth)
Category 7	10 Gbps	600 MHz	10GBaseT Ethernet or 1000BaseT over single cable
Category 7a	10 Gbps	1000 MHz	10GBaseT Ethernet or 1000BaseT over single cable (higher bandwidth)
Category 8/8.1	40 Gbps	1600–2000 MHz	40GBaseT Ethernet 1000BaseT over single cable
Category 8.2	40 Gbps	1600–2000 MHz	40GBaseT Ethernet or 1000BaseT over single cable (higher bandwidth)

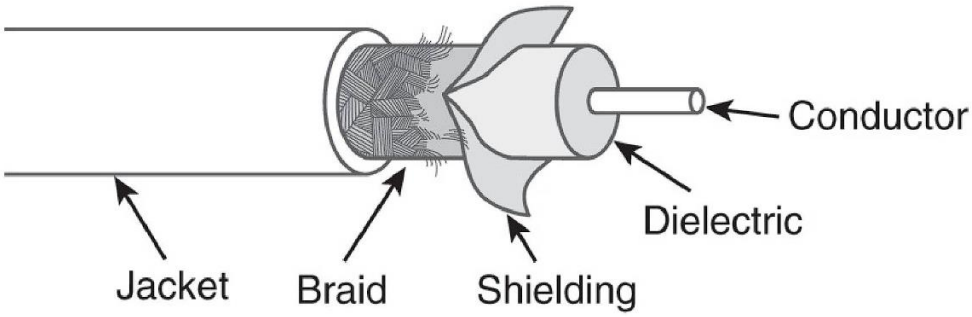


FIGURE 4-5 Anatomy of a coaxial cable.

Gigabit Ethernet is an Ethernet technology that can transmit data at speeds of 1,000 Mbps and primarily uses optical fibers for transmission. It can be used for distances ranging from 500 to 5,000 meters depending on the type of optical fiber used. The hardware required for Gigabit Ethernet is very expensive when compared with other types of Ethernet.

Standard	IEEE Specification	Medium	Distance (meters)
1000Base-T	802.3ab	CAT5, CAT6 UTP	100
1000Base-TX	802.3ab	CAT6 UTP, CAT7 UTP	100
1000Base-X	802.3z	Shielded, Balanced coax	25 to 5,000
1000Base-CX	802.3z	Shielded, Balanced coax	25
1000Base-SX	802.3z	Multimode fiber (850nm wavelength)	550 in practice (220 per specification)
1000Base-LX	802.3z	Single-mode fiber (1,300nm wavelength)	5,000
1000Base-LX	802.3z	Multimode fiber (1,300nm wavelength)	550
1000Base-LH	802.3z	Single-mode fiber (1,300nm wavelength)	10,000
1000Base-LH	802.3z	Multimode fiber (1,300nm wavelength)	550

10 Gigabit Ethernet is currently the highest speed at which Ethernet operates. It can achieve speeds of 10 Gbps, which is 10 times faster than Gigabit Ethernet. There are several standards and specifications for 10 Gbps or 10 Gigabit Ethernet, the most common of which are described in the following table.

Standard	IEEE Specification	Medium and Characteristics	Speed (Gbps)	Distance (meters)
10GBase-X	802.3ae	Multimode fiber (850nm wavelength)	9.9	65
10GBase-SR	802.3ae	Multimode fiber (850nm wavelength)	10.3	300
10GBase-SW	802.3ae	Multimode fiber (850nm wavelength)	9.9	300
10GBase-LR	802.3ae	Single-mode fiber (1,310nm wavelength), Dark fiber	10.3	10,000
10GBase-LW	802.3ae	Single-mode fiber (1,310nm wavelength), Synchronous Optical Network (SONET)	9.9	10,000
10GBase-ER	802.3ae	Single-mode fiber (1,550nm wavelength), Dark fiber	10.3	40,000
10GBase-EW	802.3a	Single mode fiber (1,550nm wavelength), SONET	9.9	40,000
10GBase-T	802.3an	CAT5e, CAT6, CAT7 UTP	10	100
10GBase-CX4	802.3ak	Four thin twin-axial cables	4 x 2.5	25

SX- short reach over multimode fiber

SR- Short Wavelength Extended Range

Base-baseband signaling

Things to remember based on the different tables above:

Cat 5 - 100Mbps, RJ-45 Connector, Twisted Pair Copper Cabling
Cat 5E – 1Gbps, RJ-45 Connector, Twisted Pair Copper Cabling
Cat 6 - 10 Gbps, RJ-45 Connector, Twisted Pair Copper Cabling, limited range of 33-35 for 10Gbps

Cat 6A – 10 Gbps, RJ-45 Connector, Twisted Pair Copper Cabling
All Categories have a max segment length of 100m for those that will be mainly tested unless you are talking about fiber optics.

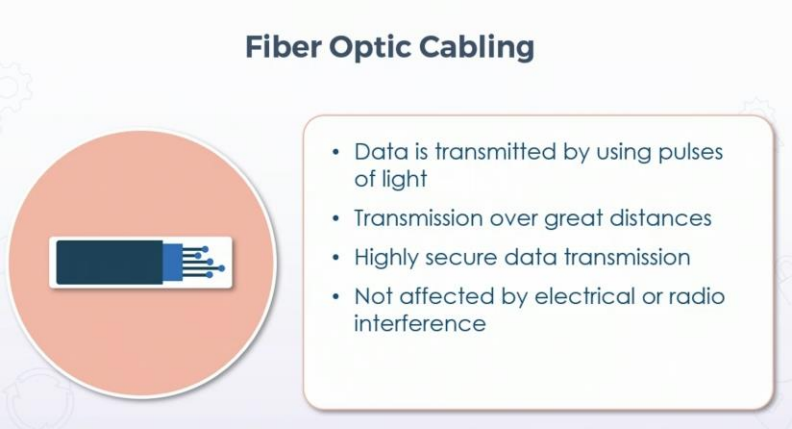
Copper Cabling types : Coaxial, UTP (unshielded), STP (shielded) – Shielded reduces electromagnetic interference but it more expensive than UTP.

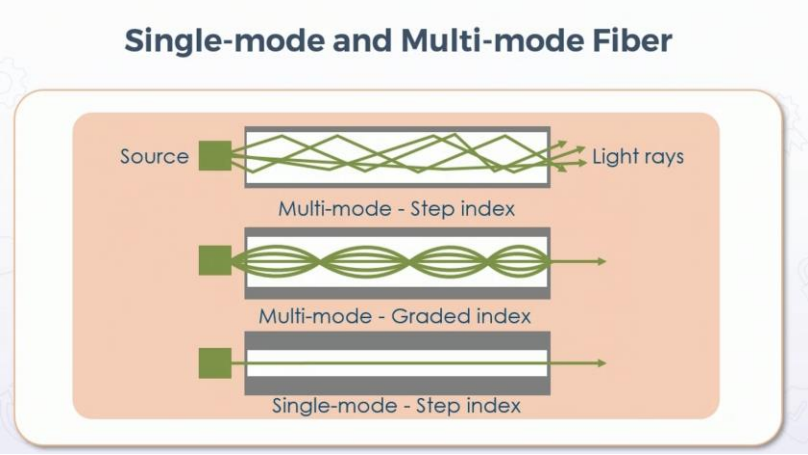
Coaxial Cables are used for carrying cable television signal, used for broadband cable internet access, protects against EMI (Electromagnetic Interference), and contains Copper Cabling.

Cross-over cables are used with like items such as PC to PC or Router to Router. In older systems (pre 99), They were needed to switch the orange and green wires in order for like devices to transmit and receive data. Most modern computers do not need to do this and will automatically detect it.

Patch Cables : are twisted pair copper cables that are made to connect workstations to network devices.

Fiber Cables





- Light source is typically an LED which can produce varying wavelengths aka multi
- Step index- sharp infraction
- Graded index – gradual infraction
- Single-mode – used in larger distances
- Multi-mode- in shorter distances
- Both can span distance in KM
- Single-mode tends to be used in WAN and Man
- Multi-mode tends to be used in LAN

The differences between Single-Mode Fiber Optics and Multi-Mode

Multi-Mode is Cheaper, Thicker, and Uses LED as a source of Light.
Single-Mode is more expensive than Multi but can run further and uses a laser as a light source.

Listed on the study guide but are not on any material in the textbook or videos

(there is one off mention of patch cables on a video without an explanation)

Crossover cable: special type of cable that helps connect two similar devices directly to each other like two computers or two switches without needing anything else in between. Usually involves flipping the green and orange pair. At higher rates MTX auto can crossover without requiring respective pairings

Patch cable: cable used inside of a wiring closet to patch from a patch panel into an ethernet switch.

Patch Panel: passive device that are used to organize network cables.

A – higher frequency, issues penetrating walls. (regulated), 54 Mbps, 5ghz

B- interference, further range (unregulated band), 11Mbps, 2.4Ghz

G-combines best of A&B, 55Mbps, 2.4Ghz (backwards compatible with 802.11b)

N-first to use MIMO for a single user aka SU-MIMO, dual band, 450Mbps, dual band both 2.4Ghz and 5Ghz (backwards compatible with backward compatible with 802.11a, b, g

AC-first to allow multi-user aka MU-MIMO, dual band 866-1.73Gbps, dual band both 2.4Ghz and 5Ghz (backward compatible with 802.11b, g, and n)

IEEE Standards for Wi-Fi

Along the way, a naming convention was developed by the Wi-Fi Alliance ("Wi-Fi #") to help the general public better distinguish between various IEEE 802.11 implementations:

- **IEEE 802.11™** is the pioneering 2.4 GHz Wi-Fi standard mentioned above from 1997, and it is still referred to by that nomenclature. This standard and its subsequent amendments are the basis for Wi-Fi wireless networks and represent the world's most widely used wireless computer networking protocols.
- **IEEE 802.11b™, or Wi-Fi 1**, was introduced to the market in 1999 with Apple's announcement. It also operated at 2.4 GHz, but to reduce interference from microwave ovens, cordless phones, baby monitors, and other sources, and to achieve higher data rates, it incorporated modulation schemes called direct-sequence spread spectrum/complementary code keying (DSSS/CCK). Wi-Fi 1 enabled wireless communications at distances of ~38m indoors and ~140m outdoors.
- **IEEE 802.11a™, or Wi-Fi 2**, also introduced in 1999, was the successor to IEEE 802.11b. It was the first Wi-Fi specification to feature a multi-carrier modulation scheme (OFDM) to support high data rates, unlike Wi-Fi 1's single-carrier design. It supported 5 GHz operation and its 20 MHz bandwidth supported multiple data rates.
- **IEEE 802.11g™, or Wi-Fi 3**, was introduced in 2003. It allowed for faster data rates of up to 54 Mbit/s in the same 2.4 GHz frequency band as IEEE 802.11b, thanks to an OFDM multi-carrier modulation scheme and other enhancements. This was appealing to mass market users, as 2.4 GHz devices were less expensive than 5 GHz devices.
- **IEEE 802.11n™, or Wi-Fi 4**, was introduced in 2009 to support the 2.4 GHz and 5GHz frequency bands, with up to 600 Mbit/s data rates, multiple channels within each frequency band, and other features. IEEE 802.11n data throughputs enabled the use of WLAN networks in place of wired networks, a significant feature enabling new use cases and reduced operational costs for end users and IT organizations.
- **IEEE 802.11ac™, or Wi-Fi 5**, was introduced in 2013 to support data rates at up to 3.5 Gbit/s, with still-greater bandwidth, additional channels, better modulation, and other features. It was the first Wi-Fi standard to enable the use of multiple input/multiple output (MIMO) technology so that multiple antennas could be used on both sending and receiving devices to reduce errors and boost speed.

Wi-Fi 6 Addresses Network Density Deeds and Provides Spectral Efficiency

IEEE 802.11ax™, or Wi-Fi 6, is the most recent standard in the series, published in 2021, and devices based on it are now being deployed in billions of devices per year.

Although its theoretical data rate is 9.6 Gbit/s, this standard isn't primarily about boosting Wi-Fi speeds per se. Rather, it addresses the fact that Wi-Fi usage is now so pervasive that network performance can be degraded in areas of dense Wi-Fi traffic, such as sports stadiums, concert halls, and public transportation hubs, and more and more even in our homes where routers must communicate with a growing number of digital gadgets simultaneously.

IEEE 802.11ax offers many enhancements. It employs a multi-user mechanism that allows the 9.6 Gbit/s data rate to be split among various devices. It also supports routers sending data to multiple devices in one broadcast frame over the air, and it lets Wi-Fi devices schedule transmissions to the router. Mechanisms to support longer-range outdoor operations are also added.

https://standards.ieee.org/

Things to remember based on the different tables above:

IEEE 802.11a channel bandwidth: 20 MHz (5 Ghz Frequency) 54 Mbps
IEEE 802.11b channel bandwidth: 22 MHz (2.4 Ghz frequency) 11 Mbps - three non-overlapping channels (1,6,11)
IEEE 802.11g channel bandwidth: 20 MHz (it combines advantages from a & b) 54 Mbps (2.4 GHz Frequency)
IEEE 802.11n channel bandwidth: 20MHz & 40 MHz (2.4 Ghz or 5 Ghz) SU-MIMO – 600Mbps
IEEE 802.11ac channel bandwidth: 160 MHz (2.4 Ghz or 5 Ghz) MU-MIMO – 6.933Gbps
IEEE 802.11ax channel bandwidth: 160 MHZ(2.4 Ghz or 5 Ghz) MU-MIMO - 9.607Gbps
All 802.11s used CSMA/CA as CSMA/CD is wired

Basic Network Commands

What is each command used for?

- **ping (Windows/Linux):** Send an Internet Control Message Protocol (ICMP) echo request and listens for reply. If reply received, displays time it took and Time To Live (TTL) left. Many options: max TTL, IPv4/IPv6, num of requests, etc. Useful for troubleshooting if no reply received can be connectivity or firewall issues. Latency can help troubleshoot performance problems, or help network architect to determine where to place devices.

- **traceroute(Linux)/tracert(Windows)**: Trace the route an IP packet takes to destination. Displays each hop (next router) in numerical list with hop IP address and time to receive packet. Useful determining where ping fails, troubleshooting performance and connectivity.

- **tracepath (Linux)**: Similar to tracerout as it displays path taken by a packet from source to destination. Differs as can be used by any user instead of superuser.

- **ipconfig(Windows):** (Internet Protocol Configuration) provides IP, subnet mask, and default gateway for each network adapter. Can also provide MAC address, DHCP status, lease info. /release command used to release all connections and renew adapters. Used in windows. Ipconfig is used to view and configure the network settings on a Windows computer. It's often used to troubleshoot network issues, like connectivity problems or incorrect IP addresses. It also works to view the current IP configuration of a computer, as the command displays the IP addresses assigned to their network adapters as well as the default gateway and DNS servers. ipconfig is an efficient tool for Incident Response (IR) teams and network administrators to troubleshoot and uncover vital network details during a cyber-security event. Some notable benefits include:
    - Discovering IP Addresses: Identify the local machine's IP, Gateway, and DNS server addresses, which might be relevant during an investigation, or while assessing network exposure or communication with rogue servers.
    - Identifying Configuration Issues: Uncover misconfigured network settings or discrepancies between IP, DNS, or default gateway addresses, which could be signs of malicious activity.
    - DNS Cache Investigation: Examine DNS cache entries as evidence of possible communication to malicious domains, or clear the DNS cache to alleviate malware behavior.
    - Troubleshooting Connection Problems: Validate network connectivity directly, from the local host or with remote hosts through tools like ping or tracert, utilizing IP addresses from ipconfig.

- **ifconfig (Linux):** Similar to ipconfig. Implemented at time of boot to configure kernel network interfaces. Also used for debugging or tuning. Used in linux. Ipconfig is used in windows.

- **arp(windows & Linux):** (Address Resolution Protocol) displays the IP to physical (MAC) address mappings for hosts discovered in ARP cache (The ARP cache maps IP addresses to MAC addresses). ARP used to add, remove, modify entries in ARP cache. Hosts need to be on local network, addresses discovered by broadcasting to everyone on network and recording reply from owner. Broadcast traffic not allowed through router so system will maintain MAC address of router.

- **netstat: (Windows & Linux)(**Network Status) displays info about network adapters, and active ports and their state. Useful troubleshooting capacity management. you can use the command netstat -an to see all the connections and their states, and then use the command netstat -b to see the executable files that are involved in the connections. You can then look for connections that use ports that are not associated with any known service or application, or that have addresses that are not part of your network or domain. You can also use the command netstat -e to see the number of failed or discarded packets, which can indicate a network problem or an attack.
- **nslookup (Windows & Linux):** (Name Server Lookup) displays and troubleshoots DNS info/problems. Displays names to UP address mappings.

- **dig(Linux & Windows pre 10 (otherwise you have to install it):** (Domain Info Groper) command used to query DNS name servers, looks up and displays answers from query. Troubleshoots DNS problems. The DIG command works by performing a DNS query from your device to the targeted IP address or hostname. The query will first arrive at your ISP's recursive name servers. If there is your answer, it will return it fast. If not, your query will be re-routed in search of the answer. There could be another recursive DNS server that can answer the query, or it could arrive at the authoritative DNS name server, who for sure will have the answer, and you will get your DNS query resolved.

- **whois (Windows & Linux)**: Look up who owns domain or block of IP addresses. Shows name, email, physical address, but info may be private.

- **route(Windows& Linux):** Display current route tables on host, or add or remove routes. Determines where to send traffic (0.0.0.0 is default gateway, where router sends things if not defined in routing table). Can be used to manually enter default gateway for a computer.
- **scp (Linux):** (Secure Copy Protocol) used to securely copy files between servers, using SSH (Secure Shell) for auth and encryption.
- **ftp (Windows & Linux): (**File Transfer Protocol) copies file(s) from one host to another. Data is unencrypted, but FTPS uses SSL/TLS (Transport Layer Security) if need encryption. Transfer uses TCP (Transmission Control Protocol) for reliability.
- **tftp (Windows (has to be enabled) & Linux):** (Trivial File Transfer Protocol) transfers a file either way between client and server using UDP (User Data Protocol). Only used on reliable (local) networks.
- **finger(Linux):** Displays info about user(s) on remote system, including log in time and username. Used on linux.
- **nmap(Originally Linux but added to Windows):** (Network Mapper) scans networks to find hosts and open ports.

