1.0 Threats, Attacks and Vulnerabilities

1.1 Analyze indicators of compromise and determine the type of Malware:

Viruses- attaches itself to a host application. Must be executed by the user or the system.
Sparse infector virus = behaves sporadically and not certain patterns.
 # Multipartite virus = can infect both program files and the boot sector.
 # Stealth = uses multiple techniques to make them harder to detect.
Worm- self-replicating malware that travels throughout a network without the assistance of host application or user interaction.
Armored virus- makes it difficult to reverse engineer.
Crypto-malware- Encrypts valuable user files
Ransomware- Takes control of a user's system or data and asks for a ransom.
Trojan- Appears to be something useful but includes a malicious component, such as installing a backdoor on a user's system. They infect the systems from rogueware, pirated software, infected USB drives etc.
the trojan and the file are the same entity, so just the trojan cannot be blocked without blocking the actual file.

1. **Rootkit-** Have root-level or kernel level access and can modify system files and system access. Rootkits hide their processes to avoid detection with hooking techniques. Tools that can inspect RAM can discover these hidden hooked processes.

 # If an attacker can access the system despite loading different OS from different media than its a type of firmware-level rootkit virus not Kernel-level.
Kernel- core part of the OS.

Firmware- initializes the hardware and starts the OS

Keylogger- keeps track of every single keystroke. Keylogging software has two major functions; record keystrokes, and transmit those keystrokes to a remote location. Local file scanning and software best-practices can help prevent the initial installation, and controlling outbound network traffic can block unauthorized file transfers.

Adware- learns users' habits for the purpose of targeted advertising. E.g. pop-ups.
Spyware- Monitors the user's computer and the user's activity and sends this information to the third party.
Bots- multiple computers acting as software robots and functioning together in a network for malicious purposes like sending spam, launching DDoS.
RAT- Remote Access Trojan made for spying on, hijacking or destroying computers.
Logic bomb- a string of code embedded into an application or script that will execute in a response to an event such as when a specific application is executed or a specific time arrives.
Backdoor- provides another way of accessing a system. Many types of malware create backdoors, allowing attackers to access systems from remote locations.

1.2 Compare and contrast types of attacks

Social Engineering:

Pharming- Web browser; Spimming- Instant Message like Facebook Messenger. Pharming is a scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent Web sites without their knowledge or consent. Pharming has been called "phishing without a lure."
Phishing- emailing users to trick them into revealing personal information or clicking a link. Spam is an unwanted email. Phishing is malicious spam.
Spear Phishing- Targeted form of phishing. Instead of sending an email to everyone like in phishing, attackers send email to target users or groups.
Whaling- Form of spear phishing that targets high-level executives.
Vishing- Use of phone calls for phishing. By spoofing caller ID etc.
Tailgating- following an employee through the door without showing credentials
Impersonation- identity theft. impersonate others like repair tech to get into the server room
Dumpster Diving- searching through trash to gain information from discarded documents
Shoulder Surfing- looking over the shoulder
Hoax- false message, often an email telling users there is virus and encouraging to delete file or change system configuration
Watering hole attack- Observing which website a user often uses and infecting it with malware.

Principles (Why Social Engineering works?)

Authority- Everyone respects authority
Intimidation- bullying tactics explaining negative consequences
Scarcity- First release of iPhone or discount to first 10 clickers
Consensus- Fake reviews to sell fake antivirus software (malware)
Familiarity- If you like someone, you are likely to do what the person asks. Shoulder surfing and tailgating
Trust- building trust to gain access.

Urgency- encourages you to act now.

Application/Service attacks:

DoS- attack from a single source to disrupt the services provided by another system
DDoS- attack from multiple computers to a single target.
Man-in-the-Middle- Uses a separate computer that accepts traffic from the sender, reads/modifies it and forwards it to the receiver.
Buffer overflow-

- common when attacking Application level servers and services.

A buffer is a memory stack that has a certain holding size.

- Through a specifically and maliciously crafted packet, information can overflow in that stack. This can result in a DoS, system compromise, remote takeover of a system etc. Use patches.

Occurs when an application receives more data than it can handle or receives unexpected data that exposes system memory. Use Input validation to prevent.
includes a series of No Operation (NOP) commands, such as hexadecimal 90 (x90). When successful they can crash applications and expose memory, allowing attackers to run malicious code on the system.
Injection- Attackers use SQL injection attacks to pass queries to back-end databases through web servers. E.g. search **Darril Gibson'; SELECT * FROM Customers; --**
Cross-site scripting- If input validation is not done, attackers can include script in their input and the script becomes a part of the web process.

- **Non-persistent XSS attack**- the injected script is executed and passed back. Doesn't store.
- **Persistent XSS attack**- permanently stored on the web server or backend storage.
- **DOM-based XSS attack**- script is executed in the browser via DOM as opposed to the web server.

To defend XSS:

- Use antiXSS libraries to strip scripts from the input sequences.
- Limit types of uploads and screen the size of uploads, whitelist inputs
- Remove scripts from input but it can be tricky!

Consequences of XSS attack:

- Theft of authentication information from a web app
- Session hijacking
- Phishing or stealing sensitive information
- Impersonating a user etc.

Cross-Site request forgery (XSRF)- causes users to perform actions on web sites such as making purchases, without their knowledge.

- # Also known as **session riding** or **one-click attack.**

For e.g. Hacker may change http://internetsite.com/user=myemail@address.com to http://internetsite.com/user=hackersemail@address.com
Privilege escalation- exploits a programming flaw or buffer overflow to obtain admin-level or root-level access.
ARP poisoning-
Normal ARP process:

1. ARP request: who has this IP: 192.168.1.1?
2. ARP reply: I have that IP. My MAC is 00-11-22-33-44-55

Attackers can reply with a spoofed MAC which poisons the victim's ARP cache. The attacker then performs a man-in-the-middle attack or DoS.

Amplification- use of a large number of machines to flood requests to one machine like DDoS attack.

DNS poisoning- modifies the IP address associated with a website and replaces it with the IP address of a malicious web site. Use DNSSEC to prevent this attack.

Domain hijacking- changing the registration of domain name without the authorization of the valid owner. Ex. register a domain name immediately after the original owner's registration expires.

Man-in-the-browser- intercept and manipulate communications immediately after a victim leaves the browser or before they exit the network interface.

Zero day- Exploits an undocumented or unknown vulnerability.

Replay- Captures data including credentials in a session and later impersonates one party in the session. Use Timestamps and sequence numbers to prevent it.

Pass the hash- Capture the hash from the authentication protocol (LM, NTLM) that does not encrypt the hash. Use the hash instead of the password to authenticate. Implement stronger protocols like NTLMv2 or Kerberos.

Hijacking and related attacks:

- **Clickjacking-** hiding malicious code in a transparent layer. Users think they are clicking one thing but in reality, are clicking the hidden control.
- **Session hijacking-** attacker learns the user's session ID from the cookies and uses it to impersonate the user.
- **Typo-squatting (URL hijacking)-** Buying domain names close to legitimate one. E.g. buying apples.com instead of apple.com and hosting malicious content.

Driver manipulation: changing the behavior of the system by changing the driver. Always use signed drivers.

- **Shimming-** putting a layer of code between the driver and the OS to enable changes between different versions of an OS without modifying the original driver code.

There's a file that has the same name as a Windows system DLL file and has the same API interface but handles the input very differently. It also looks like applications have been attached to this file rather than the real system DLL.- Shimming Not Refactoring!!

- **Refactoring-** rewriting the existing code to fix software bugs or add functionality. Attackers can add the malicious code while maintaining the functionality.

MAC spoofing- impersonating MAC address of authorized systems to bypass MAC address filtering

IP spoofing- Each IP packet contains source IP. Attackers can insert a different IP in the source field and hide its actual IP.

Smurf attack-

- attacker spoofs their IP address with victim's,
- sends the ping out as a broadcast and
- the victim gets flooded with ping responses.
- Disable directed broadcasts on routers to mitigate the threat.

SYN Flood Attack- Attacker sends a SYN packet, victim server responds with SYN/ACK, attacker never completes the handshake (does not send an ACK). Attackers flood with the SYN packets, leaving the server with multiple half-open connections. Use a flood guard.

Xmas Attack- attacker does port scan with specific flags within the TCP packet header. Based on the open ports, the port scanner can detect what services and protocols are running, the OS version etc.

Wireless Attacks:

Replay- capture data sent between 2 entities, modify it and attempt to impersonate one of the parties by replaying it. WPA using TKIP is vulnerable. WPA2 using CCMP and AES is not.
IV- IV is a random number used to create encryption keys in WEP. When the key is repeated, and IV is known it's easy to decipher the key by comparing the ciphertext.
Evil Twin- a rogue access point using the same SSID as a legit AP
Rogue AP- WAP placed within a network to sniff data
Jamming- Transmitting noise on the same frequency to degrade performance
WPS- WPS allows users to configure a wireless network by pressing buttons or by entering a short PIN; attackers can brute force.
Bluejacking- Sending unsolicited message to nearby Bluetooth device
Bluesnarfing- Unauthorized access from Bluetooth connection
RFID

- enables one way wireless communication, typically between an unpowered RFID tag and a powered RFID reader.
- RFID tags can be scanned at distances of up to 100 meters without a direct line of sight to the reader.
- Used for asset tracking in warehouses, airport baggage handling, livestock identification, EZpass and track progress of the automobiles through the production line as it is built.

NFC- subset of RFID

- capable of 2-way communication and can therefore be used for more complex interactions such as card emulation (contact less payment)
- P2P sharing because it acts as both a reader and a tag.
- requires close proximity, typically 5cm or less
- only a single NFC tag can be scanned at one time.

Disassociation- disassociate wireless client from the network with hidden SSID. when they send a reassociation request packet, read the cleartext SSID. Also causes DoS. combine with session hijacking and impersonate the client. Can also implement Evil Twin by transmitting stronger signals with the same SSID after disassociation.

Cryptographic Attacks:

Hash Collision- occurs when the hashing algorithm creates the same hash from different passwords.
Birthday- Attacker steals the hash, uses his list of passwords to produce that hash to identify the password. Same as collision attack.
Rainbow tables- Rainbow tables are huge databases of password hash. Use a search function to find password from the hash or vice versa. Use long passwords or salting to prevent this attack.
Dictionary- Uses a dictionary of words with variation as a password.
Brute force- guess all possible character combinations. Also called exhaustive attack. Use account lockout policy and complex passwords.

- **Online-** against the live logon which can be blocked by account lockout policy

- **Offline-** a hacker works on its own pc to match stolen hashes.

Hybrid- combining dictionary and brute force attack.
Downgrade- Force the system to use weak encryption (e.g. backward compatibility) so it's easier to crack.
Weak implementations- whenever an older version is allowed to continue operation, there is a risk associated with weaker implementations. E.g. 802.11 WEP, DES, SSL etc.
Replay- record a series of packets and then replay them.
Known plain text/cipher text- when a hacker knows the plain text and its cipher text, he can find the encryption/decryption method. He uses this method to decipher other encrypted files.