- **tcpdump (Linux):** Displays TCP/IP and other packets transmitted over network system. Form of protocol analyzer (sniffer), designed to show contents of network packets in human readable form for troubleshooting, security, etc.
- **telnet/ssh (Windows & Linux):** (Telnet and Secure Shell) allow user to manage accounts and devices remotely. Main dif is SSH encrypted, thus data secure.
- **cat:** allows you to create single or multiple files, view content of a file, concatenate files and redirect output in terminal or files.
- **tftp:** relies on UDP for quick transfers. It does not manage files like FTP nor use TCP for file transfer. Its only ability is to upload and download files without the ability to see which files exist or manage them in anyway and no authentication procedures. TFTP uses port 69/UDP

NOTE: Last 4 were not found in the textbook or video but were referenced from Comptia site (compare from above definitions. It will help for other test questions)

- **nmap:** network mapper is an open source tool for network exploration and security auditing. Helps map an entire network easily and finds its open ports and services
- **tcpdump:** packet analyzer. Analyzes network traffic by intercepting and displaying packets that are being created or received by the computer its running on (Linux)
- **telnet/ssh:** network protocol used to virtually access a computer and provide a two-way, collaborative and text-based communication channel between two machines. The command connects to a port on a remote service to verify if the path from the computer to the server is open over that port (Telnet for windows and SSH for Linux)

  Tool: **Wireshark** --- captures packets as they go across the network. It 'listens'. It can help with troubleshooting networks that have performance issues

Things to Remember from the above Commands

ping – checks the reachability of a remote network host

ipconfig/if config – are used to display TCP/IP configuration settings (windows and linux respectively)

nslookup – is a network software tool that allows you to obtain a domain name to IP address mapping

tracecert/traceroute – is a utility for displaying intermediary points (routers) the IPv4 packet has padded through on its way to another network node. (windows and linux respectively). It also identifies the route a packet takes between your computer and the destination computer specified

arp – is used to perform a resolution of IP to Mac address. The ARP command is similar to the ARP device used at Layer 2 & 3 to find Mac Addresses

netstat – used to identify any network connection made by a machine

route – is used to display the contents of a routing table

telnet – is a utility that provides unencrypted access to a command-line interface on a remote host

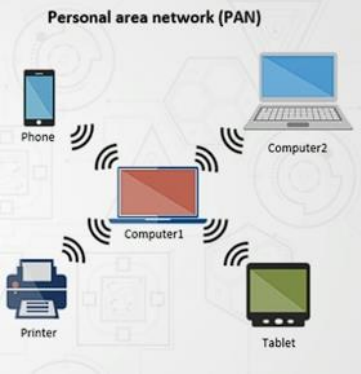
tcpdump – is a packet capturing utility

nmap – is used for discovering hosts and open ports on a network

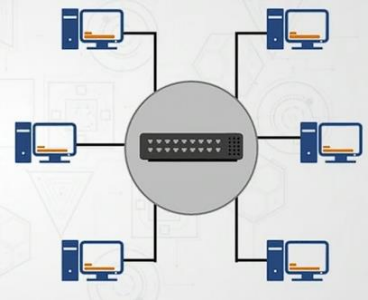
** case sensitivity is important. Just because Microsoft word adds capitalizations, keep in mind to use lowercase for commands**

Network Types

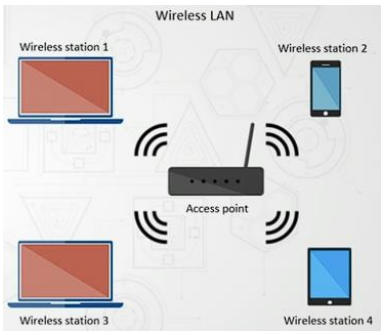
Describe each network type



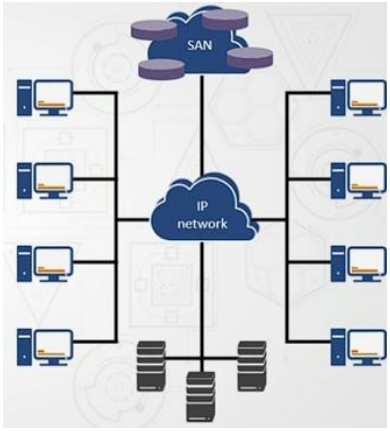
Personal Area Network (PAN): Interconnecting devices focused on personal workspace such as laptops, mobile phones, tablets, printers, and speakers. They can be NFC or Bluetooth. Phrase in the question would be “sync”



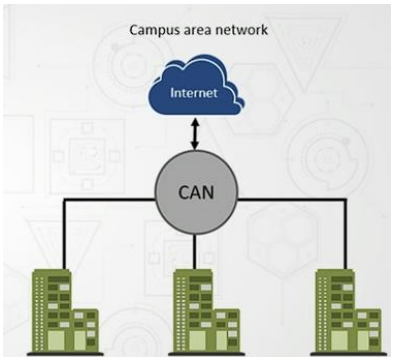
Local Area Network (LAN): Small computer network that is typically confined to a single room, building, or group of buildings. Usually connected via Ethernet



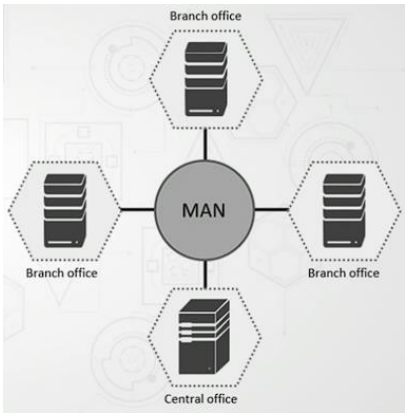
Wireless Local Area Network (WLAN): Enables wireless network communication using wireless signals as opposed to traditional network cabling



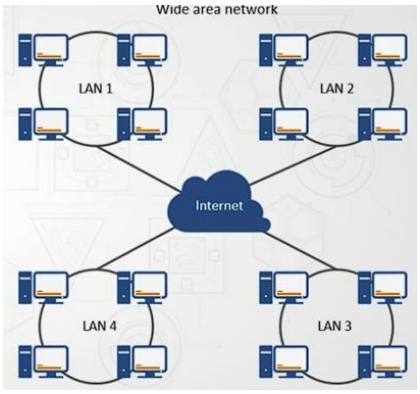
Storage Area Network (SAN): specialized high-speed network that grants block-level network access to storage. It provides storage that appears locally attached to the end user. Used for application availability, application performance, storage utilization, and data protection and security.



Campus Area Network (CAN): Proprietary local area network typically used to serve corporations, universities, and government agencies



Metropolitan Area Network (MAN): Data network design used for a city or town. It is similar to a local area network (LAN). Formed by connecting multiple LANs. They are typically between the size of a LAN and a WAN. Benefits include efficiency, fast communication, and high-speed carriers



Wide Area Network (WAN): Computers network spanning a large geographical area and typically consists of at least two LANs

Network Topologies

Every network has both – logical topology and physical topology.

- Logical Topology: This refers to how data is transmitted between nodes – the way that signals respond on the network media. Now this is a function of the network protocols in use to transmit the data across a network, for instance, Ethernet. That is a protocol a set of rules, a set of guidelines as to how things take place
- Physical Topology represents the actual layout of the network devices – how they are arranged, how they are interconnected, and how they communicate with each other.
    - hardware and cables
    - Arrangement of devices

Describe each *Physical* Network Topology

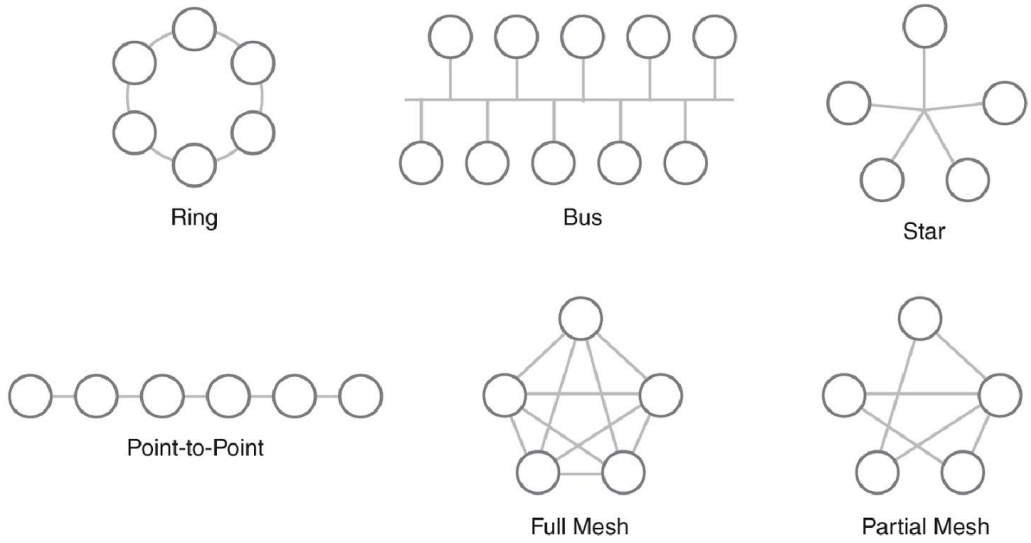
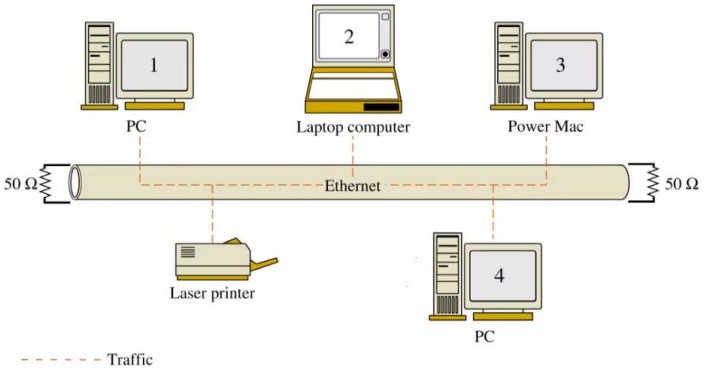


FIGURE 3-11 Common network topologies.

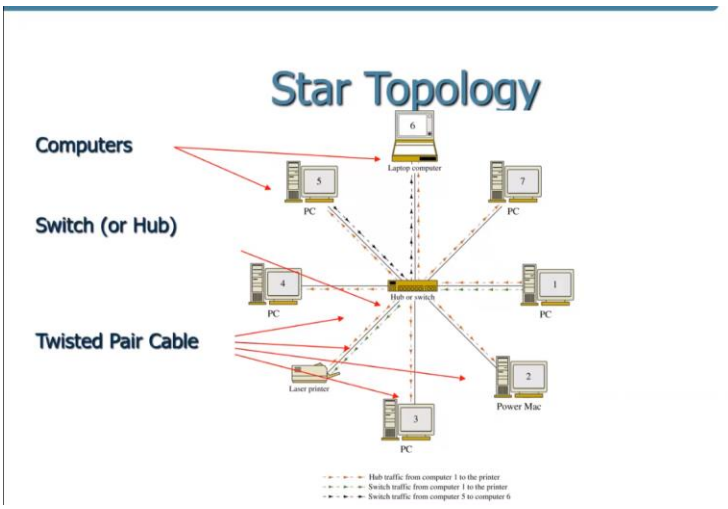
- **Ring**—A shared ring connecting multiple devices together
- **Bus**—A shared network transmission medium allowing only one device to communicate at a single time
- **Star**—A star-wired connection aggregation point, typically from a wiring closet
- **Point-to-point**—A direct link or connection between two devices
- **Mesh**—Multipoint connections and direct links between network devices
- **Hybrid/star-wired bus**—Also known as a tree topology; a

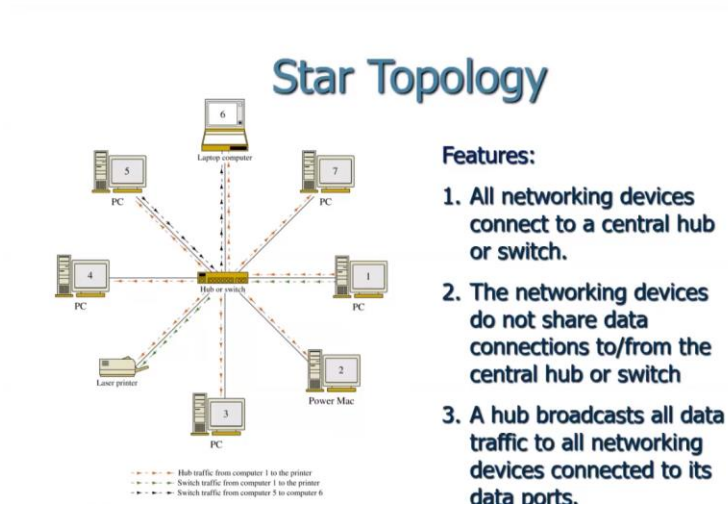
BUS TOPOLOGY



Features - network data traffic is carried over a common data link

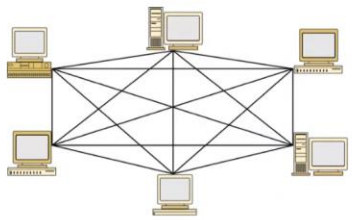
Very old Topology. Everyone had to wait their turn as only one could occur at a time. Look at the end terminals as this image demonstrates.





A Star topology is a type of network topology in which all the devices or nodes are physically connected to a central node such as a router, switch, or hub. The central node (hub) acts as a server, and the connecting nodes act as clients. It can sometimes be referred to as a Hub and Spoke pattern. At the OSI Layer 2, A hub and spoke ethernet switched LAN is a combination of multiple full mesh switched networks. Star general term while Hub and Spoke is a kind of Star.

MESH TOPOLOGY



Features:

1. All networking devices are heavily interconnected
2. Redundant data traffic paths
3. Expensive

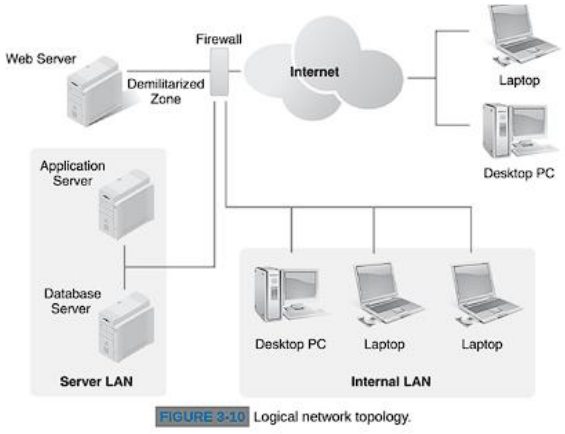
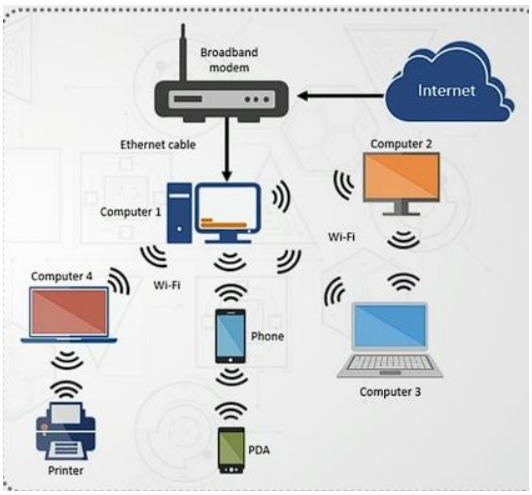


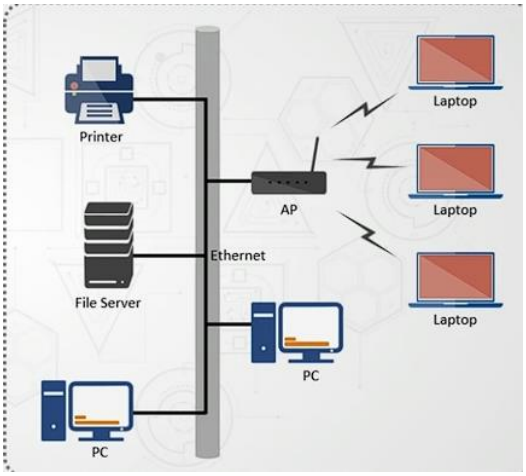
FIGURE 3-10 Logical network topology.

Logical Topology: A logical Network Topology is how the network logically works the Data Link Layer (DLL) where the Media Access Control (MAC) (L2) and the Logical Link Control (LLC) sublayers reside

There are two types: Ad-hoc and Infrastructure



Wireless Ad-hoc : LAN that is built as devices are added and connected to each other. Each device can connect to the wireless device and to each other. Advantages are that it bypasses the need for a router, mobility, and speed.



Infrastructure Networks: Devices connected to a wired network. They use Access points. WLAN does not replace the LAN but instead extends functionality to wireless devices. Advantages is that it is scalable but it can be more complex to setup than adhoc and it is higher in cost.

Above asks the question: What is the advantage of a wired network and What is the advantage of a wireless network?

Network Architecture

Explain each network architecture:

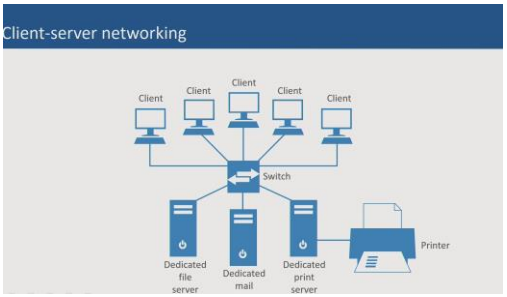
- **Centralized networks** function under the control of one main server, which handles all data transmission, storage, and processing tasks. On the other hand, **decentralized networks** distribute these responsibilities across several nodes, with no single point of authority. (neither centralized nor decentralized are discussed in the material provided for this course yet it is on the study guide.docx)

Host-based Applications

- These are early state computer systems that consisted of a central host with text-based terminals connecting them. The terminals had no intelligence other than to accept a stream of characters from host and display them to the user often known as dumb terminals. Accounting and Enterprise resource planning use host-based applications

Client-based Applications (1980s)

- 1980s allowed for client desktops to take the load for processing requirements. Known as diskless workstations. Due to the massive amount of client-side usage, it saturated networks with data reading and writing with speeds as low as 10 Mbps



Client/Server Applications (1990s-2000s)

- Splits the data and processing tasks between two main partitions: Servers handle the data while clients handle the processing. This was an upgrade from the **Client-based model.** This is popular with enterprise-class applications like accounting information systems (AISs) and Enterprise resource planning ERP systems).

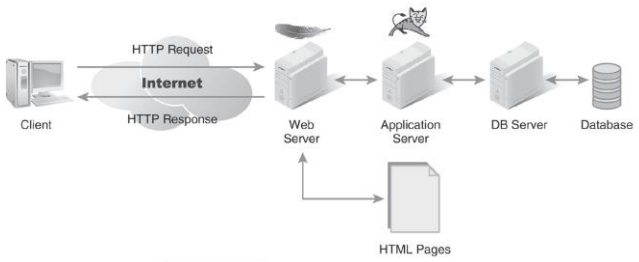
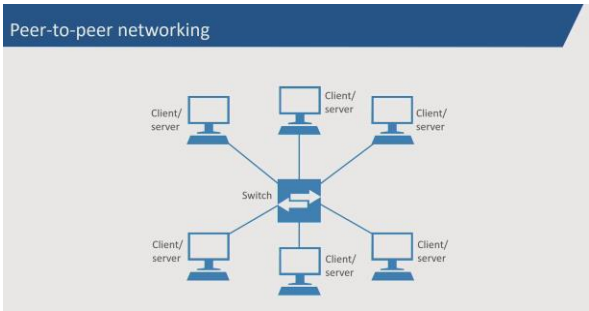


FIGURE 6-2 N-tier application architecture.

Cloud Computing/N-Tier Applications

- Application server introduction which is a program that runs on a central server that handles processing logic. appServer generally run on a server in the same data center as the database server. appServer reads vast amounts of data from the DBMS. The appServer sends only the results over the network to the client. Originally known as 3-tier architecture, due to multiple appServers, it is known as N-tier.



Peer-to-Peer Model:

- Peers share data and processing with each other. This is normally used in a trusting work collaborating environment unless blockchain technology is used.

Virtual and Cloud Computing

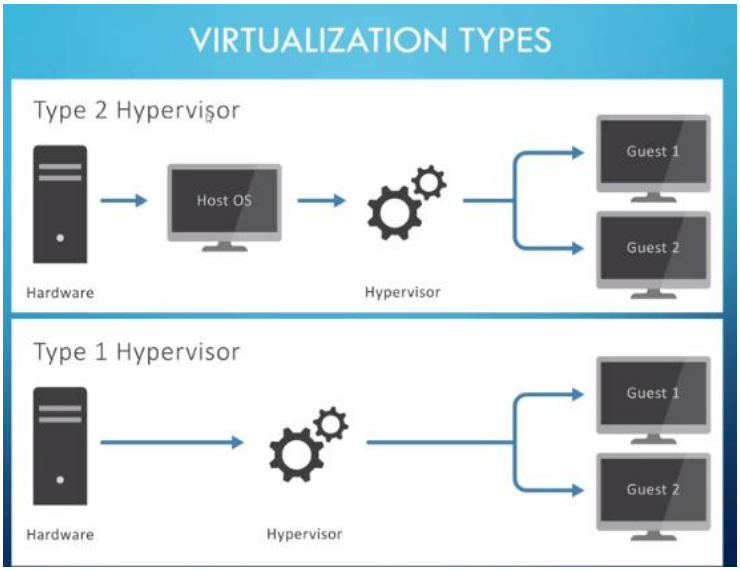
Hypervisors:

- A virtual machine (VM) can virtualize all of the hardware resources, including processors, memory, and network connectivity.
- A virtual machine monitor (VMM) or hypervisor, is the software that provides the environment in which VMs operate.

To be a VMM it needs to have the follow properties:

1. Fidelity – the environment it creates for the VM is essentially identical to the original (hardware) physical machine
2. Isolation or safety – the VMM must have complete control of the system resources
3. Performance – There should be little to no difference in performance between VM and physical equivalent

What is the difference between a Type 1 and Type 2 hypervisor?



- Type 1: Bare metal Hypervisor- Require dedicated hardware, installed as the machine's OS. Found in data centers. Limited user interface, all admin has to be performed from another computer, usually through a web browser/IP address.

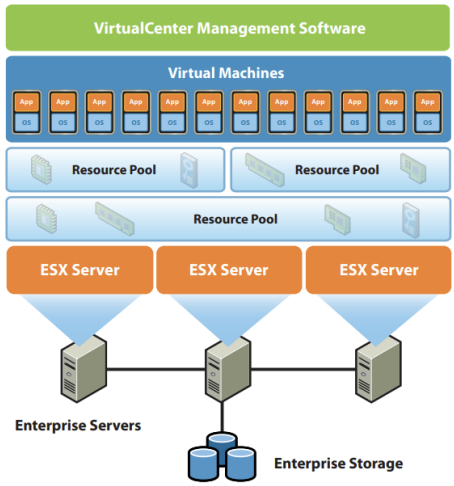
- Type 2: Hosted Hypervisor - Run on a host OS, installed as an application on existing computer OS. Allows a different OS to run on user devices through VMs.

Microsoft Hyper-V Architecture has a Parent Child Partitions

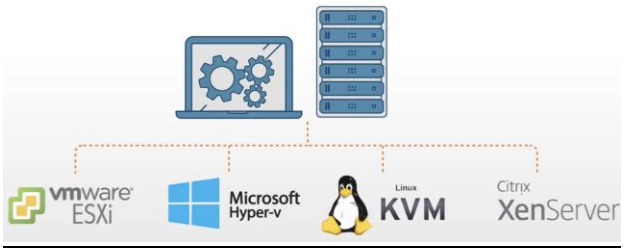
Citrix Hypervisor (Xen) has a Kernal0 vs KernalU

Testing vs Production Environment

- Testing works well on **Type 2** but they have to deal with competition for resources and can be dealing with risks to the OS such as viruses or Malware
- **Type 1** is good for Production for higher stability and no resource competitions



Consolidate many virtual machines on each VMware Infrastructure resource pool.



Advantages of VMM/Hypervisor

- Previously, there were multiple servers for each department within a company due to privacy and fiscal responsibility. Servers rarely utilized more than 5%. A single server can host multiple virtualizations that allow them to use the same hardware but be isolated from each other.
- Reduces cost with consolidation (combining multiple departments virtual but under a single server)
- Containment- Containment gives administrators a general-purpose undo capability. Administrators can suspend a virtual machine and resume it at any time or checkpoint a virtual machine and roll it back to a previous execution state. With this capability, systems can more easily recover from crashes or configuration errors. This leads to less need to upgrade systems every 3-5 years.
- More available, scalable, and management than they were on a physical server for less money
- Easily mobile during Disaster Recovery
- Sandboxes for development that will not affect the physical system
- Resource allocation – if a system has 500gb of ram, it can be distributed as needed between virtual machines. The same is true for all hardware

Security Concerns

- Single point of failure – imagine 5 VM on a single computer but that computer has a hardware failure. Need redundancy
- Denial of service – Hackers – again need redundancy and increased security
- VM escape- attacks the Hypervisor and finds way to gain into other VMs and the host

Describe the Cloud Service Models (who is responsible for what?)

Software as a Service (SaaS) - businesses can access and use software through the Internet. Companies in many industries now use Google Docs and other programs that use SaaS
Platform as a Service (PaaS) - is to be able to develop and deliver applications quickly and reliably.
Infrastructure as a Service (IaaS) - all the resources (e.g., servers, data storage) an IT department needs are located outside of the organization and are accessible by anyone, anywhere.

Attribute	IaaS	PaaS	SaaS
Benefits	▪ Highly flexible and scalable ▪ Easily accessible by multiple users ▪ Cost effective ▪ Useful for businesses of all sizes ▪ Provides complete & discretionary control over infrastructure ▪ Can help slash hardware costs by 50% or more	▪ It's a whole platform ▪ Helps to work with preferred vendors like Amazon, Microsoft, Oracle, SAS, Salesforce, etc. to get custom solutions ▪ Saves time dependent efforts ▪ Don't need an internal development team to build application codes from the scratch ▪ Highly beneficial for large enterprises with specialized applications & requirements	▪ No requirements for infrastructure deployment, software development or delivery, maintenance or operations ▪ Follows a fixed monthly usage billing ▪ Requires minimal input from users
Limitations	▪ Requires a mature operations model ▪ Needs rigorous security stacks ▪ Needs understanding cloud provider technologies ▪ Requires skill & competency in resource management	▪ Entails a vendor lock-in n terms of features ▪ Does not allow extreme customizations ▪ Hard to mitigate from one platform to another	▪ Hard to do custom workflows ▪ Creates a dependency on the service provider to make any improvements in features and reliability

Traditional IT vs. cloud: Managed by customer or provider?

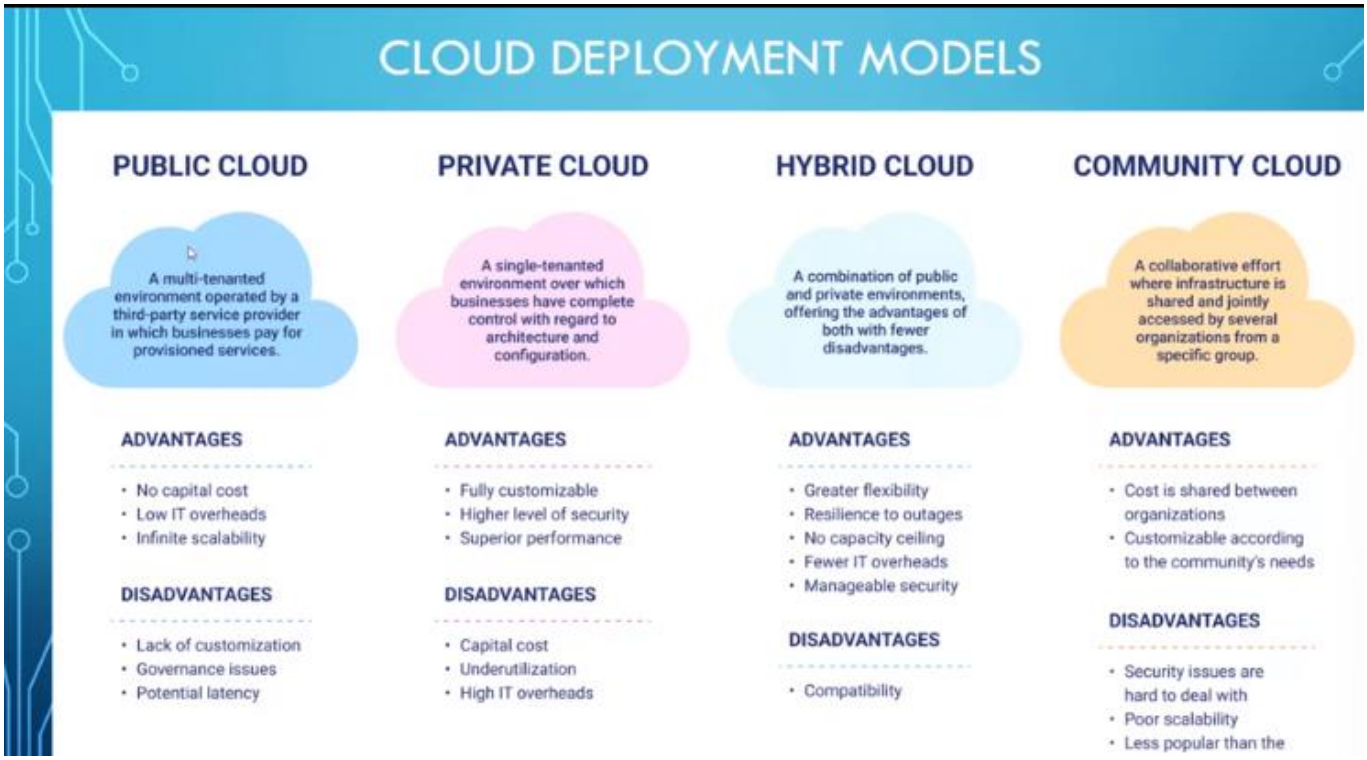
IT function	Traditional IT	IaaS	PaaS	SaaS
Data	Customer	Customer	Customer	Customer
Applications	Customer	Customer	Customer	Provider
Runtime	Customer	Customer	Provider	Provider
Middleware	Customer	Customer	Provider	Provider
OS	Customer	Customer	Provider	Provider
Virtualization	Customer	Provider	Provider	Provider
Servers	Customer	Provider	Provider	Provider
Storage	Customer	Provider	Provider	Provider
Network	Customer	Provider	Provider	Provider

Describe the Cloud Deployment Models

- **Private Cloud:** Single company, on-premises data center. Also possible to have the cloud hosted outside company's data center by leasing a part of a commercial data center, referred to as co-locating, or "co-lo". Allows ownership and control over equipment, sometimes due to regulatory restrictions.
- **Public Cloud:** AWS, Azure, GCP offer public cloud. They maintain ownership and maintenance of underlying infrastructure and facilities. Data is isolated and secure. There is also multi-tenancy where multiple companies share the same resources, but it's not as common.
- **Community Cloud:** Normally at Universities or Gov agencies. Joined and operated by the tenants. Shared between two or more organizations.
- **Hybrid Cloud:** Combination of private and public. For companies that extend applications and services between their own data centers and public cloud provider data centers. Allows ease of access to additional resources during times of demand, or allows public cloud for some

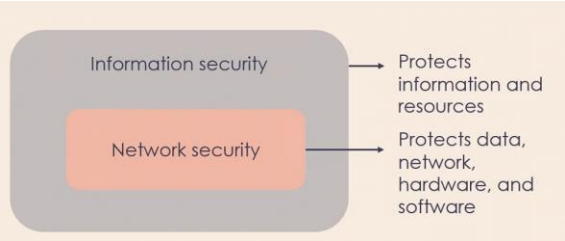
applications, minus the ones that must stay private for regulatory reasons. Dedicated connection between private and public cloud provider must exist through VPN on the internet, or access through a WAN.

- **Multi-Cloud:** Leveraging multiple cloud service provides at one like using both AWS and GCP. Allows redundancy and flexibility, or perhaps some providers do certain things better/cheaper.



Unit 2: Introduction to Network Security

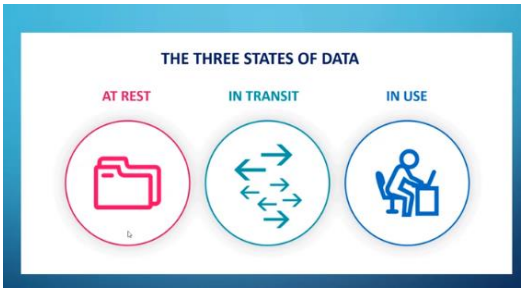
Network Security Overview



Network Security is within the overarching Information Security

Network Security prevents any malicious activities including:

- Misuse
- Modification
- Disruption
- Destruction



Prevention is made at rest and transit

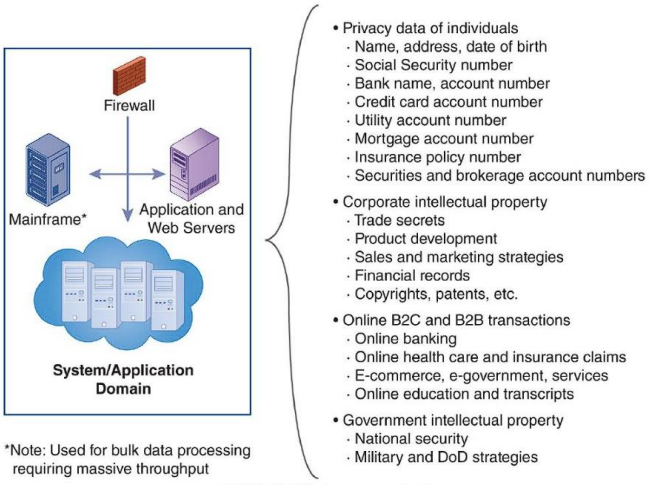


FIGURE 1-4 What are we securing?

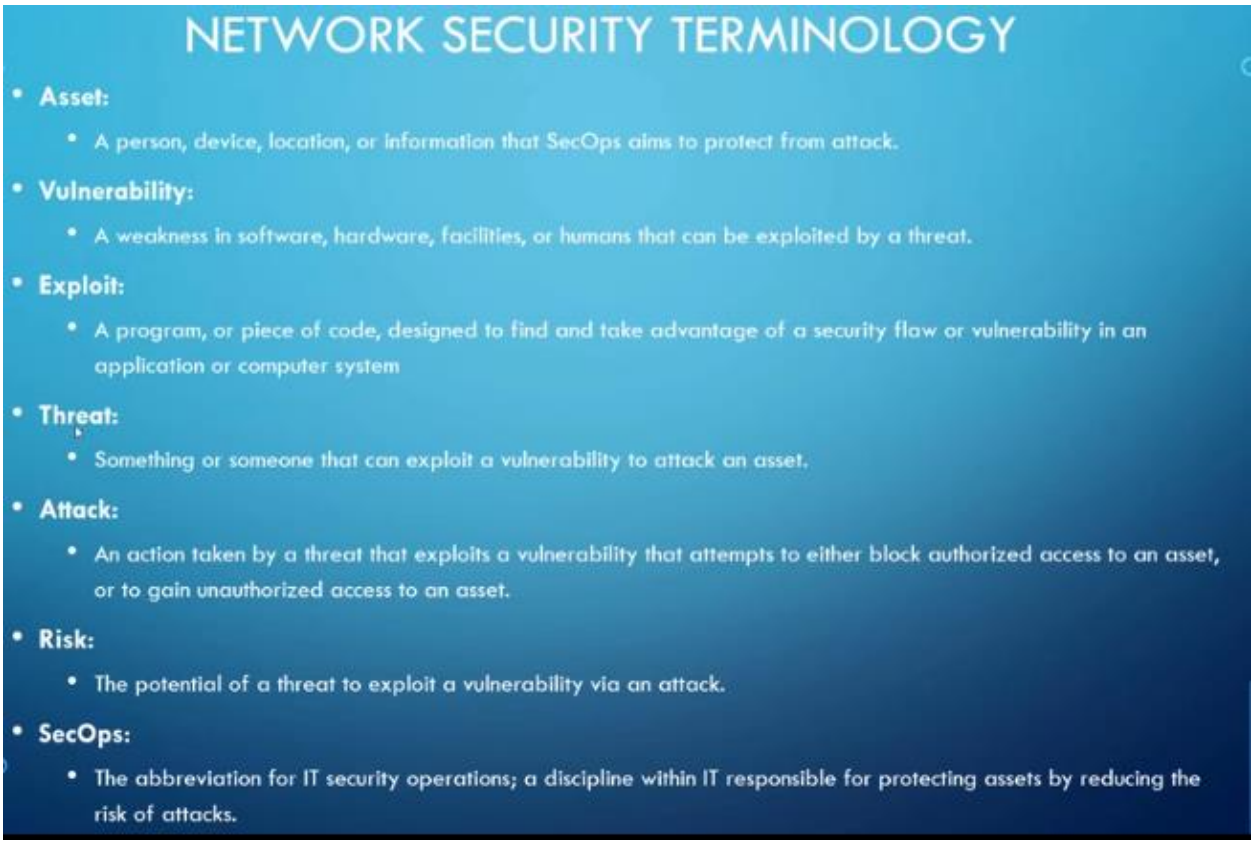
Information Systems consists of the hardware, operating system, and application software that work together to collect, process and store data for individual and organizations. The information system security is the collection of activities that protect the information system and the data stored in it.

An Event vs An Incident –

Event is a measurable occurrence that has an impact on the business while an incident is any event that violates or threatens to violate a company's security policy and that justifies a countermeasure.

Countermeasure – mitigate or address a specific threat

Define each term:



Types of Vulnerabilities

Poor Physical Security: Often measures are taken for technological preventions, but that means little if there are no physical preventions. Securing networks into rooms that with locks, employee card access, and security guards are examples of physical security measures.

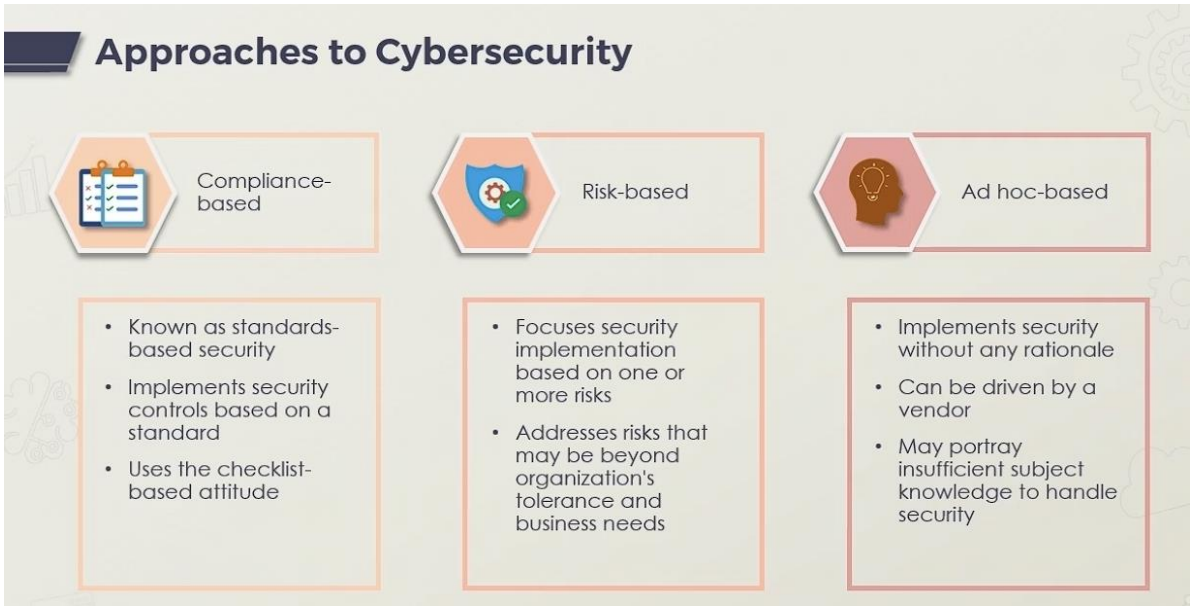
password attack/vulnerability:

- **Weak Passwords** -simple passwords are easy to compromise by guessing or breaking
    - Attacks include : password guessing, brute force attack, dictionary attack
    - Need longer, more complex passwords with 8 character minimum including upper, lowercase, numbers, and symbols

- **Default Password** – passwords that are setup by the company such as routers. Always change the admin default passwords.
- **Misconfigured Firewall Rules**: Config mistakes like leaving default password can allow attackers to gain access. Review all the rules and regularly change passwords.
- **What is the BYOD/Mobile vulnerability:**
    - Mobile Device Management Software: software that allows an organization to monitor, manage, and secure mobile devices such as laptops, smartphones, and tablets that are used in the enterprises network.
    - BYOD allows users to bring their own personal devices to use on the network. They save money but can be a possible security risk especially with malware. Some companies will require their employees to install special approved antiviruses and anti-malware
- **What is an Advanced persistent threats?** (APT) or Advanced Persistent Threat is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organization.
- **What is a Zero-day?** This is when a company first releases a product and the exploit or vulnerability is not known yet. Zero day exploit refers to vulnerabilities not yet known to public, there is no patch available, the software is unpatched. Some IPS (Intrusion Prevention Systems) include an option to forward unknown patterns and firewalls can block devices the first time they see an unknown code.
    - No pattern file exist in the anti-malware software, IDS, or IPS
    - IPS can be configured to block suspicious code patterns and forward to vendor for analysis

Types of Attacks

- **Dictionary attack:** A method of breaking a password by uses a library of commonly used words or phrases to guess possible passwords.
- **Brute Force attack:** A password attack in which the attacker uses all possible combination of characters until a password match is found. It can take thousands of guesses before a password is cracked.