1.3 Threat Actor types and Attributes

Types of actors:

Script kiddies- just enough understanding of computer systems to be able to download and run scripts that others have developed.
Hacktivist- conveys a social or political message by hacking a website or a system.
Organized Crime- to monetize the effort
Nation states/APT- elite hackers that conduct information warfare.
Insiders- employees already have access to the organization and its assets.
Competitors- information component is easier to copy, steal or disrupt than older, more physical assets making it an alluring target for competitors.

Attributes of actors:

Internal/External- internal actors have more access than external.
Level of sophistication- script kiddies are less sophisticated while nation states are more.
Resources/funding- Criminal organizations or nation run organizations have more funding.
Intent/motivation- script kiddie is trying to make a technique work, hacktivists have a social/political motive.

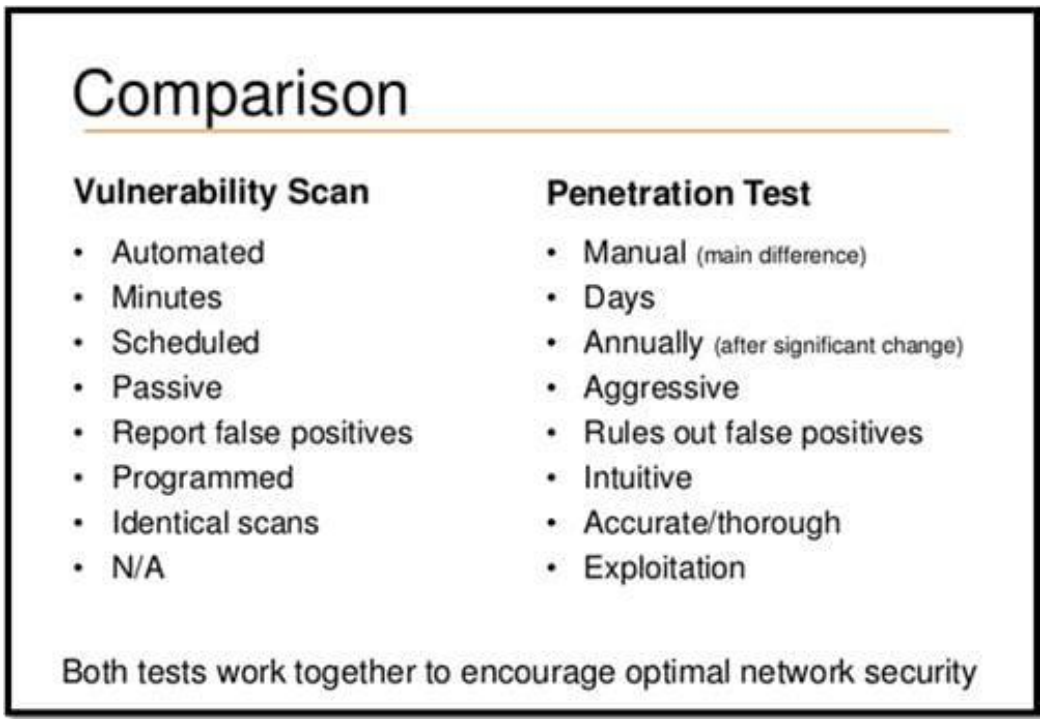
Use of open-source Intelligence (OSINT):

Use of any information that is available via web sites and social media to conduct an attack. Data that is collected through publicly available information. This can be used to help make decisions. Can be used by threat actors to help find their next target or how to best attack their target. OSINT is also incredibly helpful for mitigating risks and for identifying new threat actors.

1.4 Penetration Testing

Active Reconnaissance- use of tools that actually interact with the network and system. Their use can be detected.
Passive Reconnaissance- collecting information from google or other third-party search engines.
Pivot- tester owns one machine, moves their tools to it and examines the network and moves across a network.

Initial Exploitation- Pentester scans for vulnerability, finds it and exploits it to demonstrate that the vulnerability can actually be exploited.
 # E.g. Using a SQL injection attack to successfully bypass a login prompt
Persistence- Installing backdoors or methods to keep access to the host or networks. make it very difficult to remove the threat once they have gained a foothold.
Escalation of privilege- movement from a lower-level account to an account that enables root-level activity. Attackers can use a design flaw in an app to obtain unauthorized access to the application.
Black box- Tester have zero knowledge of the environment
White box- Full knowledge of environment like product documentation, source code, possibly even logon details
Gray box- Some knowledge but no access to all documentation or data.
Penetration testing vs. vulnerability scanning- Vulnerability scanning only identifies the vulnerabilities whereas Pentesting exploits the vulnerability



Common tools: (from the last page of exam objective.)

Nmap & Zenmap	Port Scanner
Wireshark	Traffic Analyzer
Nessus	Vulnerability Scanner
Tripwire	File integrity checker
Metasploitable	Linux box to practice pentesting
Back Orifice	Remote admin tool (rootkit,keylogger). can sniff passwords and access

	a desktop's file system and more, while remaining undetected
OpenVAS	Open Vulnerability Assessment Scanner
Cain & Abel	password recovery tool for windows. uses packet sniffing, dictionary attack, brute force and cryptanalysis attack
ohn the Ripper	password cracker
pfSense	open source Firewall/router. Installed on a physical or virtual machine. based on FreeBSD
Security Onion	free and open source IDS, security monitoring and log management solution
SourceForge	Project management. Open source.
DBAN	Darik's Boot and Nuke. erase hard drives, desktops or laptops or server
Roo	

1.5 Vulnerability scanning concept

Passively test security controls- passively identifies weaknesses but does not exploit it.
Identify vulnerability- Recognize weakness like open ports, weak passwords, default accounts and passwords, security and configuration errors etc.
Identify lack of security controls- missing security controls like lack of up to date patches, antivirus etc.
Identify common misconfigurations- incorrectly configured ports, configuration of networking devices with weak protocols like SNMPv1.
Intrusive vs. non-intrusive- intrusive exploits vulnerabilities; non-intrusive only determines if vulnerabilities exist.
Credentialed vs. non-credentialed- scanning with admin privileges vs starting without admin credentials and gaining admin access using escalation technique.
False positive- all scan results are not true. Ex. IDS alerting an event which is not an intrusion.

 # If your IP is blocked every time you perform a vulnerability scan, you've successfully done a passive test of the client's security controls.

1.6 Impact associated with types of vulnerabilities

Race conditions- when 2 or more applications or modules attempt to access a resource at the same time. Database applications have concurrency control processes to prevent race conditions.
Vulnerabilities due to End-of-life systems, embedded systems, lack of vendor support- ex. Microsoft will stop supporting Windows 7 from Jan, 2020

Use of a third party source code escrow will assist granting you the source code if the vendor goes out of business .
Improper input handling- verify proper character, preventing other, block HTML code etc
Improper error handling- causes application to fail or OS to crash. Error handling should catch the error, show generic error messages to the user but log detailed information.
Misconfiguration/ weak configuration- incorrectly configured ports, configuration of networking devices with weak protocols like SNMPv1
Default configuration- Using default VLAN as a data VLAN with default credential is a risk.
Resource exhaustion- lack of resources to complete a task.
Untrained users- can fall for SPAM and leave a PC vulnerable
Improperly configured accounts- system account or generic account.h
Vulnerable business processes- vulnerable in the process itself. E.g. Not performing background checks of new employees, allowing unlicensed software etc.
Weak cipher suites and implementations- Using WEP, DES etc. for encryption. All versions of SSL are now considered deprecated and should not be used. Switch to TLS.
Memory/buffer vulnerability

- **Memory Leak-** uncleaned memory resources because of a programming error can grow over time and referencing these values returns improper output and system can crash.
- **Integer overflow-** creating a numeric value too big for an app to handle
- **Buffer overflow-** input buffer that is used to hold program input is overwritten with data that is larger than the buffer can hold. If the input validation is not handled properly, the extra characters continue to fill memory, overwriting other portions of the program
- **Pointer dereference-** change the memory location pointed by the pointer that results in an unexpected result.
- **DLL injection-** adding an evil DLL in the correct dictionary for additional functionality.

System sprawl/undocumented assets- old OS running legacy app
architecture/design weaknesses- attackers can traverse the network more likely if the network is not segmented.
New threats/zero day- Unknown threat
Improper certificate and key management- failure to properly validate a key before use can result in an expired or compromised key being used. Improper key management results in failure to secure data.

2.0 Technologies and Tools

2.1 Install and configure network components

Firewall:

A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

A firewall with 2 network interfaces is called a dual-homed firewall. Activated only when the first interface fails.

ACL- identifies what traffic is allowed and what is blocked based on networks, subnets, IP addresses, ports and some protocols. A packet filtering firewall is based on ACLs and only examines the packet header.

Application-based vs. network based-

- Application based Firewall is typically a software installed in the host and can analyze traffic on a deeper level.
- Network based usually looks in IP and ports.
- Application based firewall is most detrimental to network performance because it requires more processing per packet.
- The packet filtering firewall provides high performance.
- Kernel proxy firewalls are built into the OS kernel.

Stateful vs stateless-

- a stateful firewall inspects traffic and decides based on the context or state of the traffic.
- It keeps track of established sessions and inspects traffic based on its state within a session.
- If it detects TCP traffic without a corresponding 3-way handshake, it will block it.
- Stateless firewalls use ACLs to make decisions.

Implicit deny- last rule in ACL that blocks all access that has not been explicitly granted above

VPN Concentrator:

VPN offers a means of cryptographically securing a communication channel and the concentrator is the endpoint for this activity.

Remote Access

- Remote access VPN allows a remote host to connect to a network; usually a roaming employee connecting to its corporate network.
- E.g. Use SSL-VPN with a fixed IP of the office.