Describe each attack Type:

- **What is a Vulnerability tester?** Penetration testers are security experts who act like bad guys to identify weaknesses in a network. These weaknesses, also called vulnerabilities, must be managed properly to avoid compromise

Describe each security team and hacker:

Threat Actor Examples

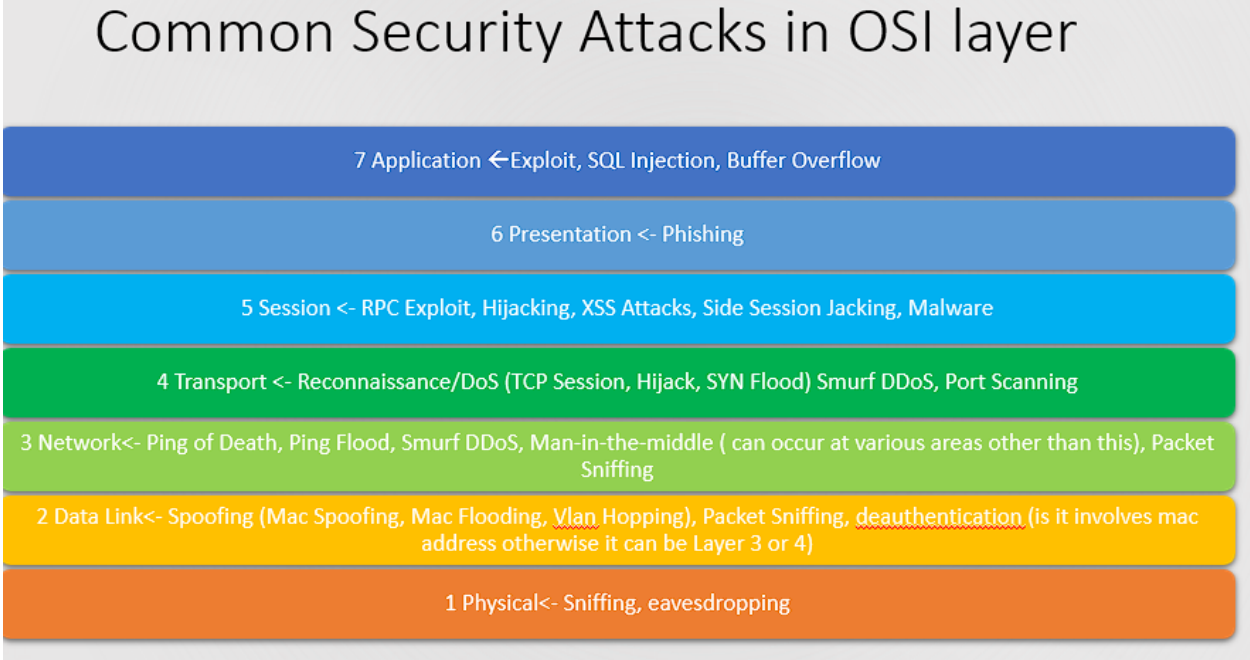
Threat actor	Organization	Government
Nation-state	IP theft	Political information theft Disrupting the functionalities
Hacktivist	Confidential data theft	Web defacement
Cyber criminal	IP theft Credentials theft	IP theft Research data theft
Insider threat	Data leakage Insider fraud	Data leakage

- **Describe a Script Kiddie:** Script kiddie is an unsophisticated individual with little or no skills when it comes to technology. The person uses code that was written by others and is freely accessible on the internet. It might copy a malicious script directly from one website to another , only the knowledge of copy and paste is required. It uses code and probably doesn't understand how it works and what the effect will be.
- **Industrial espionage** is the illegal and unethical theft of business trade secrets for use by a competitor to achieve a competitive advantage. It is often done by an insider or an employee

who gains employment for the express purpose of spying and stealing information for a competitor.

- **Nation States:** Countries attacking each other or stealing IP.

Common Threats and Attacks

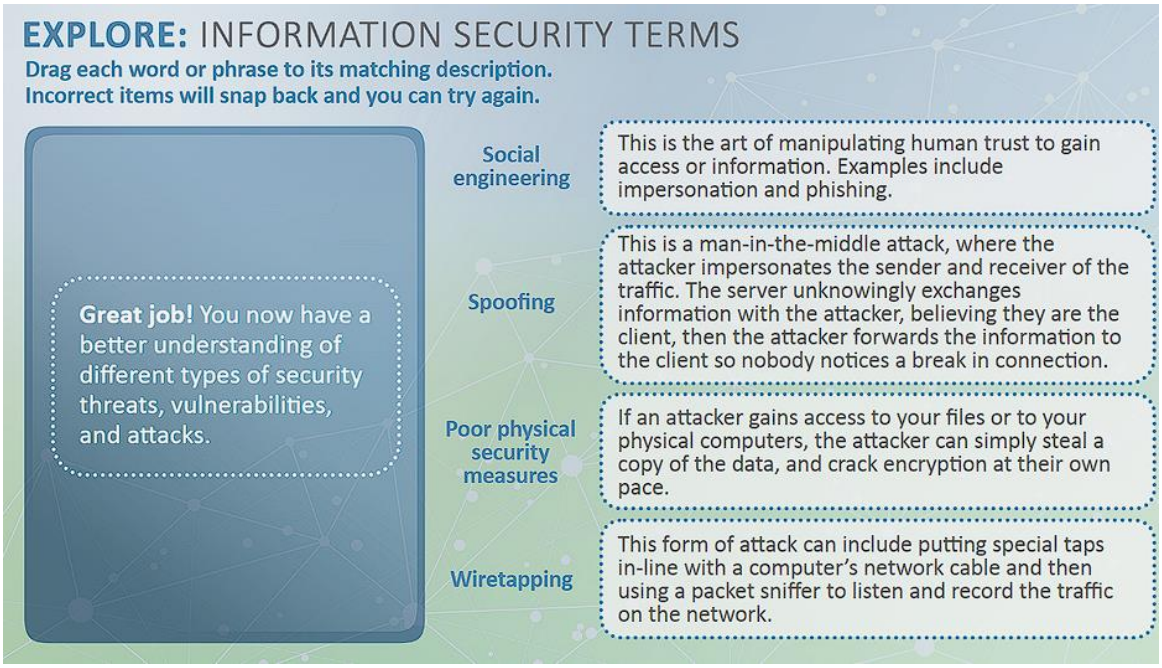


Layer	Threat	Security Solution
7. Application	SQL injection attack	Leverage a reverse proxy system and scan incoming packets for malicious behavior.
6. Presentation	Man-in-the-middle attack	Mitigate by using an application-layer proxy or an IPS, and train users about fake security certificates.
5. Session	RPC attack	Mitigate with regular OS and application patching.
4. Transport	Port scanner	Mitigate by using a packet-filtering firewall.
3. Network	Ping sweep attack	Mitigate by using a packet-filtering firewall.
2. Data Link	VLAN hopping	Configure the VLAN tagging per the switch vendor's recommendations.
1. Physical	Wiretapping	Look for physical vulnerabilities, check the locks on doors, racks, and wiring closets.

COMMON THREATS AND ATTACKS

- **Wiretapping**
  - Packet Sniffer
  - Electromagnetic Field (EMF) eavesdropping
- **Port Scanning**
  - Scan network or computer listening for open ports and services to exploit
- **Taking Control**
  - Run vulnerability scanner against open ports and services to discover exploits
  - SQL Injection: Inserting special SQL commands into input boxes instead of entering basic text
  - Buffer Overflow: Entering text that is too large to fit within a region of memory (buffer) & running executable code
- **Spoofing**
  - Man-in-the-middle attack
- **Denial-of-Service (DOS)**
  - Ping Flood: Attacker sends ICMP echo-request packets with forged source addresses
  - Smurf Attack: DDOS attack where attacker sends a forged ICMP echo-request packet to the broadcast address of a large IP subnet and all computers on the network reply to a victim computer
- **Social Engineering**

- **1. Physical**
  - **Media Wiretapping – Mitigate with Physical Security (locks on doors, equipment racks, wiring closets)**
- **2. Data Link**
  - **VLAN Hopping – Mitigate by configuring the VLAN tagging per the switch vendor's recommendations. All switch ports connected to end devices should be an access port, never a trunk port (disable auto configuration)**
- **3. Network**
  - **Ping Sweep, Ping Flood, Smurf attacks – Mitigate by using a packet-filtering firewall to filter by ICMP packets**
- **4. Transport**
  - **Port Scanner – Mitigate by using a packet-filtering firewall**
- **5. Session**
  - **Remote Procedure Call (RPC) Attack – Mitigate with regular OS and Application patching (updating)**
- **6. Presentation**
  - **Man-in-the-Middle (on-path) attack – Mitigate by using an application layer proxy or an IPS. Also train users about fake security certificates**
- **7. Application**
  - **SQL Injection attack – Mitigate by leveraging a reverse proxy system and scan incoming traffic for malicious behavior. IPS device will also protect against these threats**



- **Packet sniffing** – capturing IP packets off a wireless network and analyzing the TCP/IP packet data using a tool such as Wireshark
- **Describe a SQL injection attack:** injecting Structured Query Language (SQL) commands to obtain information and data in the back-end SQL database
- **Describe a Buffer overflow attack:** attempting to push more data than the buffer can handle, thus creating a condition where further compromise might be possible
- **Describe a Man-in-the-middle attack:** take advantage of the multi-hop process used by many types of networks. It intercepts messages between two parties before transferring them on to their intended destination. Example: web spoofing
- Describe an ARP poisoning attack: **ARP spoofing**: A hacker sends fake ARP packets that link an attacker's MAC address with an IP of a computer already on the LAN. **ARP poisoning**: After a successful ARP spoofing, a hacker changes the company's ARP table, so it contains falsified MAC maps. The contagion spreads

- **What is a Denial-of-service (DoS) attack?** Denying service to a computer, network or network server by overwhelming the victim with large amounts of useless traffic. A computer is used to flood a server with TCP and UDP packets. A DDoS attack is where multiple systems target a single system with a DoS attack. The targeted network is then bombarded with packets from multiple locations. -- Monitor Normal Traffic Patterns to mitigate DoS Attack
- **Describe a Ping of death attack:** A ping of death ("POD") attack involves the attacker sending multiple malformed or malicious pings to a computer. The maximum packet length of an IP packet (including header) is 65,535 bytes. However, the Data Link Layer usually poses limits to the maximum frame size – for example 1500 bytes over an Ethernet network. In this case, a large IP packet is split across multiple IP packets (known as fragments), and the recipient host reassembles the IP fragments into the complete packet. In a Ping of Death scenario, following malicious manipulation of fragment content, the recipient ends up with an IP packet which is larger than 65,535 bytes when reassembled. This can overflow memory buffers allocated for the packet, causing denial of service for legitimate packets.

Describe a Ping flood attack: **UDP Flood:** A UDP flood, by definition, is any DDoS attack that floods a target with User Datagram Protocol (UDP) packets. The goal of the attack is to flood random ports on a remote host.

ICMP (Ping) Flood: Similar in principle to the UDP flood attack, an ICMP flood overwhelms the target resource with ICMP Echo Request (ping) packets, generally sending packets as fast as possible without waiting for replies.

- **What is a Distributed denial-of-services?** DDoS is short for distributed denial of service. A DDoS attack occurs when a threat actor uses resources from multiple, remote locations to attack an organization's online operations. –
    - **Describe a Smurf attack:** (DDoS) attack that exploits Internet Protocol (IP) broadcast addresses and spoofed source addresses to overload a targeted device or network with bogus traffic. It allows an attacker to amplify the amount of traffic generated, with the

goal of overwhelming the target's network or device. (IP found at layer 3 OSI but if it is dealing with transport then it is OSI 4)

  - **Describe the SSL attack:** DDoS attack type that involves sending garbage SSL/TLS requests to the target server. Its aim is to exhaust target server resources and force it to deny service to legitimate users. (SSL/TLS are found at Layer 6 OSI)

- What is **Social Engineering**: methods employed by hackers to gain the trust of an end user so that the hacker can obtain information that can be used to access data or systems. Social engineering typically involves impersonating representatives of legitimate organizations to manipulate people into supplying information such as passwords or personal details. (Research target, make contact, Attack)
- **Describe Impersonation:** a hacker who pretends to be a trusted friend, colleague or business associate of the target in hopes of tricking them into divulging sensitive data or sending fraudulent payments.
- **Describe a Phishing attack:** attacker attempts to trick the victim, via email or instant message, into providing private information such as CCN, passwords, DOB, bank account numbers, ATM pins, and SSN to commit identity theft

Table from Previous Study Guide:

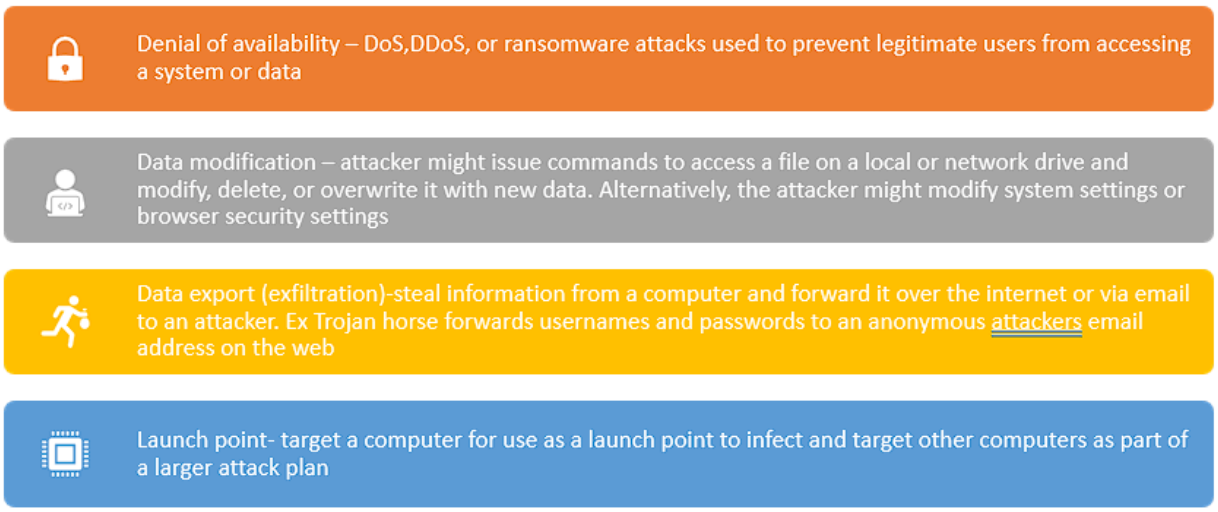
Type	Name	Description	Mitigation/OSI Layer
Database Control	SQL Injection	Attackers take control of the database by entering SQL into the input boxes on a website instead of entering basic text.	Application (7) Review source code & validate all user-entered data. Firewall: use reverse proxy system and scan incoming packets for malicious behavior. Use web-application firewall with rules to filter dangerous requests. Enable NX-bit

			(no-execute) functionality on physical computer.
	Buffer Overflow	Buffer overflow is similar to SQL Injection but instead of SQL, they enter too much information into the form which causes the app to crash or other damage.	Application (7) Coding to prevent too much input. Firewall to prevent suspicious data from being sent. Enable NX-bit (no-execute) functionality on physical computer.
Spoofing	Man in the Middle (MitM)	MitM impersonates both the sender & the receiver to intercept communication between two systems. A hacker hijacks a session between trusted client and network server.	MitM attacks occur in various OSI Layers Although MITM uses IP spoofing at its base, it goes a mile beyond that in order to gain control, by choosing sessions from one or more layers to be hijacked. Intrusion Prevention systems and IPSec can help.
	VLAN Hopping	A method of attacking networked resources on a virtual LAN (VLAN). An attacking host on a VLAN gains access to traffic on other VLANs that would normally not be accessible.	Data Link (2) Configure the switch Access Control File.
Denial of Service	Denial of Service (DoS)	Denying service to a computer, network or network server by overwhelming the victim with large amounts of useless traffic. A computer is used to flood a server with TCP and UDP packets.	Transport (4) – DoS in other OSI Layers DDoS attack blocking, commonly referred to as blackholing, is a method typically used by ISPs to stop a DDoS attack on one of its
	Distributed Denial of Service (DDoS)	A DDoS attack is where multiple systems target a single system with a DoS attack. The targeted network is then bombarded with packets from multiple locations.	customers. Basically, the site is taken down entirely so other sites on the network are not affected.
	Ping of Death	Attacker pings the target & sends a ICMP packet over the max of 65,535 bytes and	Network (3)

		causes the victim's system to crash or stop functioning. Causes buffer overflow and crashes.	Update operating systems. Configure Web Application firewall to drop malformed packets.
	Ping Flood (Starts with Ping Sweep)	A Ping Sweep is an information gathering technique which is used to identify live hosts by pinging them. After the sweep, attacker overwhelms victim's computer with a large amount of ICMP echo-request packets (pings).	Network (3) Configure firewall to disallow pings (stops outside attacks not inside). Use intrusion prevention systems at network and host levels.
	SMURF DDoS (distributed attack)	Rather than one computer sending ICMP packets, multiple computers are replying to the ICMP packet. It spoofs the source address for all ICMP packets	Network(3) & Transport (4) Disable IP-directed broadcasts on your router. Reconfigure your operating system to disallow ICMP responses to IP broadcast requests. Reconfigure the perimeter firewall to disallow pings originating from outside your network.
	Deauth Attack	Deauthentication (abbreviated deauth) is a denial-of-service (DoS) attack where the attacker can force any client (or even every client) off of the network.	Presentation (6) The simplest defense is to use WPA3 security on your WAPs because in WPA3, the management packets are encrypted. If it is not possible to use WPA3, at least use WPA2 to make sure the data traffic is encrypted.
RPC Attack	RPC Exploit	A specially crafted RPC request is sent. Successful exploitation of this vulnerability could execute arbitrary code within the context of another user. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.	Session (5) Mitigate with regular OS and application patching. Use of proxy firewalls and intrusion detection devices can prevent many RPC and NetBIOS attacks.

Social Engineering	Phishing/Spear Phishing	User clicks on a link to a nefarious site which tricks them into entering their name/email address or other secure info. Ie; sending an email about your PayPal account which isn't from PayPal. Spear Phishing targets a person with extremely specific information – hacking a CEO's phone with a specific calendar invite for their kid's soccer practice.	Training on how to recognize & report phishing emails. How to stop at the networking level? I don't know, firewall?? but you should figure this out before taking the test.

Purpose of an Attack



Risk Mitigation

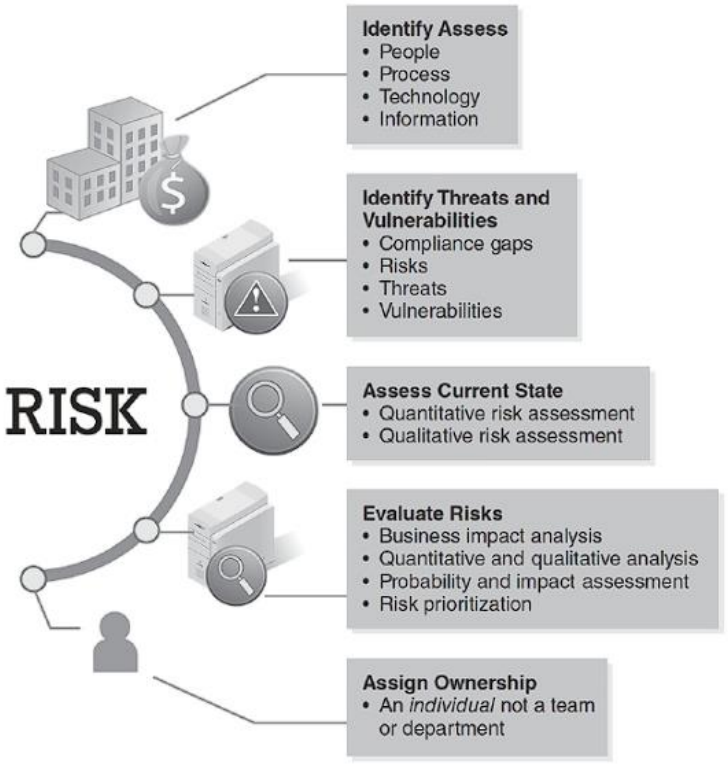


FIGURE 14-8 Network security risk assessment approach.

Quantitative Risk Assessment	Qualitative Risk Assessment
Cost or value of the identified risk and its financial impact are examined	Examined by assigning a rating for each identified risk such as critical, major, minor, high, medium, or low
Alignment with risk transfer strategy	Examine both the risk impact and the likelihood of occurrence
Easy to automate	Realized threat is expressed by insignificant to catastrophic
More objective than qualitative analysis in that it attempts to describe risk in financial terms	Fairly subjective
Drawback is that many risks have difficult-to-measure values	Helps to determine most critical risks
Numerically based and Financially objective	Needs diverse input from a pool of people from different departments to understand the ripple effect
	Scenario based and oriented

- **What is Honeypot:** It's a sacrificial computer system that's intended to attract cyberattacks, like a decoy. It mimics a target for hackers, and uses their intrusion attempts to gain information about cybercriminals and the way they are operating or to distract them from other targets.
- **Proactive and Preventative Measures:** Constantly use multiple tools and methods in an overlapping methods such as IP within Network, Firewall, and Anti-Malware on Servers

Threats and Mitigation - Wireless

Threat	Description	Mitigation
War Driving	Looking for an open wireless network while driving in a car	Decrease the wireless range Hide the SSID
War Chalking	Marking the area after SSID and credentials are known	Use WPA2 Enable MAC filtering Disable SSID
WEP/WPA Cracking	Scanning and determine the pre-shared key	Use stronger encryption protocol, such as WPA2
Evil Twin	Setting up a rogue AP for the legitimate users to sniff the data	Wireless Intrusion Prevention Systems (WIPS)
Rogue Access Point	An access point installed on the network without IT team's knowledge	Switch port tracing Monitor Mode Scanning Rogue Detector AP

Threats and Mitigation - Network

Threat	Description	Mitigation
ICMP flood	Sends large number of ICMP packets to a system	Disallow ICMP packets on the firewall
DoS/DDoS	Puts a system or network to a halt after saturating its resources	Monitor the normal traffic patterns Compare signatures of the incoming traffic Use anti-DoS/DDoS device
Fraggle	Sends spoofed UDP packets to a specific broadcast address	Disable IP broadcast Disallow ICMP packets on the firewall
Buffer Overflow	Puts more data in the buffer it can handle	Detect vulnerabilities in the code

Threats and Mitigation – Web Applications

Threat	Description	Mitigation
Injection	Injects malicious data or script in a web application	Use server-side validation Validate and sanitize the input data
Broken Authentication	Use brute-force and dictionary attacks to gain access	Implement multi-factor authentication Implement complex passwords
Sensitive Data Exposure	Theft of encryption keys and MITM attack on clear text data in transit	Avoid storing sensitive data Encrypt data in transit Disable caching
Security Misconfiguration	Attack on default user accounts or default configuration	Disable unnecessary services/features Harden the devices/OS

Risk Mitigation Response:

Detective controls – Identify that a threat has arrived. Intrusion detection system (IDS) is an example. It will then log the activity

Preventative Controls- used to stop threats from coming into contact with a vulnerability. EX Intrusion prevention system (IPS)

Corrective controls – reduce the effects of a threat. Forensics and incident response are examples

Deterrent controls – deter an action that could result in a violation. This suggests to not take a specific action where preventative controls do not allow the action to occur

Compensating Controls – implemented to address a threat in place that does not have a straightforward risk-mitigating solution

Risk Mitigation

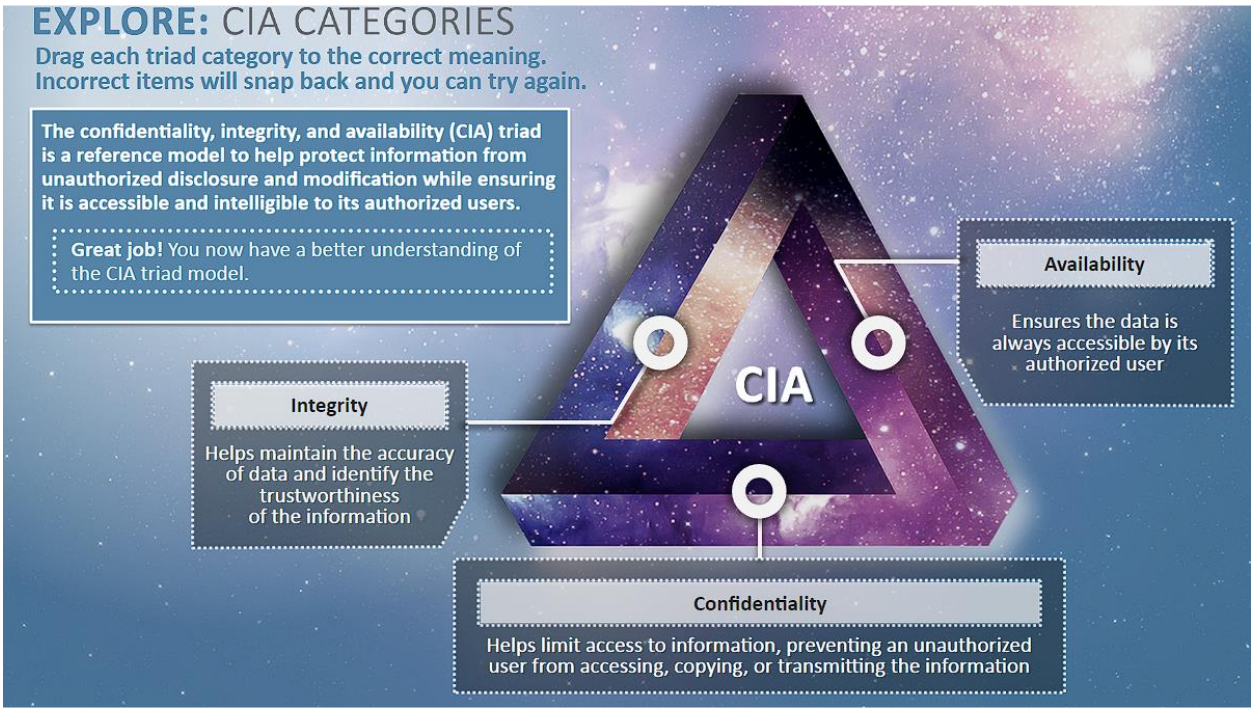
- Risk Acceptance: When a business decides to not take any action to reduce the risk because they feel the cost of mitigating risk outweighs any potential loss from the risk.
- Risk Avoidance: A business decides to eliminate a particular risk by getting rid of its cause.
- Risk Mitigation: A business works to decrease the possibility of the occurrence of the risk.
- Risk Transfer: A business shifts the potential loss due to a risk to a 3rd party. Such as an insurance company

Conducting a Network Security Risk Assessment

Risk is of great concern to organizations that are under a regulatory compliance law or mandate. Compliance laws and standards for each vertical industry have specific requirements for network security and privacy. This includes but is not limited to:

- **FERPA**—The **Family Educational Rights and Privacy Act (FERPA)** has a data security checklist of requirements for defense-in-depth or layered security requirements or educational delivery organizations.
- **FISMA**—The **Federal Information Security Modernization Act of 2014 (FISMA)** has several families and control requirements for network security, access controls, remote access, and security assessments for U.S. federal government agencies and contractors. Updated in 2014, it was formerly named the Federal Information Security Management Act.
- **GDPR**—The **General Data Protection Regulation (GDPR)** defines requirements for security of personally identifiable information (PII) data, security assessments, and data privacy assessments.
- **GLBA**—The **Gramm–Leach–Bliley Act (GLBA)** has a Safeguards Rule definition that requires the organization to build a security program and conduct periodic risk assessments for banking and financial institutions.
- **HIPAA**—The **Healthcare Insurance Portability and Accountability Act (HIPAA)** has several control requirements for access controls, network security, remote access, and performing security assessments for health care organizations.
- **PCI DSS**—The **Payment Card Industry Data Security Standard (PCI DSS)** has specific security control requirements for networks, firewalls, switches, audit and monitoring, security assessments, and incident response for merchants and service providers for accepting and processing credit card transactions.

Confidentiality, Integrity, and Availability (CIA) Triad



Confidentiality

Confidentiality keeps information secret from unauthorized users. You can lock safes, post armed guards, or whisper in someone's ear in a remote field to ensure confidentiality, but these tactics often are insufficient. Cryptography makes information unintelligible to anyone who does not know the encryption cipher and the proper key. Only authorized users or, eventually, an effective cryptanalysis can get this knowledge. The value of confidentiality is straightforward in that disclosing certain communications that contain confidential information could either harm the correspondents or help an opponent, and, in many cases, a successful attack achieves both goals simultaneously.

Authentication

Authentication confirms the identity of an entity, whether that be the sender, the sender's computer, a device, or information. Humans instinctively authenticate each other based on personal characteristics, such as facial appearance, voice, or skin texture. A traditional military authentication method is a password given to a sentry: If you give the correct password, then the sentry lets you pass. If you do not, you're in trouble. In the digital realm, cryptography provides a way to authenticate entities, the most straightforward of which is a user ID and password. Note that this form of cryptography does not provide strong authentication because anyone else who obtains this fixed information can provide it to the recipient, who will think the user is legitimate.

Nonrepudiation prevents a party from denying a previous statement or action. As an example, suppose an investor sends an email to a broker that states, "Buy 1,000 shares of XYZ at 50." Shortly after the exchange executes the order, XYZ stock drops to 20, upon which the investor denies the buy order and says it was really a sell order. How could you resolve this situation?

Using asymmetric key cryptography, you can prove mathematically—usually to the satisfaction of a judge or jury—that a particular party did indeed originate a specific message at a specific time. The fundamental principle of asymmetric key cryptography is that it uses a key pair to encrypt and decrypt and the originator is the only one who knows one of the keys, which has an irrefutable timestamp. The

Integrity

Integrity ensures that no one, not even the sender, changes information after transmitting it. If the receiver possesses the correct key and uses the right cipher and a message does not decrypt properly, someone or something probably changed the ciphertext in transit.

In addition, cryptography can enforce integrity with hashes or **checksums**, which are one-way calculations of information that yield a result that is usually much smaller than the original message and is difficult to duplicate. For example, a simple checksum of the phone number 1-800-555-1212 could be the sum of each digit, or 30. Even knowing the checksum, you could not re-create the phone number, but you can tell whether the phone number matches the checksum. If one digit is changed,

Unit 3: Network Security Operations

Firewalls

Firewalls control the flow of traffic by preventing unauthorized network traffic from entering or leaving a particular segment of a network.

Firewalls can be placed between an internal network and the outside world or within internal subnetworks to control access to particular corporate assets by only authorized users.

Simplest firewalls support access control lists (ACLs) which define rules for handling traffic from one or more hosts using a specific protocol and one or more ports.

Firewalls can filter traffic based on ports aka port security

Implicit deny – firewall deny's all messages except the ones that are explicitly allowed

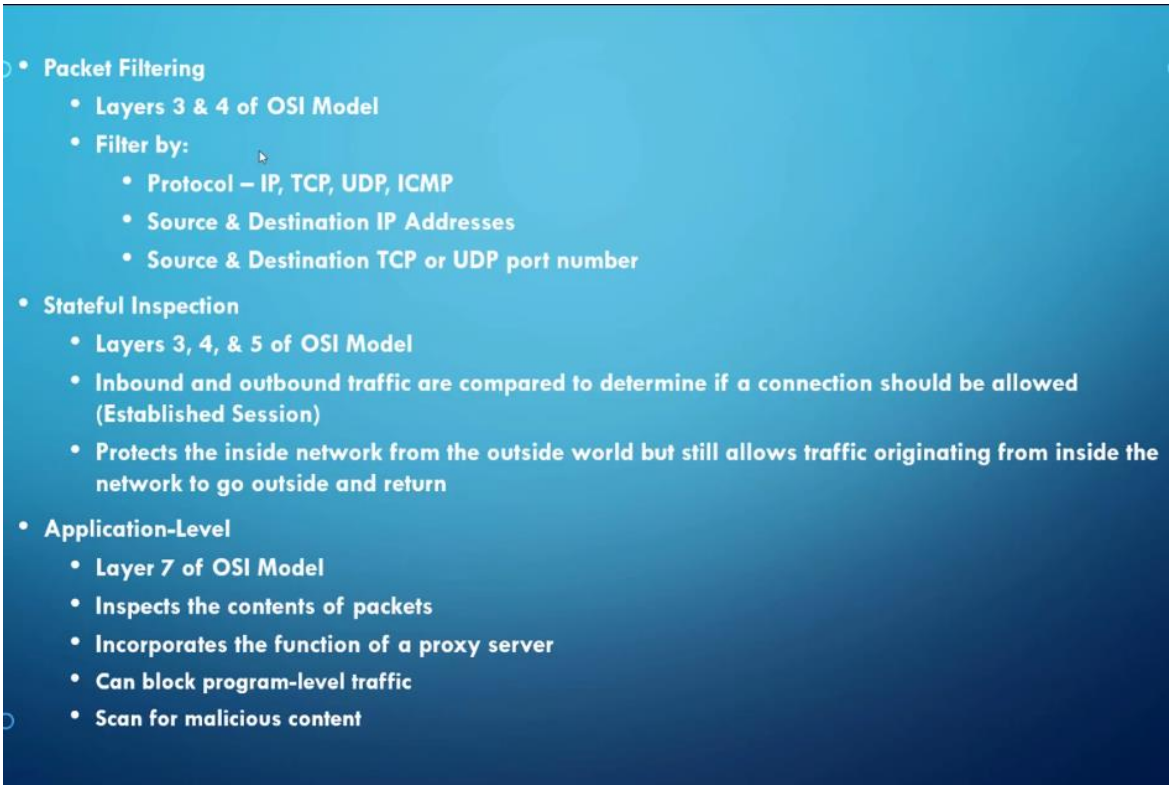
Firewalls can operate as detective controls and can log as much information as can be analyzed. Not just a prevention tool

Types of Firewalls

Packet filtering – compares received traffic with a set of rules that define which traffic it will permit to pass through the firewall. It has no memory of past packets

Stateful inspection – remembers information about the status of a network communication. It will remember from the first packet until the communication is closed. Firewall checks rules only when a new communication session starts.

Application proxy – It opens separate connections with each of the two communicating systems and then acts as a broker or proxy between the two, which allows for an added degree of protection so the firewall can analyze the information about the application in use when making the decision to allow or deny traffic



Firewall Filter Features

Flood guard – rules that limit traffic bandwidth from hosts

Loop protection – look at message addresses to determine whether a message is being sent around an unending loop (another flood form)

Network segmentation – filtering rules enforcing divisions or separations between networks, thus keeping traffic moving from one network to another

Most Firewalls run at the OSI 3 and 4 layer

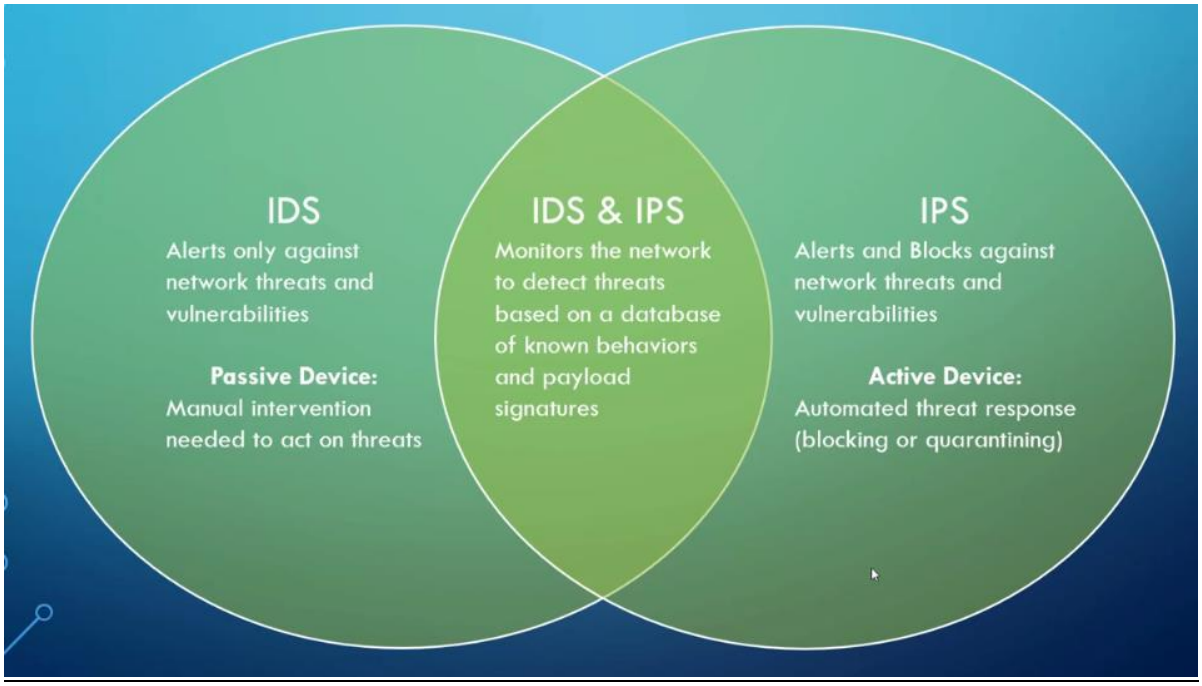
- **What is a Circuit Level Gateway?** TCP/UP based on port numbers. Type of firewall that operates on the **Session layer** of the OSI model. Instead of inspecting packets by header/source or port information, it instead maintains a connection between two hosts that is approved to be safe. This is something akin to a parent who approves the people that their children can speak with on the phone once they trust those people. In this scenario, the parent does not have to listen

into the conversation because they know they can trust the two communicating children. Similarly, a circuit-level gateway establishes a secure connection between two hosts that have been authenticated and trust each other. Foundation of NAT and PAT because it changes the IP address and TCP/UDP port numbers to allow network communication.

- **The router or firewall is responsible for implementing NAT and PAT.**
    - Network Address Translation (NAT): NAT, in which the Private IP address or local address are translated into the public IP address. NAT is used to slow down the rate of depletion of available IP address by translates the local IP or Private IP address into global or public ip address. NAT can be a one-to-one relation or many-to-one relation.
    - Port Address Translation (PAT): In PAT, Private IP addresses are translated into the public IP address via Port numbers. PAT also uses IPv4 address but with port number.
- **Web Proxy:** a server that filters the and limits access to undesirable, forbidden, or dangerous content. Used by schools and workplaces to filter where users are allowed to go on the Internet.

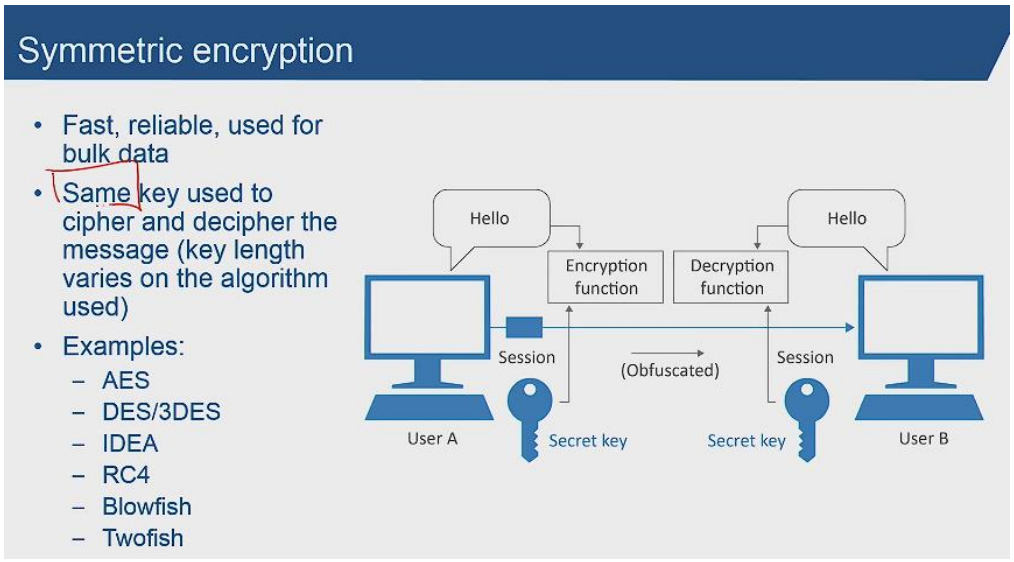
Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) identify malicious traffic based on known behaviors and payload signatures. **IDS monitors the network**, and **IPS intercepts and blocks threats.**

These can be physical devices or virtual appliances (applications).



- IDS and IPS have both a host version (HIDS/HIPS) and a network version (NIDS/NIPS). Network versions are devices places in strategic points in the network to provide protection from attacks. Host versions are software that is installed on all the devices in the network to the devices against attacks.

Encryption Fundamentals

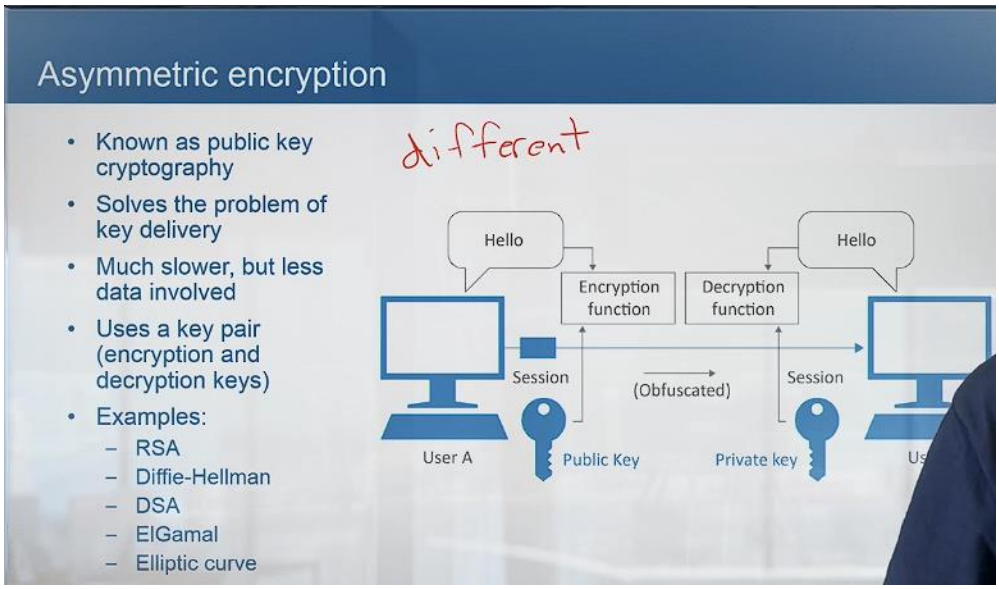


Symmetric Encryption: (Same key to encrypt and decrypt)

A Key Management System (KMS) generates a key that combines with the data to encrypt it. The encrypted data is then stored in a system along with the key. The KMS then generates a master key to encrypt the key stored with the data. The master key does not leave the KMS. Since the first key that is stored with the data is encrypted, anyone without the master key will not be able to decrypt the first key to decrypt the data.