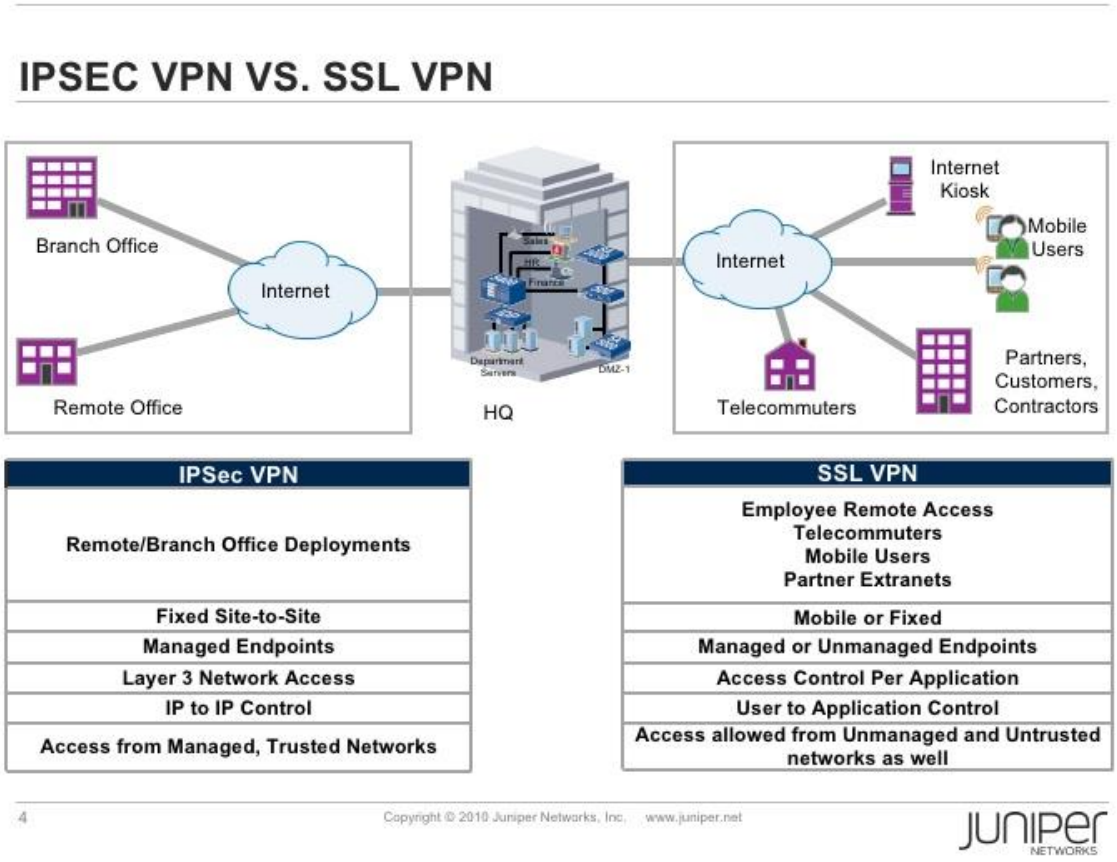
Site-to-site

- connects two networks from remote sites without requiring additional steps on part of the user.
- E.g. Use IPSec between 2 site's Firewall with static IPs on both sides.

TLS (SSL-VPN)

- Typically provides Layer 6 encryption services for Layer 7 applications.
- TLS based VPNs have some advantages over IPSec-based VPNs when networks are heavily NAT encoded.
- SSL Portal VPNs are used to securely access the web from a browser.
- SSL Tunnel VPNs allow not only web access but also applications and other network services.

- E.g. OpenVPN, OpenConnect



PPTP- old protocol
L2TP- provides a login mechanism to users. Since it does not provide security features such as encryption or strong authentication it is typically combined with IPsec.

IPSec is not a type of VPN, it is an encryption protocol.

IPSec:

IPsec (Internet Protocol Security)

- encryption protocol that defines the rules for encryption, authentication and key management for TCP/IP transmissions.
- For non-IP, you must use GRE and IPSec.

IPSec uses IKE over port 500 to authenticate clients in the IPSec conversation.
IKE is a hybrid protocol that consists of 3 protocols:
ISAKMP-

- An Internet IPsec protocol [R2408] to negotiate, establish, modify, and delete security associations (SA), and
- To exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism.

Oakley

- describes the “modes” of key exchange (e.g. Perfect Forward Secrecy for keys, identity protection, and authentication)
-

SKEME

- provides support for public-key-based key exchange, key distribution centers, and manual installation,
- outlines methods of secure and fast key refreshment.

IKEv.1 has 2 phases that create two separate tunnels.

IKE phase 1

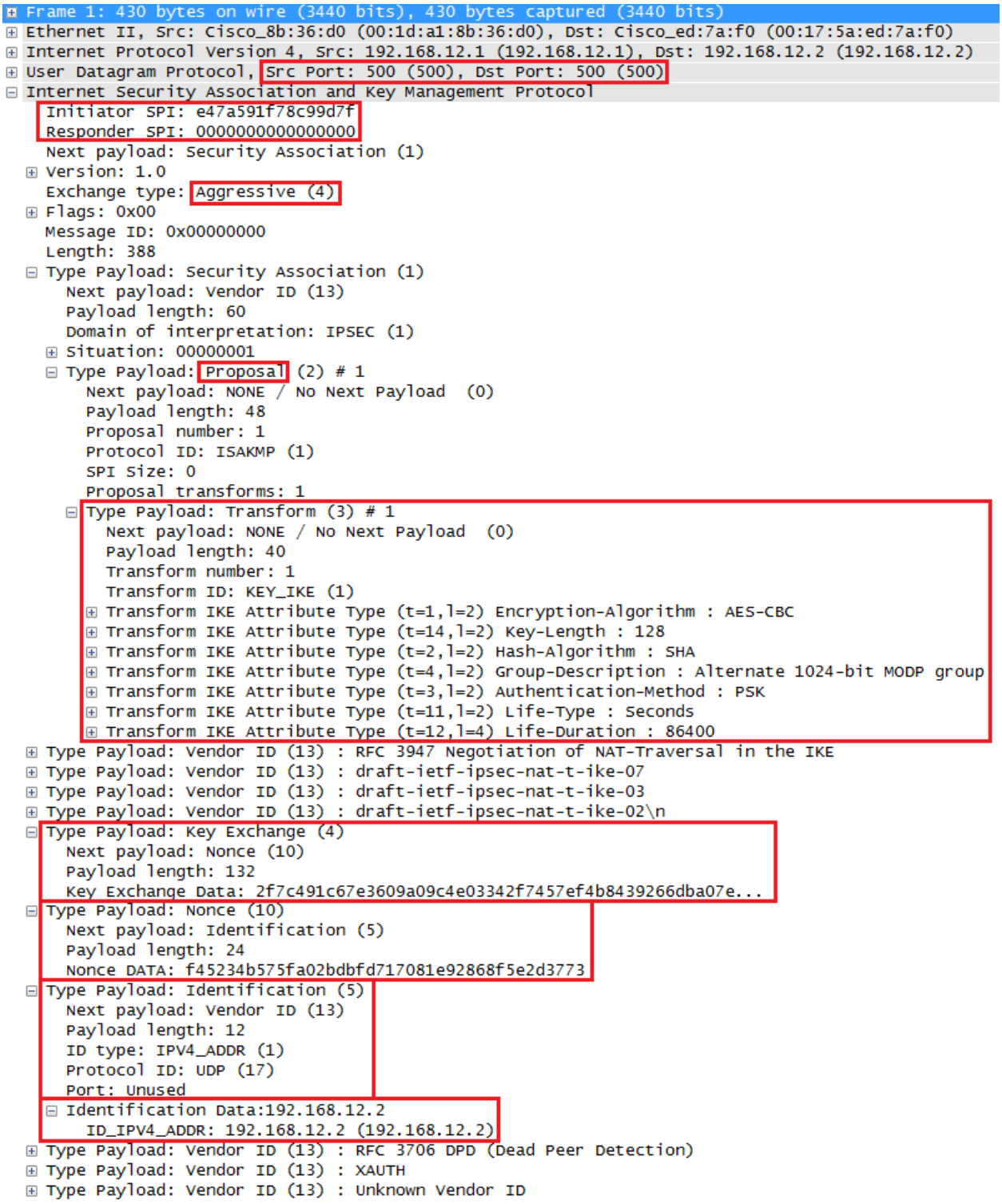
The main purpose is to establish a secure authenticated communication channel that we can use for IKE phase 2. This channel is used to negotiate the IPsec SAs to be used in phase 2.

The following happens in Phase 1.

1. Step 1: Negotiate the protocols (HAGLE)
    - H- Hashing Algorithm. E.g. MD5, SHA
    - A- Authentication of each other. E.g. PSK, RSA digital signatures
    - G- Group of Diffie-Hellman to be used. above Group 14 is good.
    - L- Lifetime of the IKE phase 1 tunnel (Security Association)
    - E- Encryption standards. E.g. DES, AES
2. Step 2: Run Diffie-Hellman Algorithm to exchange shared secret keys.
   Actual Diffie-Hellman is asymmetrical which is used to exchange the session key (symmetric) that is going to be used for symmetric encryption. It’s an example of In-band key exchange
3. Step 3: Authenticate with each other. Credentials can be a certificate or PSK. Both endpoints must use the same credential method.

Phase 1 has 2 possible modes:

1. **Main mode**- consists of 3 exchanges to process and validate the Diffie-Hellman exchange. protects the identity of the peers and the hash of the shared key by encrypting them. Aggressive mode doesn’t.
2. **Aggressive mode**- uses single exchange. Faster but less secure.



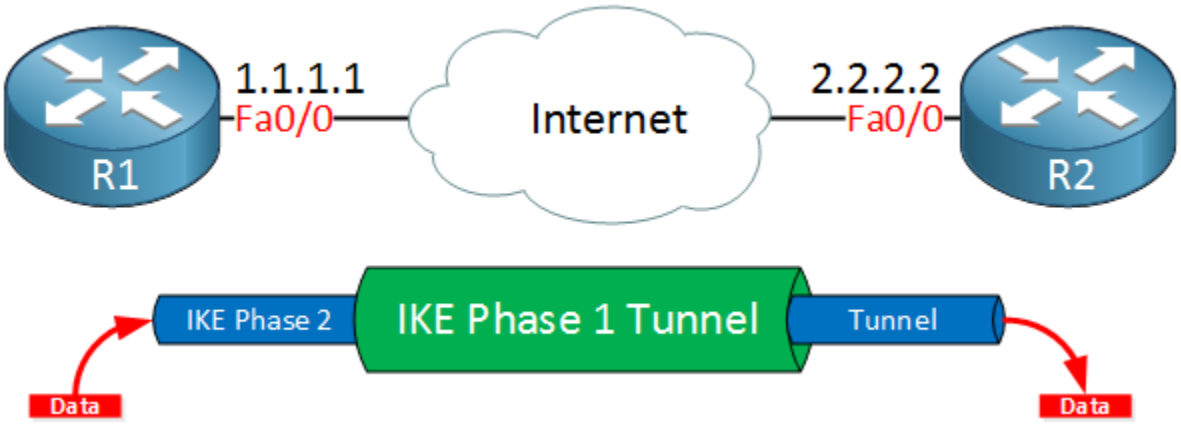
IKE phase 2

The IKE phase 2 tunnel (IPsec tunnel) will be actually used to protect user data. There is only 1 mode: Quick mode.

The IKE peers use the secure channel established in Phase 1 to negotiate Security Associations on behalf of other services like IPSec.

A separate tunnel is created in IKE phase 2 with the following negotiation.

- IPsec Protocol: do we use AH or ESP?
- Encapsulation mode: Transport or Tunnel mode?
- Encryption: DES, 3DES or AES?
- Authentication: HMAC, MD5, SHA
- Lifetime of this tunnel
- DH Exchange (optional): used for PFS.