In order to access the data, it must first enter the KMS, where the KMS will use the master key to decrypt the key with the data, and then that key is used to decrypt the data. The key with the data is considered symmetric because it's used to encrypt and decrypt the data it is stored with. The master key is also sometimes called the key-encryption key. It must be protected from being lost or compromised. The solution is to encrypt the master key with another one, then encrypt that one with another key. Usually there are not more than 3 or 4 keys. The keys are rotated periodically to help keep them from getting compromised. An example of symmetric encryption is the Advanced Encryption Standard (AES): Several version, such as AES 128 and AES 256, the latter being mostly used today in enterprise-type applications such as banking or credit

cards. Depending on key length, up to 14 transformations can be made in a single block of data, making it almost impossible to reverse the encryption. AES is a symmetric key that allows encrypting and decrypting data with the same key. Symmetric keys are known to encrypt and decrypt at very high speeds.



Describe Asymmetric Key Encryption:

Asymmetric Encryption: (Different keys to encrypt and decrypt)

An example of Asymmetric encryption is HTTPS, the S initially stood for Secure Sockets Layer (SSL). SSL has since been deprecated and replaced with Transport Layer Security (TLS). The sender and the user use two different keys to access data. Another example of asymmetric encryption is Internet Protocol Security (IPsec). Used f or encryption of traffic in-flight on an existing network. The two keys used in asymmetric encryption involve a public key and a private key. Together, they are used to set the encryption. The public key is held by the public at large by the Public Key Infrastructure (PKI). PKI is an asymmetric key solution that allows two parties to exchange encrypted data without having first exchanged a private or shared key with one another.

In PKI systems, each party that could either send or receive encrypted data must first create a key pair consisting of a public key and a private key. The key pair is created using an algorithm that enables one key to decrypt ciphertext that the other key has encrypted. Once the pair is created, the public key is published to a public repository, whereas the private key is kept secret by the owner of the key. If you wish to send this person an encrypted file, you would retrieve their public key from the internet and then use it to encrypt the file.

You could then send the encrypted file to the person or even post it for them to download. The only way to decrypt the file is to use the recipient's private key, which should be stored in a very safe place. An example is visiting an HTTPS website, where it has a TLS certificate. This certificate is published by a well-known provider. The browser will check to see if the certificate is valid, if so, the website server will have a private key, that is known only to that server. The server will then use the private key to go back and sign the communication. PKI can also be used to validate integrity of data. This is because if someone who has the public key decrypts your data, they cannot re-encrypt it since they do not have your private key. This guarantees that if someone can decrypt your data it has not be changed since it was signed (encrypted). A downside to asymmetrical encryption is that there is large computational power needed to encrypt large data.
In simple terms: Public Keys in asymmetry will be used for ENCRYPTION and will be labelled the name of the person who is decrypting. Private Key in asymmetry will be used for DECRYPTION and will be the name of the person holding the private key

Example: Dave is sending a Message to Joanna using asymmetric cryptography algorithm What key should she use to ENCRYPT the message? It would be a Public Key and it would be Joanna's

Advantages and disadvantages summary

	Advantages	Disadvantages
Symmetric	• Fast processing • Can encrypt and decrypt large amounts of data without compromising speed • Extremely secure (if the right algorithm is used)	• Management becomes exponentially more complex as keys are added • No possibility to secure the transfer of the key • Does not offer any other security functionality but confidentiality
Asymmetric	• Secures transfer of symmetric key • Easy to manage key ecosystem • Provides additional security services (non-repudiation, authentication, etc.)	• Slow processing • Can be used for shorter data only • Requires additional software to manage infrastructure (PKI)

- **What is Public Key Infrastructure (PKI)?** Certificate management (PKI/CA) – not explained in the video this is certificate authority and public key infrastructures (also known as private trust); digital certificates indicating they can protect sensitive data, provide unique digital IDs to users, and applications and secure end-to-end communications
- **Describe SSL/TLS and what is it mostly used for:** TLS for application data – not explained in the video – Transport Layer Security (TLS) prevents unauthorized access of messages when they're sent over the internet connection (currently 1.3). These two protocols provide secure connections between the client and server for exchanging information. They also provide server authentication (and optionally, client authentication) and confidentiality of information transfers.
- **Describe IPSec and what is it mostly used for:** IPSec is a set of communication rules or protocols for setting up secure connections over a network. Internet Protocol (IP) is the common standard that determines how data travels over the internet. IPSec adds encryption and authentication to make the protocol more secure. IPSec is often used between firewalls to be able to encrypt data between those devices.


HYBRID CRYPTOGRAPHY
GENERATES PUBLIC & PRIVATE KEYS
SENDS PUBLIC KEY TO SENDER
RECIPIENT
SENDER
ENCRYPTS FILE WITH SYMMETRIC ENCRYPTION BY USING THE PUBLIC KEY RECEIVED
SENDS PRIVATE KEY WITH ASYMMETRIC CRYPTOGRAM
MESSAGE

Cloud Security

Classification of data

- How secure does the data need to be?
  - *Sensitive*. Highest classification, release would cause great harm to the enterprise.
  - *Confidential*. Medium classification, release would cause some harm to the enterprise.
  - *Private*. Must be protected but likely will not cause harm to the enterprise if released (for example, certain types of PII).
  - *Public*. Available to be released to the public that will not cause harm or will cause very little harm to the enterprise.
- In what state is the data?
  - *Data in transit*. Data being transmitted between two end-points.
  - *Data at rest*. Data being stored in some type of persistent media.
  - *Data in use*. Data actively being process or stored in memory.

- **Application Security:** Use authentication service Federated Identity Management to allow users to authenticate to your app through Federate Identity Servers at Google, Facebook, Twitter, etc. where they already have an account. Once verified, the server sends a token value, which will be used to identify the user. The token value for the user will remain the same every time they are authenticated.

- **Network Security:** Any publicly accessible server is exposed to attack. Isolate public-facing servers when possible. Host servers on public cloud or private extranet where there are firewalls in place. Make more than one layer of defense so if an attacker penetrates it, they are faced with another barrier. Public servers should not be directly reachable for administration, but rather should be behind a firewall and only accessible through a Virtual Private Network (VPN) or dedicated Wide Area Network (WAN).

Cloud Security Measures

- **Private Cloud:** Scalable, single-tenant (one company) clusters of computing, storage, and networking resources, typically located in that tenant's data center. The owner is fully responsible for everything.
- **Public Cloud:** Hosted by companies like Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP). Highly scalable, multi-tenant solutions in data centers around the world. Public cloud providers responsible for physical data center and hardware security concerns.
- **Hybrid Cloud:** Combination of services running in private and public cloud. Security belong to who owns the equipment, with the addition of the data link between the two networks which is often maintained by a third party.

Wireless Security

Wi-Fi Security protocols in order of Weakest to Strongest:

	WEP	WPA	WPA2	WPA3
Brief description	Ensure wired-like privacy in wireless	Based on 802.11i without requirement for new hardware	All mandatory 802.11i features and a new hardware	Announced by Wi-Fi Alliance
Encryption	RC4	TKIP + RC4	CCMP/AES	GCMP-256
Authentication	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-Personal WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Data integrity	CRC-32	MIC algorithm	Cipher Block Chaining Message Authentication Code (based on AES)	256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)
Key management	none	4-way handshake	4-way handshake	Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA)

3DES: (Triple DES). Antiquated symmetric encryption using DES three times in a row. DES is only 56-bit and can be compromised easily by brute force with modern equipment.
AES: Advanced Encryption Standard (AES) is a symmetric key algorithm. It is very secure today, but with advances in quantum computing, may not be safe for long. Can use 128-bit, 192-bit, and 256-bit keys. Longer keys are exponentially harder to crack but use more cpu. Most sites today use AES-256. AES New Instructions
(AES-NI) allow CPU to process encryptions at very high speeds, can encrypt and transmit at native wireless speeds.
WEP: Wired Equivalent Privacy. WEP key 10 or 26 hexadecimal digits, each digit 4 bits, so 40-bit or 104-bit. Can be compromised today easily with modern hardware. WEP superseded by WPA.
WPA: Wi-Fi Protected Access. Uses variable-length alphanumeric passphrase, ranges from 8 to 63 characters. Has Temporal Key Integrity Protocol (TKIP) encryption process, which gives significant security boost by generating new, unique 128-bit encryption key for every packet.
WPA2: Like WPA but has mandatory support for Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), which is part of AES. Provides data confidentiality, authentication, and access control.
WPA3: Like WPA2 but minimum key strength increased to 192-bits for enterprise. Eliminates passphrase or key that WEP, WPA, and WPA2 use to join personal-mode wireless networks. Instead uses Simultaneous Authentication of Equals (SAE) method to exchange network key (eliminates need to tell others the key before connecting). WPA3 also has Perfect Forward Secrecy (PFS) which ensures a compromised key will only affect data exchange for that encryption session. WPA3 also doesn't allow de-association (Deauth Attacks) after encryption established.
Ad-hoc: All wireless communication is peer-to-peer, does not involve a WAP. Usually used to set up a new device (camera or printer).
Infrastructure: Most cases use a WAP (wireless router) to connect our wireless devices to the internet. The WAP acts like an ethernet switch in a wired network and often has a physical cable to attach it to other networks.

Security Standards: 802.1x Security Standard: Provides network access control at the port level, whether physical or wireless, and an authentication standard based on Extensible Authentication Protocol (EAP). Uses RADIUS or EAP to forward network request, then validates based on credentials. 802.1x also can check for version num of antivirus and malware scanners on a pc, which can be configured as a requirement for access.

Wireless Attack Types:

Deauth Attack: Deauthentication is a Denial-of-Service Attack where the attacker can force clients off a network, even without joining that network. This prevents access to the network, forces users to reconnect to
the attacker's fake access point, and captures the 4-way handshake of WPA to gain access to the client network. Best defense is to use WPA3 with a long, complex passphrase because management packets are encrypted.

Fake Access: When an attacker gets a victim to connect to their own WAP. Best defense is to never use unsecured Wi-Fi, but if you absolutely must, use a VPN.

User Authentication and Access Control

There is a difference between Access Control and Access Controls. Access Control are the theoretical parts of the standard known as AAA while Access Controls are the way to protect resources. Access control list (ACL) is made up of rules that either allow access to a computer environment or deny it.

Parts of Access Control

Identification – Who is asking to access the asset? This process determines the identity of the subject. First step of Authorization. This is done with assigned identifiers like username, ID, or an account number. Nonrepudiation is in place so each user is unique

Authentication- Are the requestors' identities verified to be claimed identities.

Authorization-what, exactly, can the requestors access? And what can they do? This is a process of deciding who has access to which computer and network resources (see video references on authorization groups)

Accountability- how can actions be traced to an individual?

Policy Definition Phase – Authorization

Policy Enforcement Phase – Identification, authentication, authorization execution, and accountability

Physical Access Controls – Control access to physical resources such as buildings, parking lots, and protected areas. Another example is smart cards programmed with employee's ID number

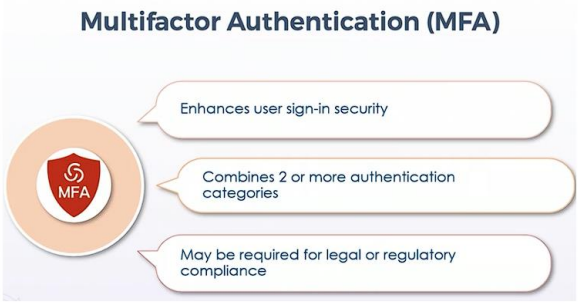
Logical Access Controls – Control access to a computer system or network. Ex a username and password allow personnel to use an organization's computer system and network resources

Authentication

7 types of Authentication

1. Knowledge –pin, password, passphrase
2. Ownership –smart card, key, badge, token
3. Characteristics –fingerprint, retina, or signature – something you are
4. Action/Perform –reproducing a signature – something you can do
5. Behavior – something you exhibit
6. Location – Somewhere you are
7. Relationship – someone you know

Multifactor Authentication (MFA)



Authentication Categories

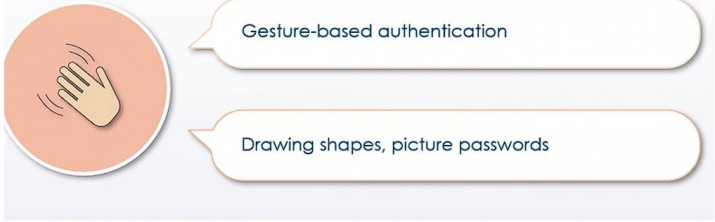
Something You Know

Something You Are

Somewhere You Are

Something You Have

Something You Do



Policies and Procedures for Accountability

Step 1 –identified Step 2- authenticated step 3- Authorized. Final step Accountability

Accountability is the last part of access control process.

Accountability involves tracing an action to a person or process to know who made the changes to the system or data, which is important for conducting audits and investigations as well as tracing errors and mistakes.

Accountability is done by:

1. Log Files – records detail who logged onto the system, when they logged on, and what information or resources they used.
2. Monitoring and Reviewing
3. Data retention, Media Disposal, and Compliance Requirements
    1. HIPPA –privacy of personal health data and gives patients rights to information
    2. FACTA-requires any entity that keeps consumer data for business purposes to destroy before discarding
    3. CCPA – California Consumer Protection Act
    4. GDPR – requirements on how long to retain data when disposal is mandatory

Formal Models of Access Control

Discretionary Access Control (DAC) – owner of the resource decides who gets in and changes permissions as needed

Mandatory Access Control (MAC) – permission to access a system or resource is determined by the sensitivity of the resource and the security level of the subject. Permissions cannot be transferred

Nondiscretionary Access Control – closely monitored by security not the system admin

Rule-Based Access Control – A list of rules, maintained by the data owner, determines which users have access to objects

Attribute (ABAC) – temporary based such as location or time based access

Context-based (CBAC)- advanced firewall deep packet inspection looking at the contents of the packets and how the packets are grouped together.

Role-based Access Control (RBAC) – assigning permissions to users based on their role within the organization. Ex Software engineer would have access to GCP, AWS, and Github while Finance role would have access to Xero and ADP.

DAC

- Owner of the resource decides who gets in and permissions can be transferred
- Operating systems
- Applications

MAC

- Determine level of restriction by how sensitive the resource is, which is represented by a sensitivity label or classification.
- Owner and system jointly make the decision to allow access
- Government, Military, Intelligence agencies

NAC

- Rules are closely managed by security admin not the system owner or ordinary users
- Can be used on Many Operating systems
- More secure than DAC does not rely only on users' compliance with organizational policies
- System security is monitored, enforced and tamperproof
- Less administrative overhead of MAC

RAC

- Access is based on a list of rules that determine who should be granted access
- Success depends on how much the data owners are trusted because AC pushes much of the administration to them
- Useful for technical and security-conscious users but not for many users

Centralized Access Control

CAC – single common entity such as an individual, department, or device, decides who can get into systems and networks

Centralized Authentication Services are applied and enforced through the use of Authentication, Authorization, and Accounting (AAA) servers

AAA benefits

1. Involves less administration time. Users accounts are maintained by a single host
2. Reduces design error
3. Reduces Security Administrator training
4. Improves and eases compliance auditing because access requests are handled by a single system
5. Reduces help-desk calls because UI is consistent

RADIUS (AAA Types)

RADIUS – Remote Authentication Dial-In User Service (popular as of 2021)

Authentication server that uses two configuration files

1. Client configuration file that contains the client address and the shared secret for transaction authentication
2. User configuration file that contains the user identification and authentication data as well as the connection and authorization information

Authentication Steps:

1. NAS (Network Access Server) decrypts the user's User Datagram Protocol (UDP) access request
2. NAS authenticates the source
3. NAS validates the request against the user file
4. NAS responds by allowing or rejecting access or by requesting more information

TACACS+ (AAA types)

Terminal Access Controller Access Control System Plus – Internet Engineering Task Force (IETF) standard that uses a signal configuration file to:

1. Control server operations
2. Define users and attribute/value pairs
3. Control authentication and authorization procedures

Developed by CISCO systems before being released as an open standard

Steps in authentication process:

1. Using TCP, the client sends a service request with the header in cleartext and an encrypted body containing the user ID, password, and shared key
2. The reply contains a permit/deny as well as attribute/value pairs for connection configuration, as required

DIAMETER (AAA types)

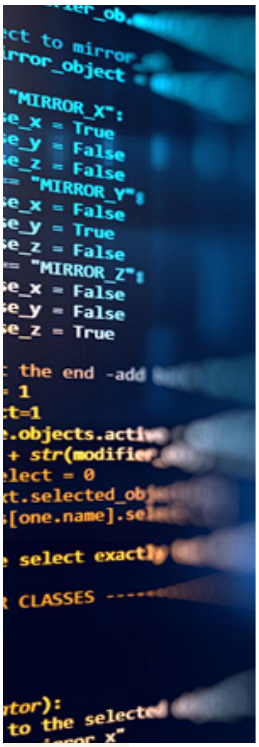
DIAMETER is a protocol based on RADIUS that defines how AAA server should communicate and operate. It only works in a highly fluid or mobile workforce. Works well in stable and static workforces

Protocol includes:

1. Base protocol – defines the message format, transport, error reporting, and security used by all extensions
2. Extensions- conduct specific types of authentication, authorization, or accounting transactions.

Datagrams – messages sent from computer applications using UDP to other hoses on an IP network without requiring special transmission channels or data paths

DIAMETER uses UDP in P2P mode rather than client/server. In P2P mode a user provides another user with direct access to his or her drive and in turn the second user also has access to the first user's hard drive. No centralized structure exists



SAML (AAA type)

- Security Assertion Markup Language (SAML) – open standard used for exchanging both authentication and authorization data.
- Based on Extensible Markup Language (XML)
- Designed to support access control needs for distributed systems
- Now completely centralized AAA system but rather a data forma specification.
- Depends on central trust authority to issues security tokens

Decentralized Access Control

DAC handles access control decisions and administration locally

In the hands of the people closest to the system users

Confusion can occur due to loss of standardization ad to overlapping rights

DAC eliminates the single-point-of-failure problem and ends perception that central controlling body cannot respond effectively to local conditions

Examples of DAC:

1.Password Authentication Protocol (PAP) – cleartext usernames and passwords

2. Challenge-Handshake Authentication Protocol (CHAP) – more secure than PAP because it hashes the password with a one-time challenge number to defeat eavesdropping-based replay attacks

What is Multifactor Authentication: an use of access controls under authentication by knowledge. Multi-factor authentication involves the use of two or more methods or factors of proving and verifying user identity.

Device Hardening

What is device hardening? System hardening is a way of reducing vulnerabilities to decrease the risk of cyberattacks.