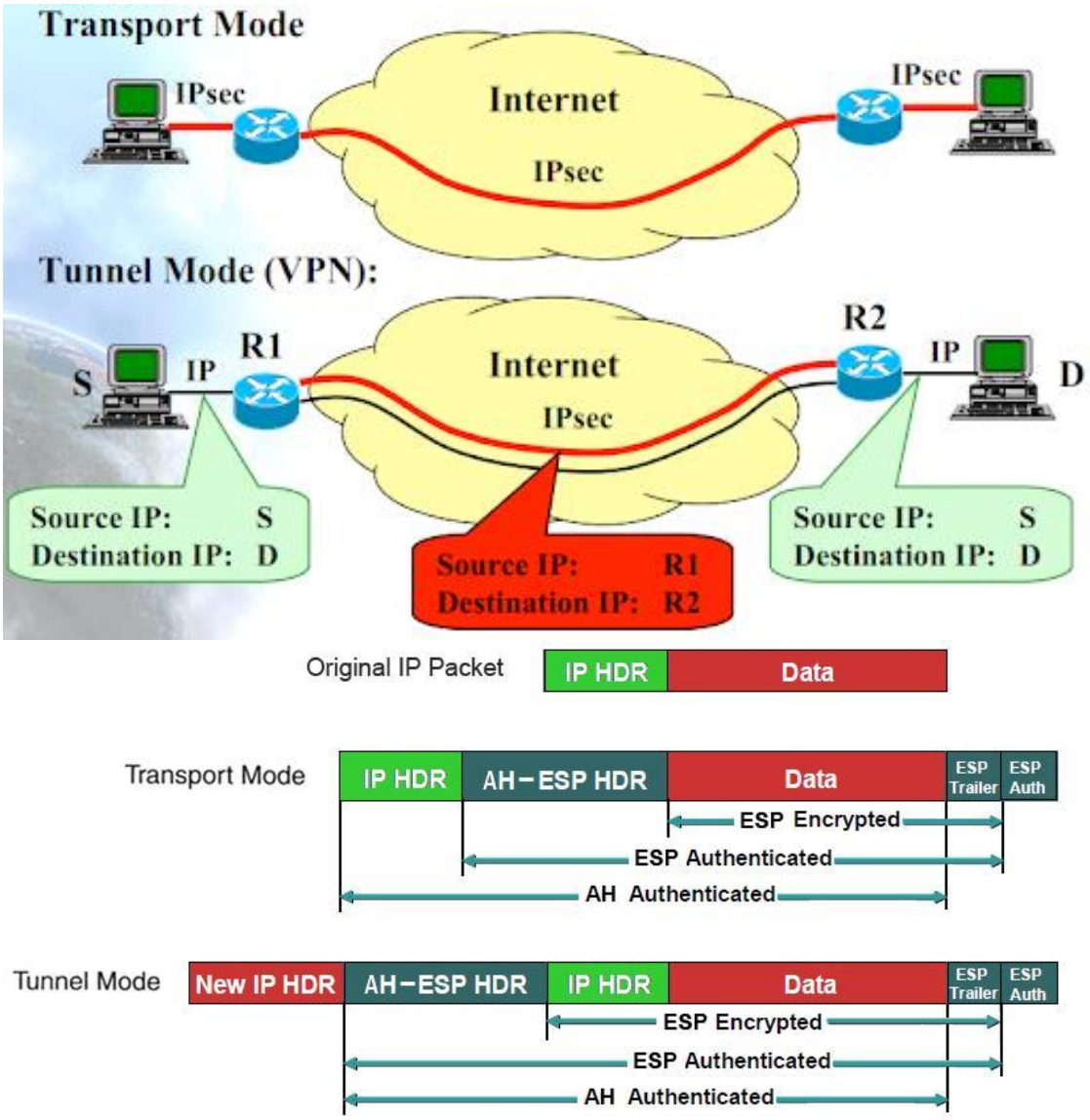


IPsec Protocols:
IKE builds the tunnels for us but it doesn't authenticate or encrypt user data. AH and ESP are 2 protocols that we use to actually protect user data.

- **AH-** provides authentication for the data and the IP header of a packet using one way hash. Doesn't offer encryption service. Doesn't play well with NAT/PAT.
- **ESP-** provides confidentiality (encryption), data origin authentication, connectionless integrity, anti-replay service and limited traffic-flow confidentiality by defeating traffic flow analysis. Since ESP supports encryption, it is more popular.

Both Protocols support 2 different modes.

- **Tunnel Mode-** Entire packet is encrypted and/or authenticated. Used with VPNs transmitted over the (public) internet. Site-to-site
- **Transport mode-** Only IP payload is encrypted; the destination and source IP addresses and other IP header information are readable. Used in a PRIVATE network.



IKEv2 (streamlines the processes of IKEv1)

- requires less bandwidth than IKEv1
- supports EAP authentication (next to PSK and digital certificates)
- built-in support for NAT traversal (required when your IPsec peer is behind a NAT router).
- built-in keepalive mechanism for tunnels.

Split tunnel

- Not all traffic is routed via the VPN to avoid encryption bottlenecks.
- For e.g. Internet search will not be encrypted but any traffic going to the office will be encrypted.

Full tunnel

- Encrypts all traffic including internet traffic.
- Even if you are browsing the internet it will be encrypted and the traffic is sent to the office before going to the internet.
- Full tunneling can significantly spike the traffic flow. Always pay attention to this before deploying.

Always-on VPN- self-configures and connects once an internet connection is sensed and provides VPN functionality without user intervention.

NIPS/NIDS:

- NIDS is the low maintenance device involved in analyzing traffic in the network.
- Easy and economical to manage because the signatures are not configured on all the hosts in a network segment.
- NIDS cannot analyze encrypted information

Signature-based (misused-based)- identifies issues based on known attacks or vulnerabilities. lower false alarm rates.

Heuristic/behavioral-

- looking for evidence of compromise rather than the attack itself.
- low false positive than Anomaly based but higher than signature based.
- Heuristic model uses artificial intelligence to detect intrusions and malicious traffic.

Anomaly-

- 2 step approach. starts with a performance baseline of normal behavior and then compares network traffic against this baseline.
- Can detect potentially a wide range of zero-day attacks.
- Most likely to produce a high number of false alerts because deviations from normal behavior does not always indicate a possible attack.
- May miss novel attack if they don't stick out

Inline

- NIPS is considered inline
- Refers to being in between the Firewall and the rest of the network.
- stops the traffic if it spots the signature match or anomaly before it hits the network.

Passive

- Not inline but mirrored.
- NIDS is a passive network solution
- may sit on the inner network side, DMZ or WAN.
- alerts admin of suspicious connection or potential threat

In-band vs. Out-of-band

- IPS can detect, react and prevent attacks. It is placed in-line with the traffic hence called in-band.
- IDS monitors and responds to an attack. It is not in-line but instead collects data passively hence called out-of-band.

Rules-

- helps differentiate between good traffic and suspicious traffic.
- uses simple signature-based rules, such as Snort or complex Bayesian rules to determine whether an event of interest has occurred or not.

Analytics

- **False positive-** alert on events that are harmless.
- **False negative-** does not detect actual attack

Router:

ACLs- identifies what traffic is allowed and what is blocked based on networks, subnets, IP addresses, ports and some protocols
Anti-spoofing- enable source IP checking in router to prevent spoofing from the network to perform DDos attack.
Network Address Translation (NAT)- NAT router acts as the interface between a LAN and the internet using one IP address.

Switch:

Port security- Disable unused ports and limit the number of MAC per port. Use 802.1x server to provide port-based authentication.
Layer 2 vs Layer 3- layer 2 switch routes traffic based on MAC within same network while layer 3 switch routes traffic based on IP between 2 different networks
Loop prevention- loops occur when 2 ports of a switch are connected together. Use STP, Rapid STP to prevent switching loop
Flood guard- by monitoring traffic rate and percentage of bandwidth occupied by broadcast, multicast and unicast traffic, flood guard can detect when to block traffic to prevent flooding attacks like ping floods, SYN floods, ICMP floods (smurf attacks) etc.

Proxy:

1. **Proxy Server-** acts as an Internet gateway, firewall and internet caching server for a private network. Hosts on the private network contact the proxy server with an Internet Web site request.

Forward proxy

- Forwards request for services from client.
- Provides caching to improve performance and reduce internet bandwidth usage.
- Uses URL filters to restrict access to certain sites;
- logs user activit

Reverse proxy

- Typically installed on the server side.
- Receives request on behalf of client
- Also called a surrogate proxy.
- Used for hiding internal servers, load balancing.

Transparent-

- Accepts and forwards requests without modifying them.
- Doesn't require client side configuration.
- Non-transparent proxies can modify or filter requests such as filtering traffic based on destination URLs.

Application/multipurpose- proxy for a specific application or for multipurpose.

Load balancer

Scheduling

- **Affinity**

    - Uses client's IP address to ensure the client is redirected to the same server during a session.
    - Designed to keep a host connected to the same server across a session.
    - For new connections, it creates a new affinity entry and assigns the session to the next server in available rotation.
- **Round-robin**
    - Sends each new request to the next server in rotation.
    - Can use weighting factors to take server load into account.

Active-passive- active load balancer does the balancing job and passive balancer steps in if active balancer fails
Active-active- both share the load balancing duties. Efficient performance but failure of one will lead to session interruption and traffic loss.
Virtual IPs-

- use of virtual IPs for servers so that the router only sends packets to the balancer and does not see actual IP of servers to send packets directly.
- An IP address and a specific port number that can be used to reference different physical servers.
- Provides IP addresses that can float between two or more physical network nodes and provide redundancy.
- Virtual IP load-balancing doesn't take a load of each interface and assumes all loads are similar

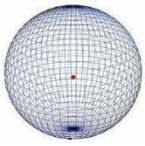
Access point:

SSID- identifies the name of wireless network
MAC filtering- blocks unauthorized devices by only allowing certain MAC on AP. Attacker can use sniffer to discover allowed MAC and circumvent by spoofing its MAC
Signal strength-

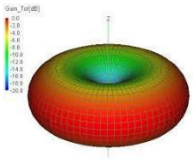
- **Decibels-isotropic (dBi)** identifies gain on omnidirectional antennas. Higher the better.
- **Decibels-dipole (dBd)** identifies gain on the dipole antenna. Higher dBd indicates the antenna can transmit and receive over greater distance.
- **Decibels-milliwatt (dBm)** identifies the power level of the WAP and refers to the power ratio in decibels referenced to one milliwatt. Higher the better.
- Cannot modify the dBi or dBd gain without changing physical properties.
- Many WAPs include power settings to change power level.

Band selection/width- select 2.4GHz for b/g and n and 5GHz for a, n and ac.
Antenna types and placement

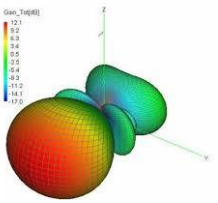
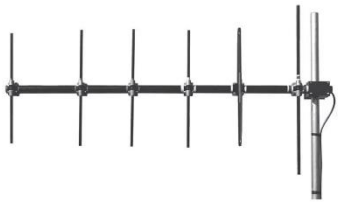
- **Isotropic-** theoretical antenna with perfect 3D radiation pattern of 360 degrees both horizontally and vertically.



- **Dipole-** an actual omnidirectional antenna with a radiation pattern of 360 degrees horizontally and about 75 degrees vertically. Earliest, simplest, and most widely used antenna.




- **Yagi-** Directional antenna that uses a dipole, folded dipole, or half-wave dipole combined with additional elements like reflector or director element. High gain with narrow radiation pattern.

Perform site survey for proper antenna selection and placement. Enough strength to cover all workspace but not very wide to prevent security issues.
Fat vs. thin- fat APs are standalone and thin APs are controller based.
Controller-based vs. standalone- controller based APs allows for centralized management and control, which can facilitate better channel management for adjacent APs, better load balancing and easier deployment of patches and firmware updates. Easier for NAC. standalone is simpler than controller-based.

SIEM: Security Information and Event Management

- Classifies and analyzes security data from numerous sources.

(T)- Time synchronization- use UTC for correlation across the entire enterprise and local time for local process meaning.
(A)- Aggregation- collecting information in a central place, in a common format from system event logs, firewall logs, security appliances log etc.
(C)- Correlation- connection of events based on time, common events, behavior etc. useful to look for patterns.
(A)- Automated alerting and triggers- through the rules or analytical engines, SIEM can issue an alert or react to the event.
(L)- Logs/WORM- logs are written once in the SIEM database and read many times by different rules and analytical engines. *Write Once Read Many*. best option for long-term storage and security.
(E)- Event deduplication- SIEM uses a special correlation to determine which records are duplicates of a specific event, and then delete all but a single record.

DLP

USB blocking- prevents data loss by blocking USB ports.
Cloud-based- detects the data moved to cloud and blocks.
Email- email server like exchange also has DLP.

NAC:

Agent

- code is stored in the host machine

Agentless

- the code resides on the network and is deployed to memory for use in a machine requesting connections.

Permanent

- Agents are pre-deployed to the endpoints

Dissolvable

- Deployed when needed and removed after use. Has a minimum impact than Agentless.

Host health checks- NAC uses health agents to inspect clients for health, such as having up-to-date antivirus software and restrict access of unhealthy clients to a quarantine network.

Mail gateway

Spam filter- blocks spam. Ex. Appriver, mimecast.
DLP- blocks data leak by implementing Data Loss Prevention policy.
Encryption- encrypts the mail traffic. Add-in solutions like Pretty Good Privacy (PGP), built in S/MIME (secure/Multipurpose Internet Mail Extensions) etc.

Bridge- network segregating device operating in layer 2. most convenient for interconnecting two or more physically separated network segments.
SSL/TLS accelerators- use this transparent device between web server and the internet for encrypting traffic per SSL/TLS instead of using larger and larger web servers to encrypt traffic.
SSL decryptors- opens the SSL/TLS traffic using man-in-the-middle technique, screens the traffic and re-encrypts it. Prevents encrypted attack.
Media gateway- handles different protocols for voice and video signals and translates them to common protocols used in a network.
Hardware security module- manages and stores encryption keys. Typically, a peripheral device connected via USB or a network connection.

2.2 Tools to assess security posture

Protocol Analyzer-

- Captures, displays and analyzes packets sent over a network.
- Useful to troubleshoot network communications, detect attacks that manipulate or fragment packets.
- NIC must be configured to use promiscuous mode to capture all traffic.
- E.g. Wireshark, Tcpdump

 # Promiscuous mode = accept and process every packet it sees- not just packets destined for this specific system.

Network scanners-

- Scans all devices on a network.
- Searches for live hosts, open ports, TCP/UDP services etc.
- E.g. Nmap, zenmap
- **Rogue system detection-** helps detect unknown devices on network.
- **Network mapping-** shows how networking devices are connected to each other.

Wireless scanners/crackers- scan to find who is connected, what are they accessing etc. e.g. Kismet, NetStumbler.

Password cracker- to audit weaker passwords in your network
Vulnerability scanner- Recognizes weakness like open ports, weak passwords, default accounts and passwords, security and configuration errors etc. E.g. Nessus
Configuration compliance scanner- establish a baseline configuration upon its first operation and set to measure deviations in future cycles.
Exploitation frameworks- tool sets to assist with the tasks associated with exploiting vulnerabilities. E.g. Metasploit.
Data sanitization tools- to destroy or purge a system before retiring and disposing it.
Steganography tools- for hiding messages in images, videos or audio files etc.
Honeypot- sloppily locked down servers to divert attackers from live networks. Provides opportunity to observe current attack methods and gather intelligence on these attacks.
Backup utilities- tools for backing up critical data. E.g. Veeam.
Banner grabbing- technique used to gain info about remote servers. Ex. Telnet google.com 80 might reveal some info by grabbing HTML banners.
Passive vs. active- passive tools do not interact with the system in a manner that would permit detection whereas active tools can be detected.
Command line tools

- **Ping-** to test connectivity for remote system
- **Netstat-** shows active TCP/IP network connections, routing tables and protocol statistics
- **Tracert-** lists routers between 2 systems
- **nslookup-** gather information from DNS servers, lookup names and IP addresses. Replaced by dig.
- **dig-** Domain Information Groper. More advanced than nslookup and shows more detailed domain information. Is primarily used for Linux but can be used in windows as well.
- **Arp-** to identify MAC from IP (IP to MAC)
- **ipconfig/ip/ifconfig-** shows TCP/IP configuration such as IP address, subnet mask, default gateway, MAC address, DNS server etc.
- **Tcpdump-** command line packet analyzer for Linux just like Wireshark.
- **Nmap-** network scanner that has many capabilities including identifying all the active hosts and their addresses in a network, the protocols and services running on each of these hosts and the OS of the host.
- **Netcat-** used to remotely administer systems and can also perform banner grabbing. Banner grabbing gathers info on OS, services and applications. Hackers can open a backdoor using this.

2.3 Troubleshooting common security issues

Unencrypted credentials/clear text- never use obsolete protocols that transfer passwords in clear text.
Logs and events anomalies- objective should be to record event anomalies. Should decide what to log and what not to log.
Permission issues- outdated user rights lists can create permission issues.
Access violations- should be logged and alerted.

Certificate issues- occurs when a user attempts to use a certificate that lacks a complete chain of trust back to a trusted root, leaving the certificate hanging without any means of violation.
Data exfiltration- attacker attempts to steal data.
Misconfigured devices

- **Firewall-** ruleset based on packets. Over time, ruleset becomes less orderly and has issues due to exceptions.
- **Content filter-** set of rules based on content. Sometimes content filters can be too broad.
- **Access points-** can use ACL, RADIUS or NAC for defining rules.

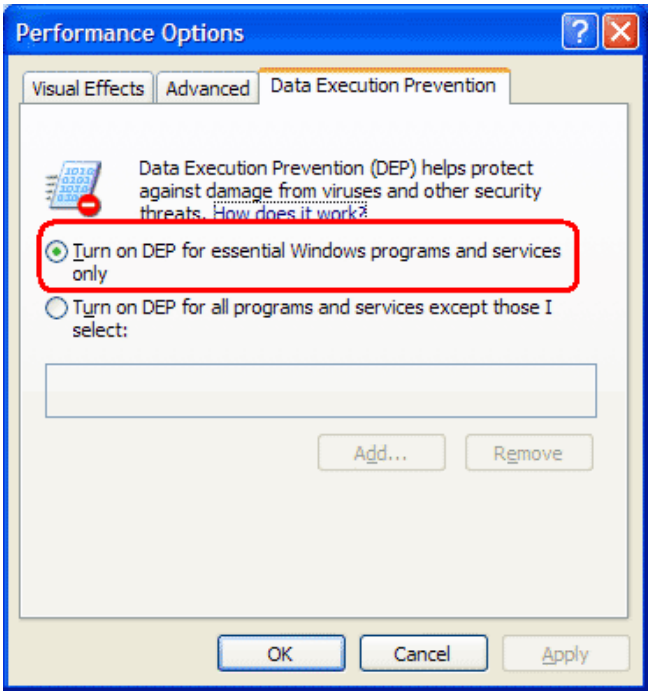
Weak security configurations- choose strong cipher suites, strong password policies etc.
Personnel issues- train users

- **Policy violation-** educate about policy
- **Insider threat-** enforce separation of duties.
- **Social engineering -** train users
- **Social media-** enforce social media policy
- **Personal email-** one way of data exfiltration

Unauthorized software- Well defined policy and regular audit.
Baseline deviation- change from system's desired state of security readiness
License compliance violation- can create inadvertent availability issues.
Asset management- maintain accurate asset records.
Authentication issues- block unauthorized access while ensuring authorized access at all time.

2.4 Analyze and interpret output from security technologies

HIDS/HIPS- alert on behaviors based on signatures.
Antivirus- alerts, prevents, and logs malicious attack attempts.
File Integrity check- by comparing the original hash and calculated hash. E.g. Kernel Integrity Subsystem
Host-based firewall- firewall in the host machine. E.g. Windows Virus
Application whitelisting- only special applications are allowed to be installed.
Removable media control- should prevent data exfiltration using encryption technology.
Advanced malware tools- Specialized malware removal and recovery tools. E.g. Yara.
Patch management tools- helps patch OS as well as applications. E.g. PDQ deploy
UTM- all in one security acting as, firewall, IDS/IPS, anti-malware, anti-spam, content filtering etc.
DLP- detects and prevents data transfer
Data execution prevention- OS works with the CPU to prevent programs to execute in certain parts of memory. Memory regions are marked as non-executable which prevents code from being executed. This protects against memory abuse attacks such as buffer overflows.

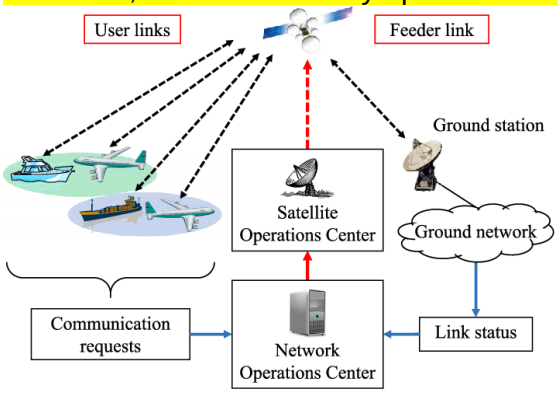


Web application firewall- performs restrictions based on rules associated with HTTP/HTTPS traffic.
 # WAF provides load balancing.

2.5 Deploy mobile devices securely

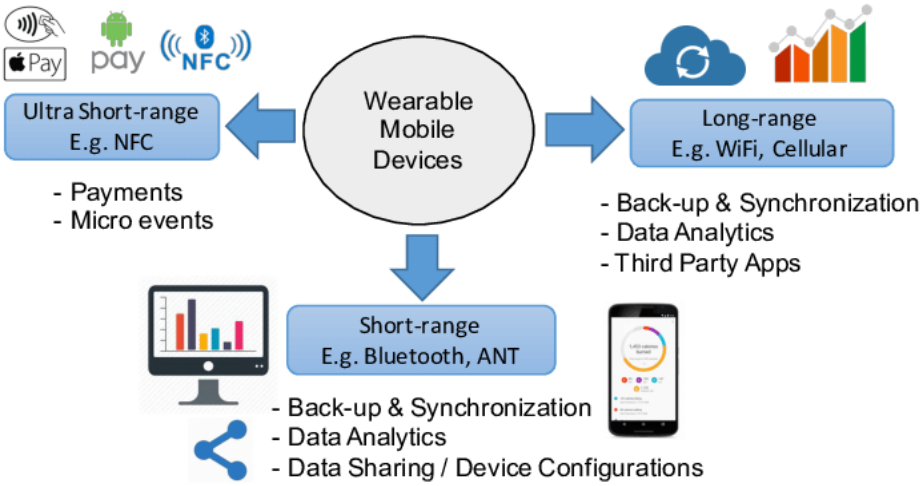
Connection Methods:

Cellular- Less available in rural areas. Cellular devices are susceptible to traffic monitoring, location tracking, and gain access to the device from anywhere in the world
Wi-Fi- connect to SSID with Pre-Shared key.
SATCOM- Satellite communication. Cost and line-of-sight is an issue in high-density urban areas. Satellite Communications that is used for communications in remote areas and during natural disasters. SATCOM devices are at risk of leaking geopositioning data and remote code execution, and are not easily updated remotely.