Approaches to securing any network

1. Removing network connectivity to sensitive resources
2. Adding countermeasures to protect the network and any sensitive resources

Approaches to securing any network focus on

1. Countermeasure number
2. Type
3. Placement

Network Device Hardening: Countermeasure categories

A centralized device to protect the entire network – all network traffic flows through a single security device. It examines every packet for malicious intent

A dedicated countermeasure for each device or resource – each resource connected to the network has an embedded security device or security device between the resource and the network

A countermeasure for each type of threat- compromise between the two previous approaches. Several security devices are attached to the network that filter traffic with one particular type of attack. Ex one for DoS and DDoS attacks; another for unauthorized reconnaissance

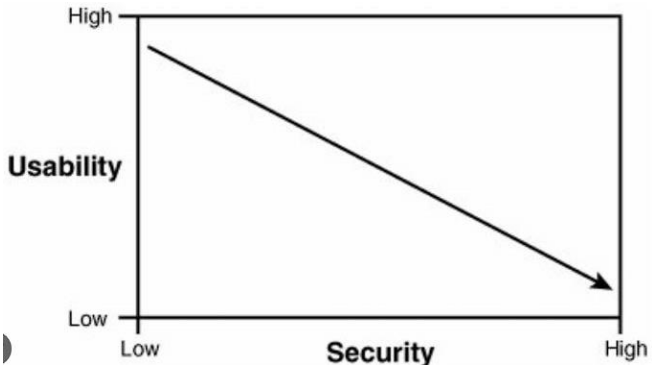
Examples of Countermeasures Taken

Least privilege – limiting access to users based on the level of permissions they need to perform their duties

Separation of duties- breaking a task into subtasks so that different users must carry them out; prevents one person (except the person who assigned the duty) the ability to know how to do all of the parts of the task

Job rotation – minimizes risk by rotating employees among various systems or duties and thus prevents collusion

Mandatory vacations – suspend access to the organization's environment preventing them from working from home



Usability	Usable security	Security
• Effectiveness • Efficiency • Accuracy • Learnability • Memorability • Satisfaction • Additional factors	• Least surprise • Good security now • Standardized security policies • Consistent, meaningful vocabulary • Consistent placement of controls	• Confidentiality • Integrity • Availability • Authenticity • Additional factors

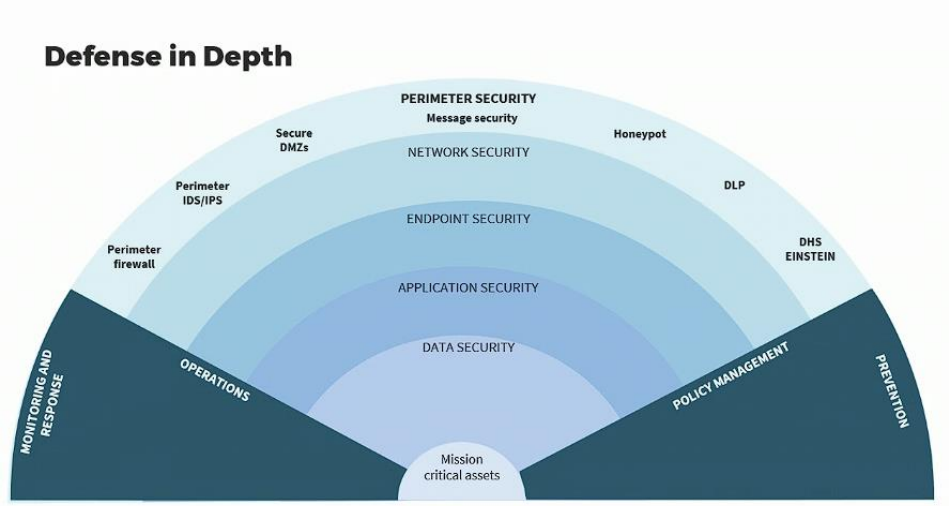
It is important to balance between Usability and Security

Multilayered defense (DiD)- multiple countermeasures that an attacker must compromise to reach any protected resource. It is often known as series of concentric rings around protected resources or defense in depth

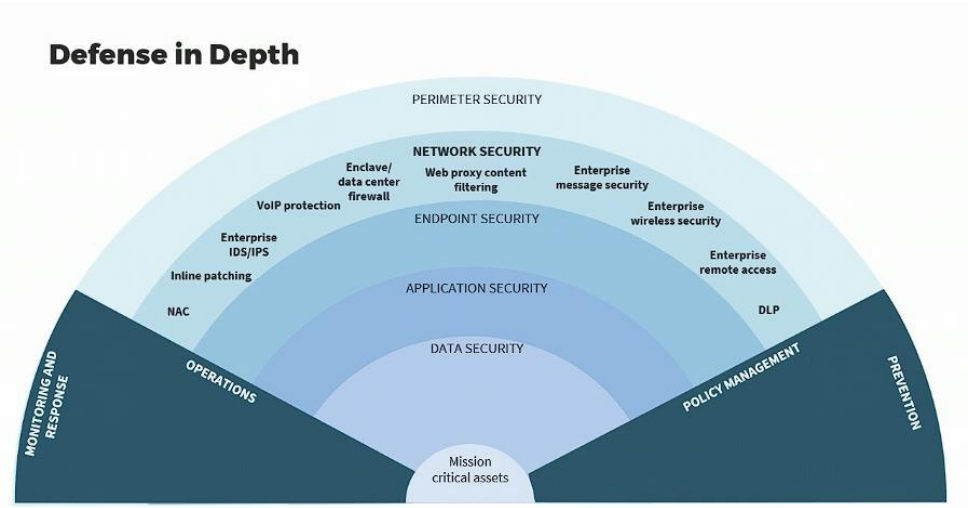
Defense in Depth or DID

1. Referred to as layered defense
2. Using the least privilege and DID principles is a function of “due care”
3. Should be systematically planned and designed with outward-in or inward-out approach
4. Can be applied to physical security or technical controls
5. Can technically be deployed physically or virtually

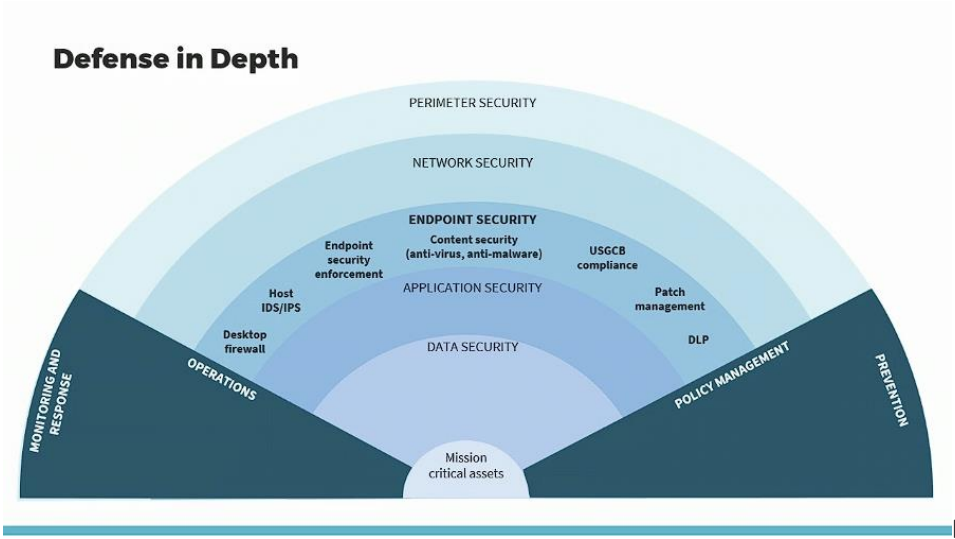
Different levels of Defense in Depth (visual representation to help with the concepts)



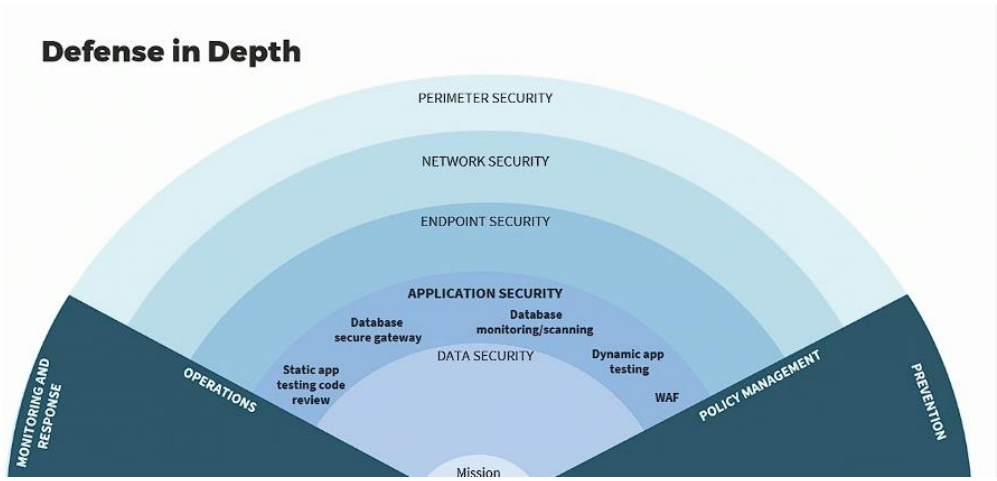
Perimeter Security



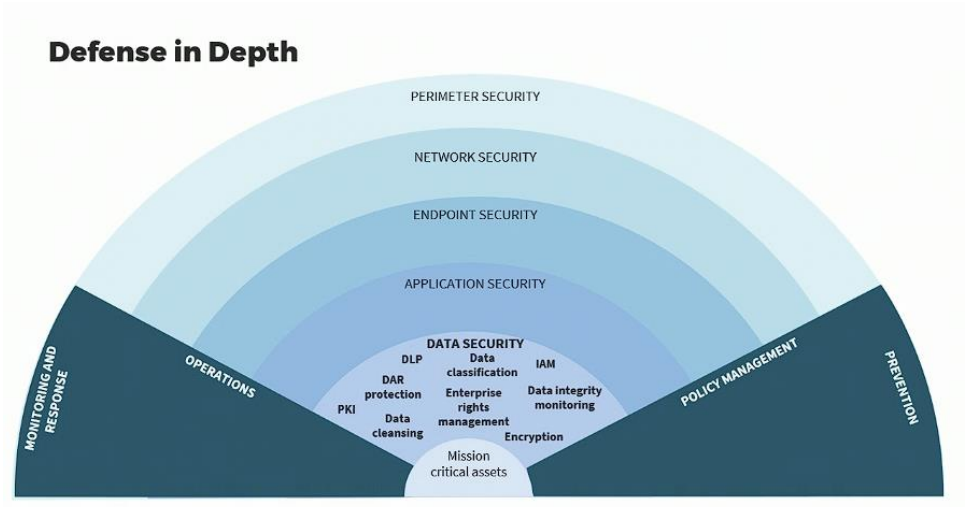
Network Security



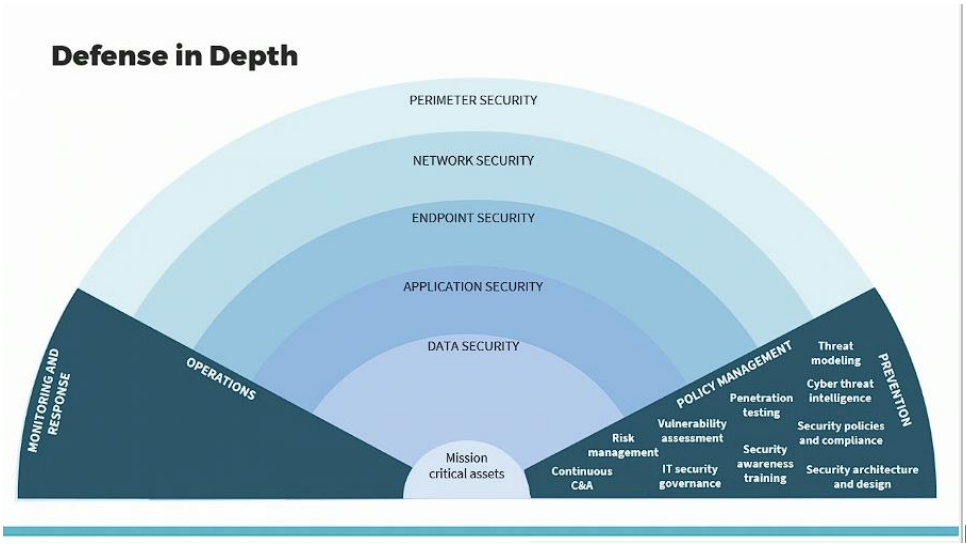
End point security



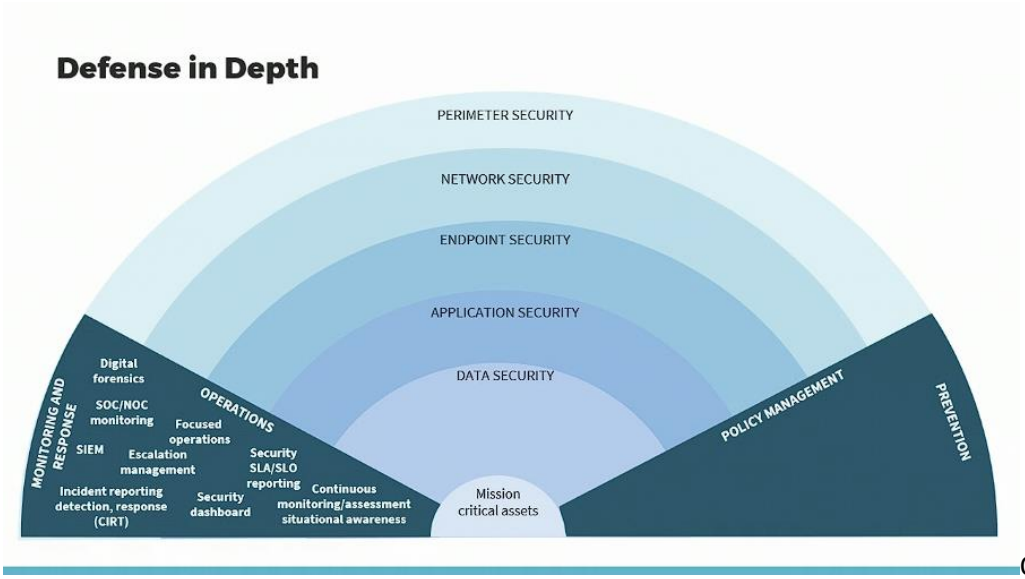
Application Security



Data Security



Policy Management



Operation

Management

Section 3 Lesson 1.1-1.11 (common material on the exam yet not included in the guide) (if you watch no other videos, watch this string of videos for this section

https://wgu.percipio.com/courses/d24c3b97-baa6-47bd-b3cf-517d281e6985/videos/afcf690e-b12f-4dae-bd07-f37eccfc29f0?sharelink=lJ5DOnc-s

Acceptable Use Policy (AUP) – an agreement between two or more parties that outlines the appropriate use of access to a corporate network or the internet. Describes what users may or may not do when accessing the network.

What is included in (AUP)

1. Data access and disclosure
2. Data Retention
3. Asset Custodianship
4. Passwords
5. System Access
6. Clean desk policy
7. Removable device policy
8. Web Surfing
9. Augmented reality
10. BYOD

Ingredients in Privacy Policy

Intellectual property (IP) – organizational secrets, copyrights, digital rights, formulas, future products, marketing campaigning…etc

Personal Identifiable information (PII) – ID numbers, addresses, preferences..etc

Personal Health Information (PHI)

Asset Classification Policy -Policy defines requirements for the appropriate classification of Institutional Information and IT Resources to ensure their confidentiality, integrity and availability.

Asset Management Policy -provides a set of guiding principles, intentions, goals and methods for asset management. The policy provides a template for decision-making so people can achieve the best possible outcomes for each task while meeting the organization's goals.

Economy of Mechanism – Keep things simple, determine essentials and remove what is not needed.

Complete Mediation – Request Access must happen every time and not circumvented

Open Design – Security is independent of its design. Algorithm must be open and accessible. Security must not be dependent on design

Least Common Mechanism – Prevent unintentional sharing. Use separation of duties and compartmentalization.

Human Centered Design

Human-centered design focuses on solving root issues (not just symptoms) with people as the central focus, adopting a systems view, and engaging in continuous prototyping and testing.

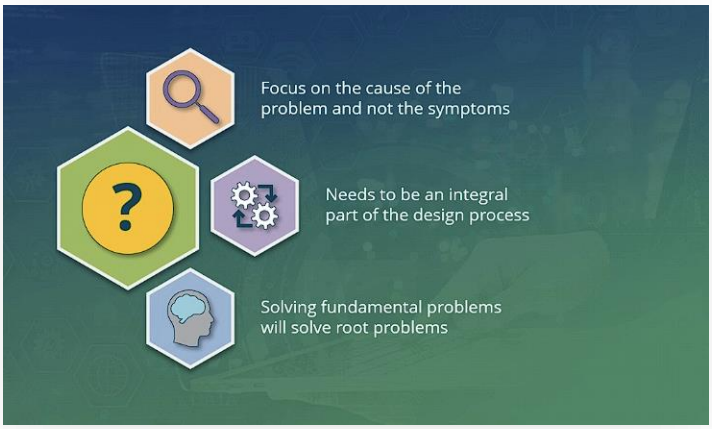
1. Focus should be on people and not tech
2. Take into account the history, culture, and beliefs of the group
3. Focus on the situation motivation and expected outcomes

Look at all parts (holistically)

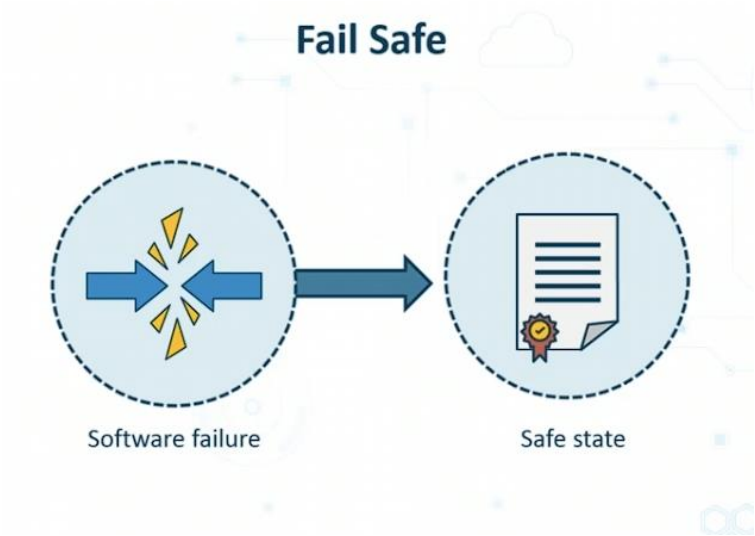
Improving one part should not weaken another part

Returning should be as easy as purchasing the item

Prototyping and testing -Iterative process (small parts at a time) with feedback, and testing should always be real use



Fail/Safe



Fail Safe is a measure needed to make sure that if there is a failure that it can enter a safe state without compromising the system. Errors and Exceptions occurs but they fail safely then return to normal function. Fail-safe design ensures that systems fail securely without compromising security, with errors and exceptions handled predictably and acceptably. This design also emphasizes the adoption of principles like "deny by default."

One Fail Safe Principle is Explicit Deny by Default so when it fails it does not fail to an open state to allow for more access to attackers.

Error Codes should then be used instead of messages so they are not easy to understand from the outside.

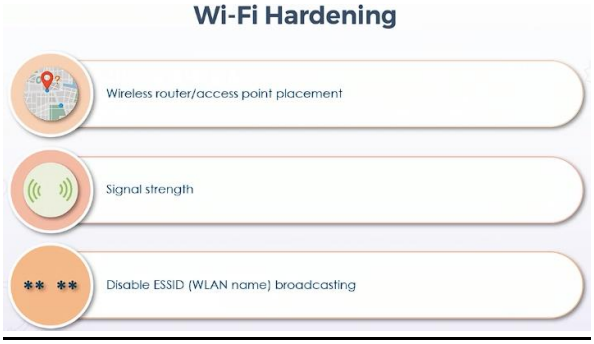
Psychological Acceptability: Any perceived difficulty due to the security system design will cause users bypassing security. Psychological acceptability refers to the idea that security systems should be user-friendly and not impede users' tasks, as complex security measures might lead to bypassing and compromises.

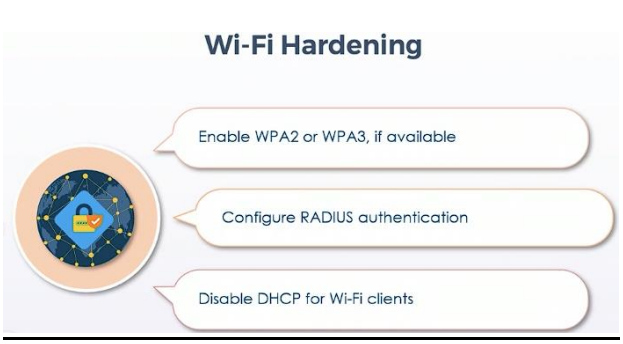
Users should understand risks involved, why controls exist, and effectively.

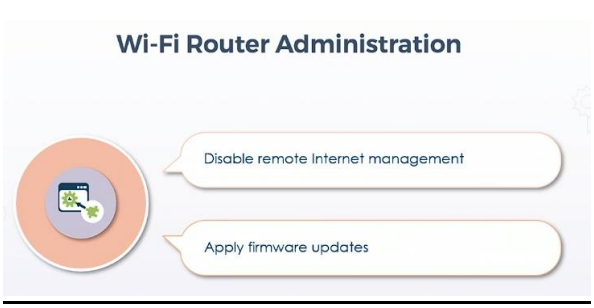
Security should be transparent, simple and easy like passwords and screen layout

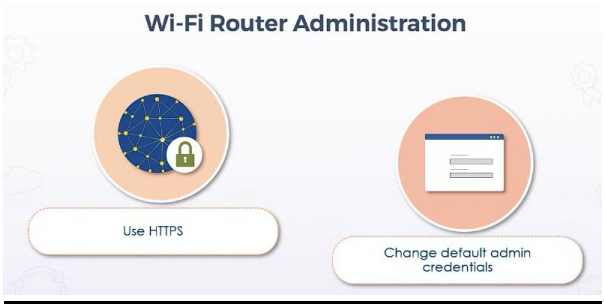
Additional Sections that did not have questions on the study guide but should be reviewed

Section 3 Lesson 3.6









Section 3 Lesson 4: What is IT Governance?

- OECD defined corporate governance as the system by which business corporations are directed and controlled
- IT governance is the framework for the leadership, organizational structures and business processes, standards and compliance to these standards, which ensures that the organization's information systems support and enable the achievement of its strategies and objectives

Drivers to adopt IT Governance Strategies

1. Requirements in the UK of the Corporate Governance Code and the Risk Guidance; for US-listed companies, Sarvanes-Oxley; for banks and financial institutions BIS and Basel 2/3; and for businesses everywhere the requirement of their national corporate government regimes
2. Increasing intellectual capital value that organization has at risk
3. The need to align tech projects with strategic organizational goals and to ensure that they deliver planned value
4. The proliferation of threats to information and information security
5. Increase in the compliance requirements of information and privacy-related regulation, particularly the EU GDPR and regulations inspired by it.

Effective Management of Risk in information and IT

1. Organization's strategic deployment of IT in order to achieve its business goals
    a. Transparency with which they are planned, managed and measured, and the way in which risks are assessed and controlled
2. The way in which the risks associated with information assets themselves are managed

Section 3 Lesson 5: Security Governance

Federal Regulations and where they tend to apply

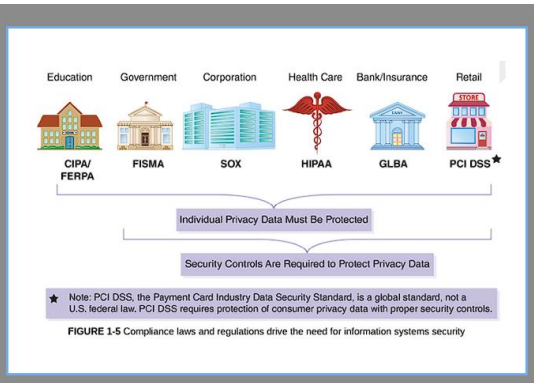


FIGURE 1-5 Compliance laws and regulations drive the need for information systems security

Compliance Laws and Regulations Drive the Need for Information Systems Security

Cyberspace brings new threats to people and organizations. Individuals need to protect their privacy, and businesses and organizations are responsible for protecting both their intellectual property and any personal or private data they handle. Various laws require organizations to use security controls to protect private and confidential data. Current laws and regulations related to information security include the following:

- **Federal Information Security Management Act (FISMA)**—Passed in 2002, FISMA requires federal civilian agencies to provide security controls over resources that support federal operations.
- **Federal Information Security Modernization Act (FISMA)**—Passed in 2014, FISMA was enacted to update FISMA 2002 with information on modern threats

as well as security controls and best practices.

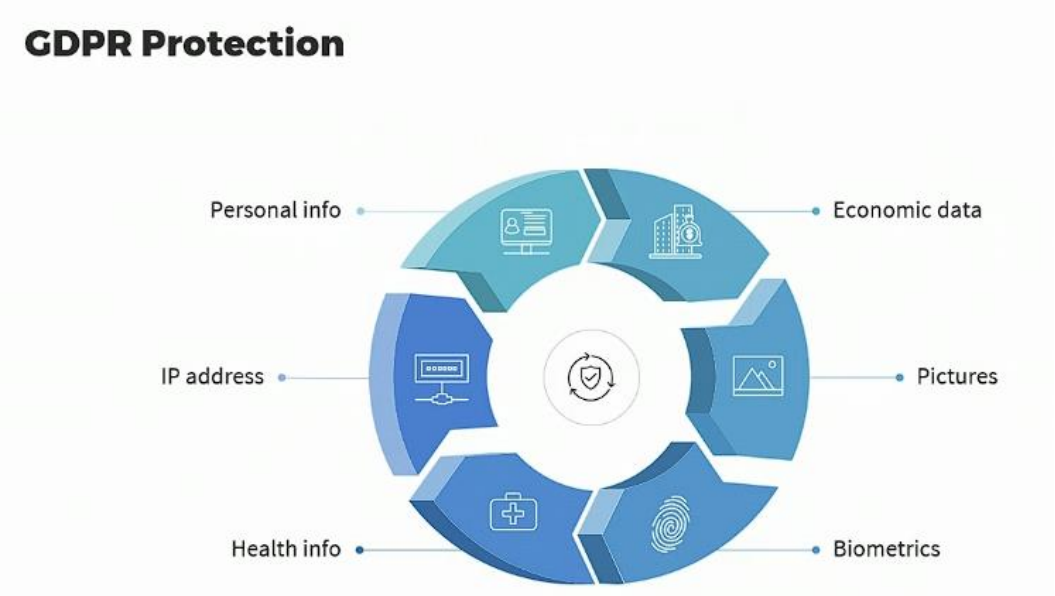
- **Sarbanes-Oxley Act (SOX)**—Passed in 2002, SOX requires publicly traded companies to submit accurate and reliable financial reporting. This law does not require securing private information, but it does require security controls to protect the confidentiality and integrity of the reporting itself.
- **Gramm-Leach-Bliley Act (GLBA)**—Passed in 1999, GLBA requires all types of financial institutions to protect customers' private financial information.
- **Health Insurance Portability and Accountability Act (HIPAA)**—Passed in 1996, HIPAA requires health care organizations to implement security and privacy controls to ensure patient privacy.
- **Children's Internet Protection Act (CIPA)**—Passed in 2000 and updated in 2011, CIPA requires public schools and public libraries to use an Internet safety policy. The policy must address the following:
  - Restricting children's access to inappropriate matter on the Internet
  - Ensuring children's security when they are using email, chatrooms, and other electronic communications
  - Restricting hacking and other unlawful activities by children online
  - Prohibiting the disclosure and distribution of personal information about children without permission
  - Restricting children's access to harmful materials
  - Warning children on the use and dangers of social media
- **Family Educational Rights and Privacy Act (FERPA)**—Passed in 1974, FERPA protects the private data of students and their school records.

General Data Protection Regulation (GDPR) – Most known privacy law in the European Union but applies to any organization that conducts business in the EU

Regulations include

1. Standardization of privacy rules
2. Implementation of privacy requirements
3. Ensuring the privacy of personal data

Data Protection Regulation include how data is collected, stored, and used.



PIPEDA – Personal Information Protection and Electronic Documents Act – Federal privacy legislation for Canadian private sector organizations. It promotes trust and data privacy in ecommerce. Governs the collection, use, and disclosure of personal information.

PIPEDA Fair Information Principles found at priv.gc.ca

Principle 1 – Accountability

An organization is responsible for personal information under its control. It must appoint someone to be accountable for its compliance with these fair information principles.

Principle 2 – Identifying purposes

The purposes for which the personal information is being collected must be identified by the organization before or at the time of collection.

Principle 3 – Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Principle 4 – Limiting collection

The collection of personal information must be limited to that which is needed for the purposes identified by the organization. Information must be collected by fair and lawful means.

Principle 5 – Limiting use, disclosure, and retention

Unless the individual consents otherwise or it is required by law, personal information can only be used or disclosed for the purposes for which it was collected. Personal information must only be kept as long as required to serve those purposes.

Principle 6 – Accuracy

Personal information must be as accurate, complete, and up-to-date as possible in order to properly satisfy the purposes for which it is to be used.

Principle 7 – Safeguards

Personal information must be protected by appropriate security relative to the sensitivity of the information.

Principle 8 – Openness

An organization must make detailed information about its policies and practices relating to the management of personal information publicly and readily available.

Principle 9 – Individual access

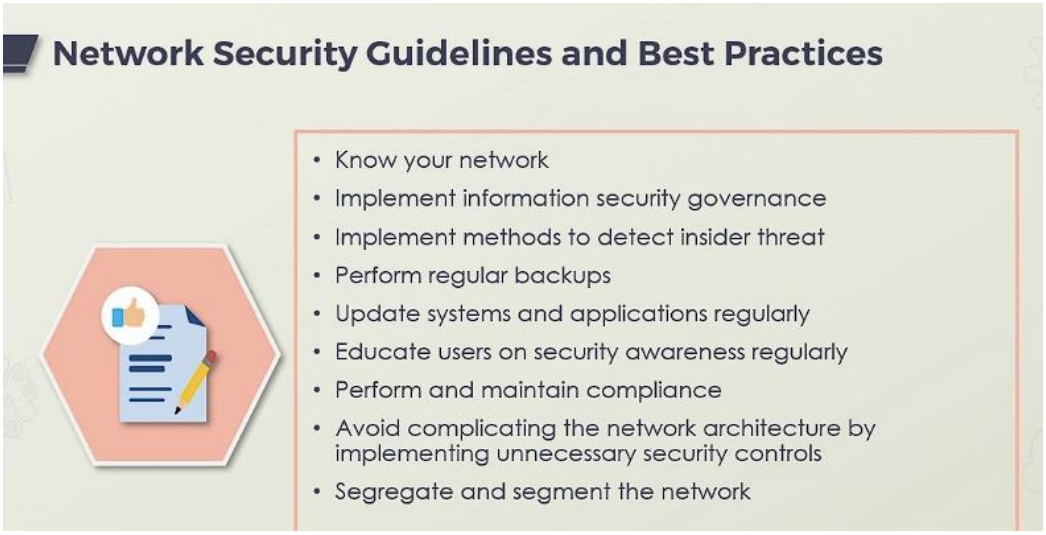
Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

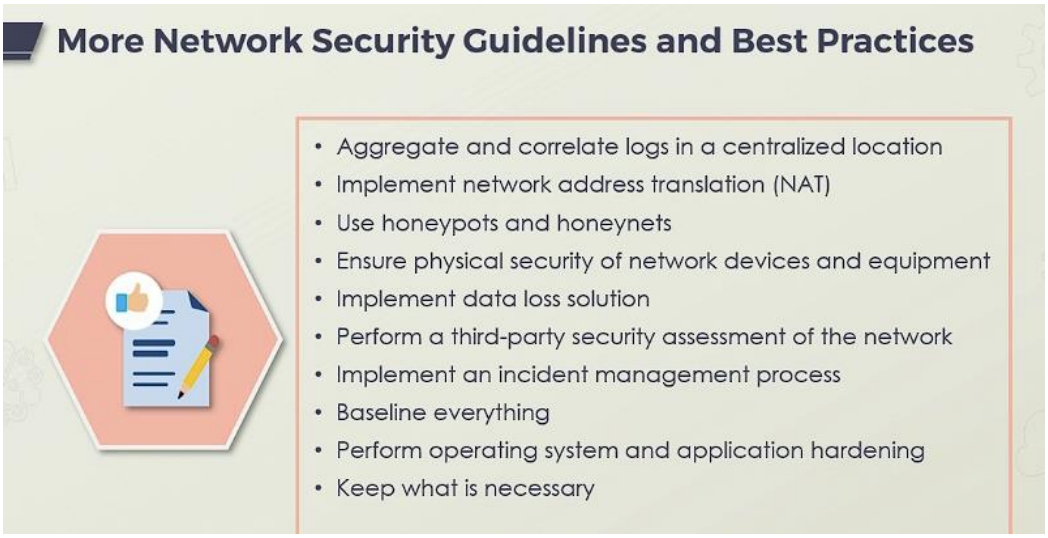
Principle 10 – Challenging compliance

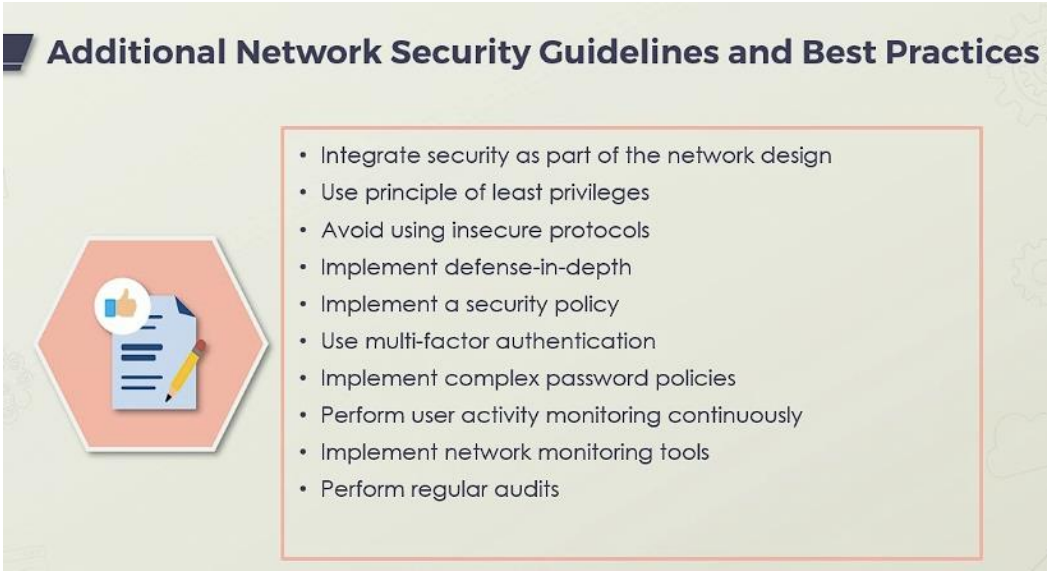
An individual shall be able to challenge an organization's compliance with the above principles. Their challenge should be addressed to the person accountable for the organization's compliance with PIPEDA, usually their Chief Privacy Officer.

PIPEDA – Think about how a company holds customer's personal information

Make sure they Disclose how the information is used and for security, implement appropriate security safeguards for storing personal information. Every part of this is AAA. It is making sure that information of a customer is appropriate used, stored, and accurate.

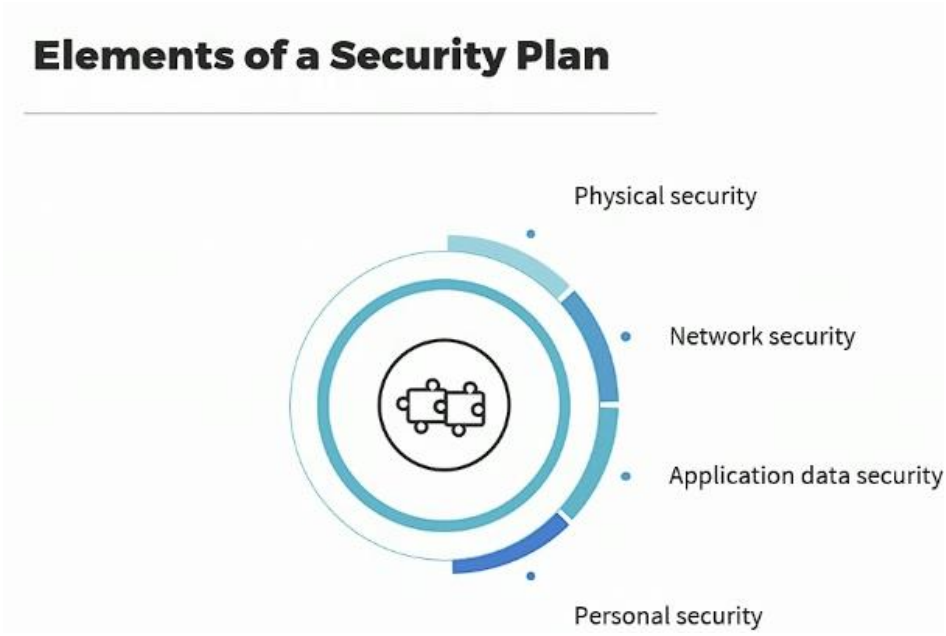






Security Planning and Communicating

1. Install only necessary components
2. Lock and expire default user accounts
3. Change default user passwords
4. Practice the principle of least privilege



Section 3 Lesson 3.3 Application Security, Access Control, and Network Security

Degaussing – applying a strong magnetic force to magnetic media usually makes all electronics unusable

Physical Destruction – destroy the media on which data is stored guarantees that you eliminate any confidential material

Overwriting data – repeatedly overwriting data on media reduces the change that any data can be recovered

Additional Resources

Supplemental Materials section contains quizzes and a practice test for this course. One quiz labelled Network cabling redirects to Net+ quiz and contains a lot of materials not on the exam so keep that in mind

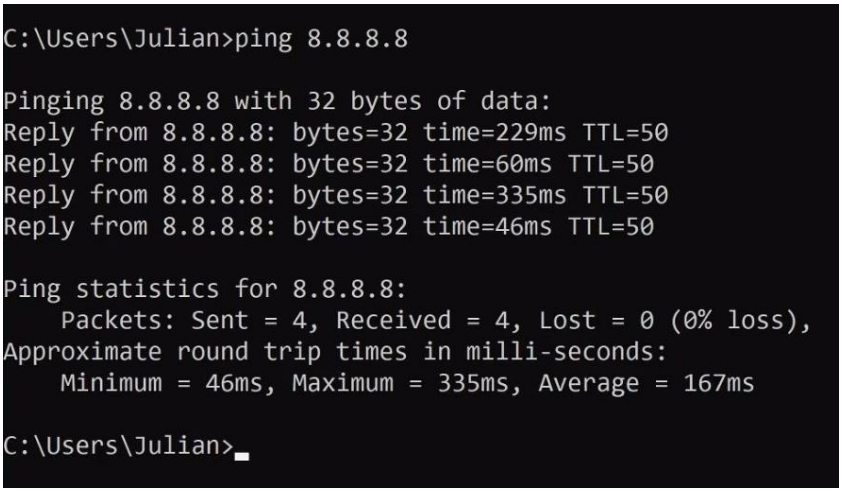
1. https://www.youtube.com/watch?v=bj-YfakjIlc&list=PLIFyRwBY_4bRLmKfP1KnZA6rZbRHtxmXi Practical Networking is a 15 video playlist that gives you detail on understanding the process of OSI (1-4 and later 5-7), going from bit to frame to packet to segment, and how ARP is involved. Not all of the videos are needed but the first 6 or 7 definitely helped.
2. Section 1 and part of section 2 can be found in this Udemy course called introduction to computer networks for non-techies. Despite the name, it goes into deep dives on all the different types of physical devices, network protocols, and there are labs via cisco that help you interact with physical topologies. https://wgu.udemy.com/course/introduction-to-computer-networks/learn/lecture/16044392#overview
3. This udemy course allows you to understand some of the main windows command lines from a networking perspective and places on the screen what each command does for you (Section 6 is the most useful) https://wgu.udemy.com/course/the-complete-windows-command-line-

course/learn/lecture/20257924#overview from there understand what the different names are if it is a linux system vs a windows system traceroute/tracert and ifconfig/ipconfig

4. Cohorts #1 & 2 (do not do 3), and look at the archived videos playlist 10-16 (currently located in announcements => view all by Jim Nichols)
5. Section 3 Lesson 1 has sub-lessons for Fail-Safe all the way to Least Privelege. The entire playlist is worth watching https://wgu.percipio.com/courses/d24c3b97-baa6-47bd-b3cf-517d281e6985/videos/b0894600-11cb-4552-a9d0-fd5e264bd00d?sharelink=4TtfSzXOYC
6. Much of the tests seemed to be focused on the type of attacks that happen. Here is a course that may better explain them and other cybersecurity features like AAA and CIA Triad https://wgu.udemy.com/course/cybersecurity-from-beginner-to-expert/learn/lecture/23485046?start=0#overview
7. Understanding PIPEDA - https://www.youtube.com/watch?v=8_MaDSnBNJM
8. Understanding GDPR - https://www.youtube.com/watch?v=I-VuonciKWk
9.

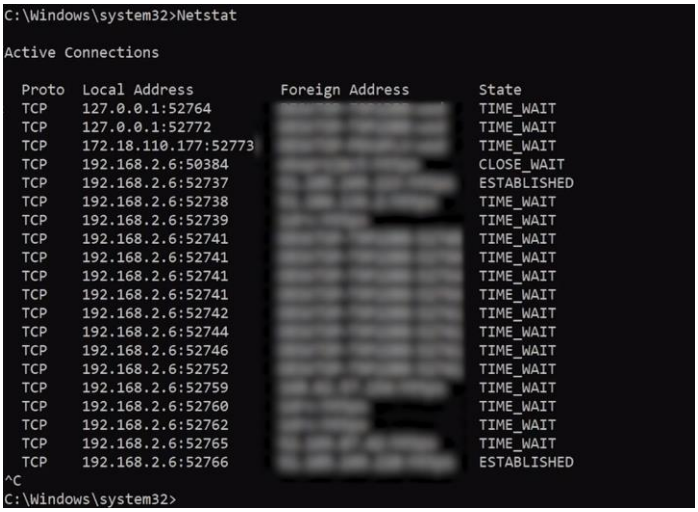
For those that want to visually see what different commands look like in windows:

ping



Tracert (windows traceroute for linux)

netstat



Ipconfig (windows ifconfig linux)

```
C:\Users\Julian>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : mshome.net
   Link-local IPv6 Address . . . . . : fe80::e4e4:1bf7:fe15:ba20%6
   IPv4 Address. . . . . . . . . . . : 192.168.220.182
   Subnet Mask . . . . . . . . . . . : 255.255.255.240
   Default Gateway . . . . . . . . . : 192.168.220.177

C:\Users\Julian>
```

Arp