Bluetooth- Bluetooth 4.0 supports 3 modes: Classic, high speed and Low energy. Bluetooth Smart is used in medical devices.
NFC- radio communication over a short proximity. commonly used as a payment gateway.

ANT- operates in a 2.4GHz ISM (industrial, scientific, and medical) band to communicate. Used in heart monitors, sports and fitness sensors. Usage with Fitness sensors such as Fitbit. collects data on users and uses ANT to send the data to mobile device applications.



Infrared- line-of-sight wireless technology. used in remote controls, wireless keyboard and mouse.
USB- used to connect devices physically.

Mobile device management concepts:

Application management- MDM can restrict what application can be installed and prevent unapproved applications.
Content management
Remote wipe- delete content when mobile device is lost.
Geofencing- allow apps to respond when the device is within geofence.
Geolocation- to locate lost device
Screen locks- require PIN/password etc. to authorize access.
Push notification services- send messages to mobile devices from app using MDM
Passwords and pins- to allow access to the device.
Biometrics- prevent unauthorized users.

Context aware authentication- use of multiple elements for authentication. E.g. user's identity, geolocation, time of day, type of device etc.
Containerization- by running an application in a container, it isolates and protects the application, including any of its data.
Storage segmentation- Users would store corporate data in encrypted segments and personal data on other segments.
Full device encryption- helps against loss of confidentiality on mobile devices including laptop

Enforcement and monitoring for:

Third party app stores
Rooting/Jailbreaking- Rooting is a process of modifying an Android device to give the user root-level access. Jailbreaking refers to Apple. MDM blocks access to its network if it detects such events.
Sideloading- process of copying an application package in the APK format to the device and then activating it. Doesn't work in Apple.
Custom firmware- overwriting android firmware with custom firmware just like rooting.
Carrier unlocking- locked by carrier
Firmware OTA updates- Updating firmware of a device on-the-air as opposed to connecting locally from LAN.
Camera use
SMS/MMS- Cleartext SMS and MMS are unsecure.
External media
USB OTG- Mobile to mobile connection using USB to transfer data. use MDM to prevent users from copying enterprise data by blocking USB On-The-Go.
Recording microphone
GPS tagging

Wi-Fi direct
- Allows devices to connect without AP.
- Uses single hop, meaning the camera will not have access to the internet.
- E.g. using a camera app to connect to the camera to download images.

Ad hoc
- is similar but it uses multiple hop. Hence, has access to the internet.

Tethering
- Allows you to share one device's internet connection with other devices.
- Wi-Fi tethering is the same as Mobile Hotspot.
- Can be used to bypass corporate web security to access prohibited websites while still being connected to the LAN. Implement a policy against tethering to prevent this.

Payment methods

Deployment models:

BYOD- allow users to bring their own mobile device to work and attach them to the network.
COPE (Corporate Owned, Personally Enabled)
- Can be used for personal use as well.

CYOD (Choose Your Own Device)
- Organization creates a list of acceptable devices
- Employees can purchase those and bring to work

Corporate-owned- Organization purchases devices and issues them to employees.

VDI- Virtual desktop that a user can access from a mobile device
VMI- Virtual Mobile Infrastructure would allow the field teams to access their applications from many different types of devices without the requirement of a mobile device management or concern about corporate data on the devices.

2.6 Implement secure protocol

Protocols:

DNSSEC- DNS Security Extension prevents DNS cache poisoning by providing validation for DNS responses. DNSSEC records are signed so all DNSSEC responses are authenticated but not encrypted. Use TLS not SSL. DNS requests use UDP 53, DNS zone transfer uses TCP 53.
SSH- encrypts traffic in transit and can be used to encrypt other protocols such as FTP.
S/MIME- MIME does not provide security. S/MIME is commonly used in modern email software.
SRTP- Provides encryption, message authentication and integrity for RTP. can be used for both unicast and multicast transmission. AES is used to encrypt traffic over SRTP.
LDAPS- used to securely communicate with directories such as AD DS. LDAPS encrypts data with TLS on TCP 636.
SFTP- FTP for file transfer and SSH for encryption. Uses port 22
FTPS- FTP for file transfer and TLS for encryption. Uses port 989/990
SNMPv3- man age and monitor network devices using UDP 161/162.
SSL- Primarily used to secure HTTP traffic as HTTPS. SSL can also encrypt SMTP and LDAP. Has already been compromised by POODLE attack. Use TLS instead.
POODLE: Padding Oracle on Downgraded Legacy Encryption.
 # SMTP by itself is not secure. Use TLS to create a secure link.
TLS- replacement of SSL.
HTTPS- uses SSL or TLS to encrypt traffic using port 443.
Secure POP/IMAP- POP3 uses TCP 110. Secure POP3 encrypt transmission using SSL or TLS and uses port 995. IMAP4 uses TCP 143. IMAP4 with SSL or TLS uses TCP 993 but STARTTLS is recommended to create secure connections on port 110.

Use cases

Voice and video- RTP delivers audio and video over IP networks. This includes VoIP, streaming media, video teleconferencing applications and devices using web-based push-to-talk features. SRTP provides encryption, message authentication and integrity of RTP. SRTP provides protection against replay attacks.
Time synchronization- NTP and Simple NTP is used. Use NTPSec.
Email and web-

- SMTP transfers email between SMTP servers. Use S/MIME
- POP3 transfers emails from servers down to the clients.
- IMAP4 is used to store email on an email server.

Web servers use HTTP to transmit web pages to client's web browsers.
HTTPs encrypts web traffic.
File transfer- SSH, IPSec, SFTP are used to encrypt data-in-transit while FTP and TFTP are unsecured protocols. Use FTPS or SFTP.
Directory services- provides secure access to the network. E.g. AD DS, LDAP.
Remote access- To access systems from remote locations. RDP uses TCP or UDP 3389.
Domain name resolution- DNS is used for resolving host names into IP. Use DNSSEC

Routing and switching-

- R**/**STP prevents switching loops.
- Flood guards block MAC flood attacks.
- Port security prevents unauthorized users.
- VLANs provide increased segmentation.

Network address allocation- IPv4 and IPv6. Private IPs are defined in RFC 1918. Use it to mitigate DHCP starvation attacks. “Gobbler” can be used to execute a DHCP starvation attack.
Subscription services- E.g. Office 365 uses a subscription model.

3.0 Architecture and Design

3.1 Frameworks, best practices and secure configuration guides

Framework- a collection of standardized policies, procedures and guides, meant to direct a user, firm, or any organization.

Industry-standard frameworks and reference architectures

Regulatory- based on mandated laws and regulations. E.g. HIPAA.
Non-regulatory- The common standards and best practices that the organization follows.
National vs. international
Industry-specific frameworks

Benchmarks/secure configuration guides

Guidance for setting up and operating computer systems to a secure level that is understood and documented.
Platform/vendor-specific guides

- **Web server-** Center for Internet Security (CIS) guides are available for Apache, IIS etc. The OWASP (Open web application security project) is the standard for web application security
- **Operating system-** CIS and from DoD DISA STIG
- **Application server**
- **Network infrastructure devices-** use manufacturer's guide

General purpose guides- includes rules for ISO compliance, adhering to NIST guidelines and confirming to PCI-DSS and other standards.

Defense-in-depth/Layered security:

Implementing several layers of protection
Vendor diversity- implementing security controls from different vendors to increase security.
Control diversity- use of different security control types such as technical controls, administrative controls and physical controls.

- **Administrative-** policies, regulations, laws etc. System TESTING and security awareness.
- **Technical-** Firewalls, IDS proxy server

User training- informs users of threats, helping them avoid common attacks.

3.2 Implement secure network architecture concepts

Zones/topologies:

DMZ- buffer zone between the internet and an internal network. Implement every computer in DMZ as a bastion host. A bastion host is a hardened device to resist attack. All services and ports should be disabled that are not used.
Extranet- part of the network that can be accessed by authorized entities from outside of the network. They can be business partners, customers, vendors etc.
Intranet- internal network for sharing content with other employees.
Wireless- use of AP to bridge wired connection.
Guest- typically a wireless connection for guests.
Honeynets- honeypots are sloppily locked down servers allowing an attacker relatively easy access to observer current methodologies used in attacks and gather intelligence on these attacks. Honeynets are a group of honeypots.
NAT- translates public IP to private IP. NAT is not compatible with IPsec. Static NAT uses a single public IP, Dynamic NAT uses available public IP based on load.
Ad hoc- (as needed). Connecting wireless devices without an AP. Like a personal hotspot.

Segregation/segmentation/isolation:

Physical- E.g. SCADA operates on their own network.
Logical (VLAN)- create separate VLAN for routers, switches, VOIP phones etc.
Virtualization- provides server isolation. Cheaper solution than Failover cluster
Air gaps- an air gapped system is not connected to any other systems.

Tunneling/VPN:

Site-to-site- encrypted traffic between 2 sites.
Remote access- from user to the site
IPSec is not a type of VPN. It is the encryption protocol used in VPN solutions.

Security device/technology placement:

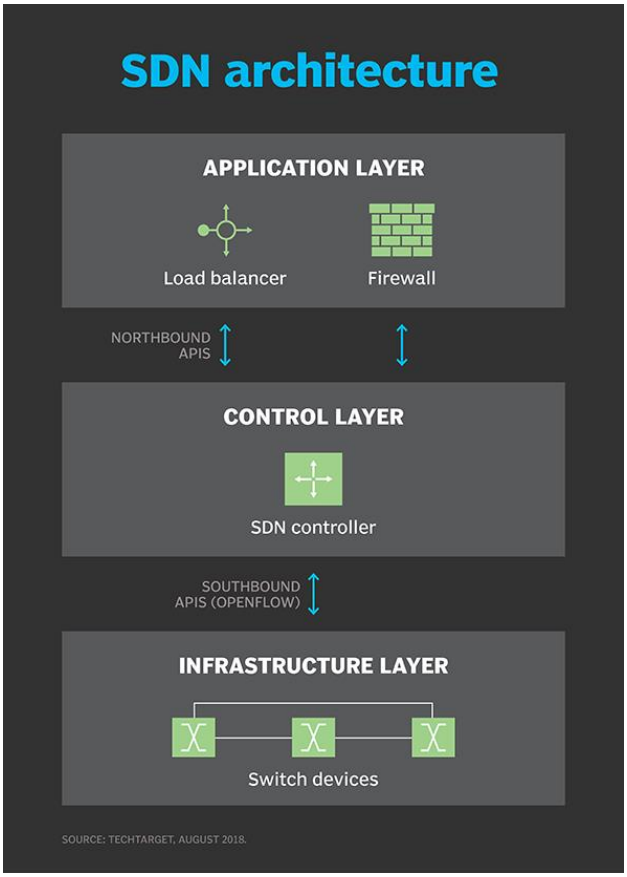
Sensors- Gathers information from networking devices. Can give transactions, logs, or other raw data. Can be integrated or built-into switches, servers, firewalls, routers, or other network devices.
Collectors- Collects information from sensors and sends information to correlation engines.
Correlation engines- analyzes event logs and alerts possible breaches.
Filters- filters packets based on rules.
Proxies- a proxy server forwards requests for services from a client. Reverse proxy accepts requests from the internet. Middle man in communications.
Firewalls- advanced filtering. Usually placed on the ingress or egress of the network.
VPN concentrators- allow encrypted connections to and from the company internal network.
SSL accelerators- removes load from the web server by providing SSL/TLS encryption/decryption. Should be placed between web server and client.
Load balancers- takes incoming traffic from one network location and distributes it across multiple devices.
DDoS mitigator- position at the very edge of the network before other devices.
Aggregation switches- core switch that other switches connect to.
Taps and port mirror-

- Switch Port Analyzer (SPAN) port or mirror port copies all frames and sends for analysis.
- Test Access Point (TAP) is a separate piece of hardware that copies all the packets it receives and rebuilds the packets.
- Use TAP instead of port mirroring for copying 100% traffic if network transfer rate is high.

Firewall --- DMZ -- Firewall --- SSL accelerator --- Load balancer --- web server

SDN:

Uses virtualization technologies to route traffic instead of using hardware routers and switches. SDN separates the logic used to forward or block traffic (data plane) and the logic used to identify the path to take (control plane). Hardware routers use rules within an ACL to identify whether a router will forward or block traffic on the data plane. This is always proprietary because it's implemented on specific hardware routers. SDN implements the data plane with software and virtualization technologies, allowing an organization to move away from proprietary hardware.



3.3 Implement secure systems design

Hardware/firmware security

FDE/SED-

- Full Disk Encryption encrypts the entire disk and not just files and folders.
- E.g. VeraCrypt is an open source utility.
- SED is a special form of FDE which has hardware based encryption.

TPM-

- Hardware chip in motherboard that generates random numbers and stores cryptographic keys.

- Key stored in TPM is not accessible via normal software channels.
- Normally used in clients.
- Can be used for server authentication.

HSM-

- Hardware Security Model is a removable device that can generate, store and manage RSA keys.
- Significant performance advantages due to the dedicated piece of software.
- Normally used in servers.
- Can be used to store HTTPS encryption keys.

UEFI/BIOS- BIOS provides basic instructions on how to start. It runs basic checks, locates the OS and starts. UEFI provides some enhancements. E.g. boot from larger disks and designed to be CPU-independent.
BIOS password management is also the most fundamental integrity technique because, without this, other options like TPM prove less effective.
Secure Boot- Creates hash of boot loader and associated drivers, then compares to previously stored hash. Hash is stored locally on TPM.
Attestation- same as secure boot but the file is saved in a remote system as opposed to TPM
Supply chain- hard to determine where the parts of hardware have come from. Some hardware might come with preloaded malware.
Hardware root of trust-

- concept that if one has a trusted source of specific security functions, this layer can be used to promote security to higher layers of a system.
- E.g. TPM includes a unique RSA asymmetric key burned into the chip that provides a hardware root of trust, or a known secure starting point.

EMI/EMP- EMI generates from motors, power lines, fluorescent lights and can be prevented with shielding. Electromagnetic Pulse can be produced from ESD, lightning etc. Use ESD straps, surge protector etc. to prevent these short bursts of electromagnetic energy.

Operating systems:

Types:

- **Network-** IOS runs in cisco routers, switches etc.
- **Server-** server OS like Windows Server 2019
- **Workstation-** Windows 10
- **Appliance-** Embedded OS
- **Kiosk-** Locked down OS for specific purposes. Like LTSC
- **Mobile OS-** iOS, Android OS

Patch management- ensures that OS and applications are up to date with current patches.

- Hotfix- small line of code typically developed in reaction to a discovered problem
- Patch- more formal and larger software update. Often contains enhancement and fixes bugs.
- Service Pack- large collection of patches and hotfixes rolled into a single large pack.

Disabling unnecessary ports and services- minimizes risk
Least functionality- system should be deployed with the least amount of applications, services and protocols.
Secure configurations
Trusted operating system- meets a set of predetermined requirements of the organization.
Defined by EAL4.

Application whitelisting/blacklisting- Whitelist: list of applications authorized to run. Blacklist: list of applications a system block.
Disable default accounts/passwords-

Peripherals

Wireless keyboards & Wireless mice- can send information in clear text. Risk of keylogging. Wireless mouse is susceptible to mouse spoofing but not malware infection.
Displays- if the display shows sensitive or private data, their view should be limited. Disable telnet if being used to download content from the internet.
Wi-Fi-enabled MicroSD cards
Printers/MFDs- can be remotely managed. Turn off telnet, SSH if not using.
External storage devices- data exfiltration risk
Digital camera

3.4 Secure staging deployment concepts

Sandboxing- Use of an isolated area for testing.
Environment

- **Development-** process of creating applications. Includes version control and change management control.
- **Test-** attempts to discover any bugs or errors. QAs will evaluate the functionality of the app.
- **Staging-** Simulates production environment and is used for late stage testing. performance baselines are created.
- **Production-** final product. Live environment.

Secure baseline- document the minimum specifications for an application, system or service that is considered secure. Change can be compared to the baseline to determine whether minimum security levels are maintained.
Integrity measurement- process of monitoring where the application, system or service complies with the security baseline.

3.5 Security implications of embedded systems

SCADA/ICS- Industrial Control System refers to systems within large facilities such as power plants or water treatment facilities. ICS is controlled by a Supervisory Control and Data.
Use security layers, firmware version control, manual updates, application firewalls, network segments (VLAN), ACLs etc. to mitigate security risk.
Smart devices/IoT- Linux-type kernel as a core engine
HVAC- Keeps computing systems at the proper temperature and proper humidity.
HVAC systems have the most impact on availability. If it gets too hot, the systems will fail to run. HVAC systems have no effect on confidentiality, fire suppression, and/or monitoring access to the datacenter.
SoC- System on a Chip is an IC that includes all the functionality of a computing system within the hardware. E.g. Raspberry Pi, chip credit card, media player
RTOS-

- Real Time OS are built for specific purposes. No Multitasking.
- Processing must be in real time.

- E.g. anti-lock braking computer in a car. flight control system, real time monitors.

Printers/MFDs- local storage of print jobs. Printers may allow users to connect through Telnet or SSH. If the protocols are not used, turn them off.

Camera systems

Special purpose

- **Medical devices-** can be manipulated for false reporting and collect the patient's protected medical data.
- **Vehicles-** hackers can hack into "Smart" automobiles and drive them remotely or change settings.
- **aircraft/uav**

3.6 Secure application development and deployment

Development life-cycle models

- **Waterfall-** You finish one stage to go to the next stage. Cannot go back to the previous stage.
- **Agile-** Uses iterative cycles. Each cycle creates a working if not complete product.
  - **Extreme Programming (XP)-** advocates frequent "releases" in short development cycles, which is intended to improve productivity and introduce checkpoints at which new customer requirements can be adopted.
  - **Scrum-** framework centered on process perspective. Built around 30-days cycle.

Secure DevOps- Includes extensive communication between Software Developer, Operations personnel and security consideration throughout the project.

- **Security automation-** run automated tests on each update to ensure it is error free.
- **Continuous Integration-**
  - ELI5: There is a central repository of mainline code. As a software developer you check out the part of code, work on it for a day and merge it. If conflict occurs, it's easier to fix because it's just one day worth of work.
  - It includes a version control and supports roll back.
  - involves a series of steps that are automatically performed to integrate code from multiple sources, create a build and test. Each time a build or a set of code passes the tests, it's automatically deployed out to a staging environment where further testing such as load testing and manual exploratory testing is conducted. This process can be repeated for days depending upon the project delivery requirements.
  - CI is done using platforms designed specifically for the purpose and implementing CI is as simple as using the right tool. E.g. Jenkins, Bamboo.
  - CI server runs automated tests on every new commit that emerges into the remote repository mainline. Also issues custom notifications when a test or build fails, triggering releases generation, triggering deployments to a specific environment and so on.
- **Baselining-** applying changes to the baseline code every day and building the code from these changes.
- **Immutable Systems-** servers are never modified after they're adopted. If something needs to be updated, fixed, or modified in any way, new servers built from a common image with the appropriate changes are provisioned to replace the old ones.

- **Infrastructure as code-**
  - means by which engineers define the computer systems their code needs to run.
  - refers to managing and provisioning data centers with code and that defines the VM.
  - Configuration Orchestration tools like Terraform and AWS CloudFormation are designed to automate deployment of servers and other infrastructure
  - Configuration management tools like Chef, Puppet help configure the software and systems on this infrastructure that has already been provisioned.

Version control and change management- change management prevents unauthorized changes. version control system documents each change with rollback features. Tracks who made the change and when.
Provisioning and deprovisioning- allocating resources based on demand of that resource. Deprovisioning an app means removing the app.
Secure coding techniques

- **Proper error handling-** applications should show generic error messages to users but log detailed information. If an application doesn't catch an error, it often provides debugging information that an attacker can use against the application. Control the information provided when the application catches an error.
- **Proper input validation-** check input data for validity before using it. For e.g. verify proper characters, block HTML code and certain characters used by SQL like -, ', = etc. to prevent SQL injection.
- **Normalization-** organizing the tables and columns to reduce redundant data and improve overall database performance.
- **Stored procedures-** SQL queries that execute on the server side instead of the client application. The client application calls the procedure on the server and this prevents the client from making any changes to the actual SQL queries.
  Create a SQL code and save it. Next time you need to run the code, you can use the stored procedure instead of building from scratch. Also provides security by not allowing any code to run. Prevents SQL injection attack.
- **Code signing-** applying digital signature to code for verifying the code integrity.
- **Encryption**
- **Obfuscation/camouflage-** intentionally complicate code so that others cannot understand the code easily.
- **Code reuse-** use the old code that has already gone through internal. Saves time.
- **Dead code-** May be executed but results are never used. Dead code elimination may have unintended consequences. For example, if you copy a code that creates a user, modifies the user and authenticates the user but your new application does not require modifying the user then that part of the code is a dead code.
- **Server-side vs client-side execution and validation-** use input validation in both client and server side. Many web browsers allow users to bypass client-side validation by disabling JavaScript.
- **Memory management-** prevents things like memory leak- a situation where the program does not free up the memory after completing its use.
- **Use of third-party libraries and SDKs-** Using third-party libraries saves time and SDK provides an environment to write code for certain applications. For example, Android

SDK includes software tools that will help us build android apps. But a flaw in SDK may impact every application developed using that SDK.

- **Data Exposure-** loss of control over data from a system during operations.

Code quality and testing

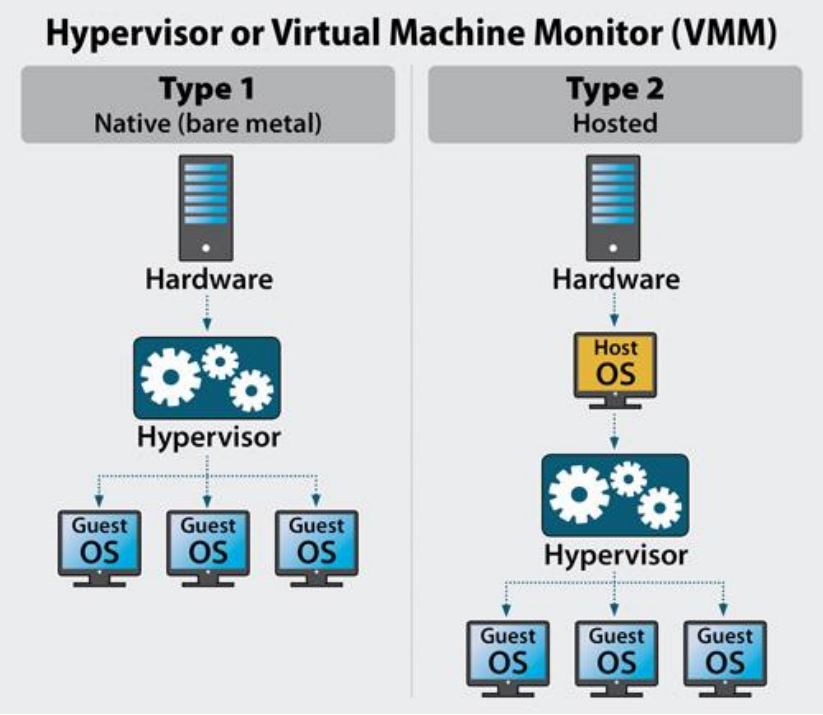
- **Static code analyzers-** examines code without executing it. Automated tools can analyze them and mark potential defects. Ensures memory allocations have corresponding deallocations.
- **Dynamic analysis (E.g. fuzzing)-**
  - checks the code on a real or virtual processor.
  - Fuzzing sends invalid, unexpected or random data to the application to check if it crashes, have memory leaks etc.
- **Stress testing-** simulates a live environment to determine how application operates with a load.
- **Sandboxing-** isolated area used for testing purposes.
- **Model verification-** to ensure if the software fulfills its intended purpose.

Compiled code- User doesn't see the source code, it's all compiled.
Runtime code- Source code is visible

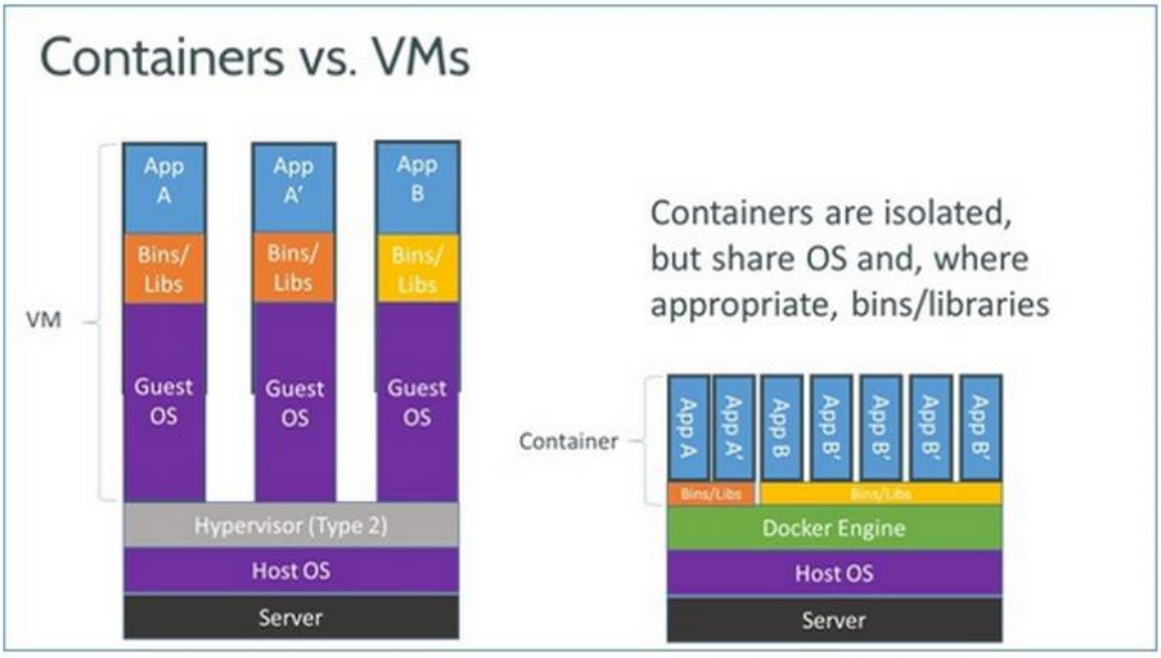
3.7 Cloud and Virtualization concepts

Hypervisor

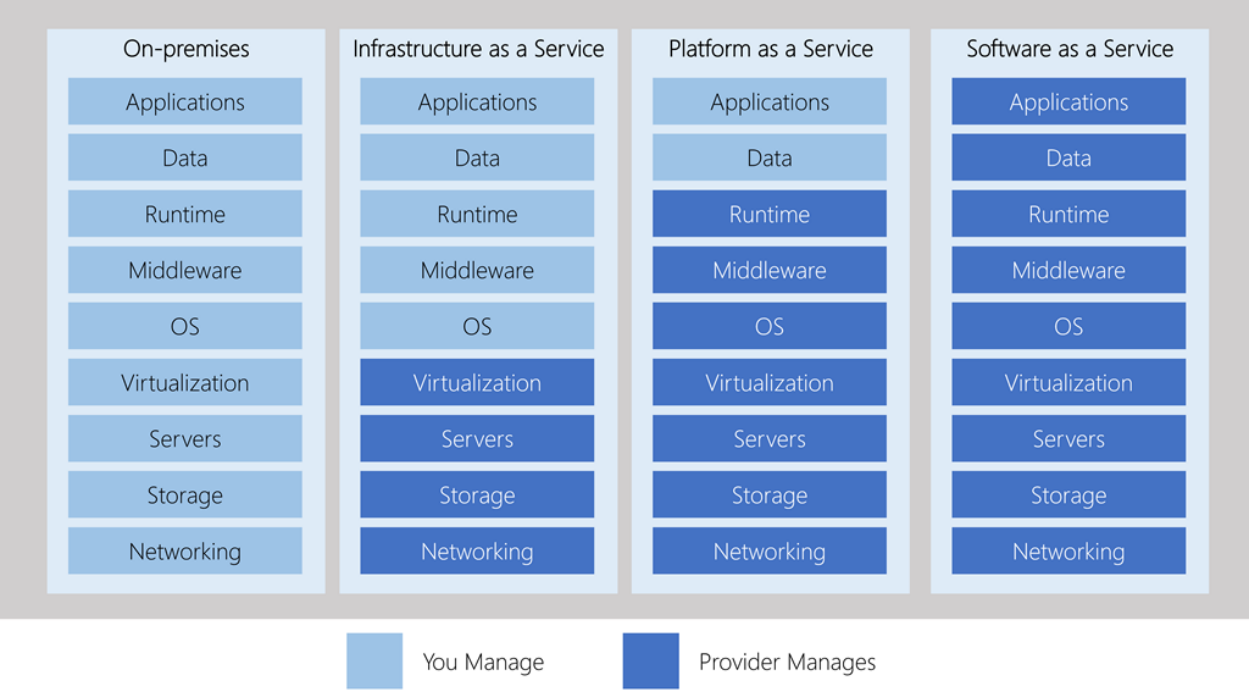
- **Type I-** runs directly on the hardware. Optimizes speed and efficiency. Maximizes # of guest OS. E.g. Xen, Hyper-V (even though it runs as a feature)
- **Type II-** runs on the host OS. VirtualBox, VMware.



- Application cells/containers-
  - Containerization runs small applications on a host OS with virtually no overhead.
  - Multiple containers can share an OS.
  - Like a Hypervisor, but shares kernels with regular system OS to use less space and be more efficient. Therefore, you can't have Linux container on Windows without some fanciness



VM sprawl avoidance- Non-physical servers are difficult to locate.
VM escape protection- When software, malware or attacker escapes from one VM to the underlying OS.
Cloud storage- ensure encryption
Cloud deployment models



- **SaaS-** Appropriate for highly scalable, on-demand applications. Eg. google mail, google docs etc.availability
- **PaaS-** Suitable for STANDARD resources. Provides customers with a fully managed platform, which the vendor keeps up to date with current patches. provides infrastructure to create and host applications.
- **IaaS-** Appropriate for highly customized, poorly scaling solutions that require specific resources to run. provides customers with access to hardware in a self-managed platform. Customers are responsible for all OS updates and patches.
- **Private-** costly
- **Public-** fewest security control
- **Hybrid**
- **Community-** Shared resources for a specific purpose

On-premise vs. hosted vs. cloud- On-prem: all resources are owned, operated and maintained within the organization's building. Hosted: org rents access to resources from a specific org.
VDI/VDE- advantages: desktop can be accessed from a variety of devices, session can follow the user and if a device is lost, it contains no corporate data.
easier to manage patches, configurations and software installations/updates/maintenance in a single location.
Cloud access security broker (CASB)- specialized tools or services that sit between cloud service consumers and cloud service providers used to protect cloud infrastructure and data.
Security as a Service- The provider implements their security services into your environment via the cloud, such as: authentication anti-virus, anti-malware, IDS, and event management. offers scale, cost and speed efficiencies

3.8 Resiliency and automation strategies

Resilient system can return to normal operating conditions after an upset.

Automation/Scripting

- **Automated courses of action-** reduces errors.
- **Continuous monitoring-** confirms if controls are functioning properly
- **Configuration validation-** ensure that the system will do what it is supposed to do and only what it is supposed to do with no added functionality.

Templates- allow rapid, error-free creation of systems and services, including configurations, connection of services, testing and deployment.

Master Image- premade fully patched image of your organization's system

Non-persistence- does not save changes to configuration or application

- **Snapshots-** easy to revert to the previous configurations if the change contains errors.
- **Revert to known state-** can affect more than just the OS
- **Rollback to known configuration-** change to the system configuration, not necessarily what it is on.
- **Live boot media-** disc or USB with a complete bootable system

Elasticity- configure the system to scale up and down.

Scalability- enables a system to accommodate larger workloads by adding resources either making hardware stronger, scale up or adding additional nodes, scale out.

Distributive allocation- allocation of requests across a range of resources just like load balancing.

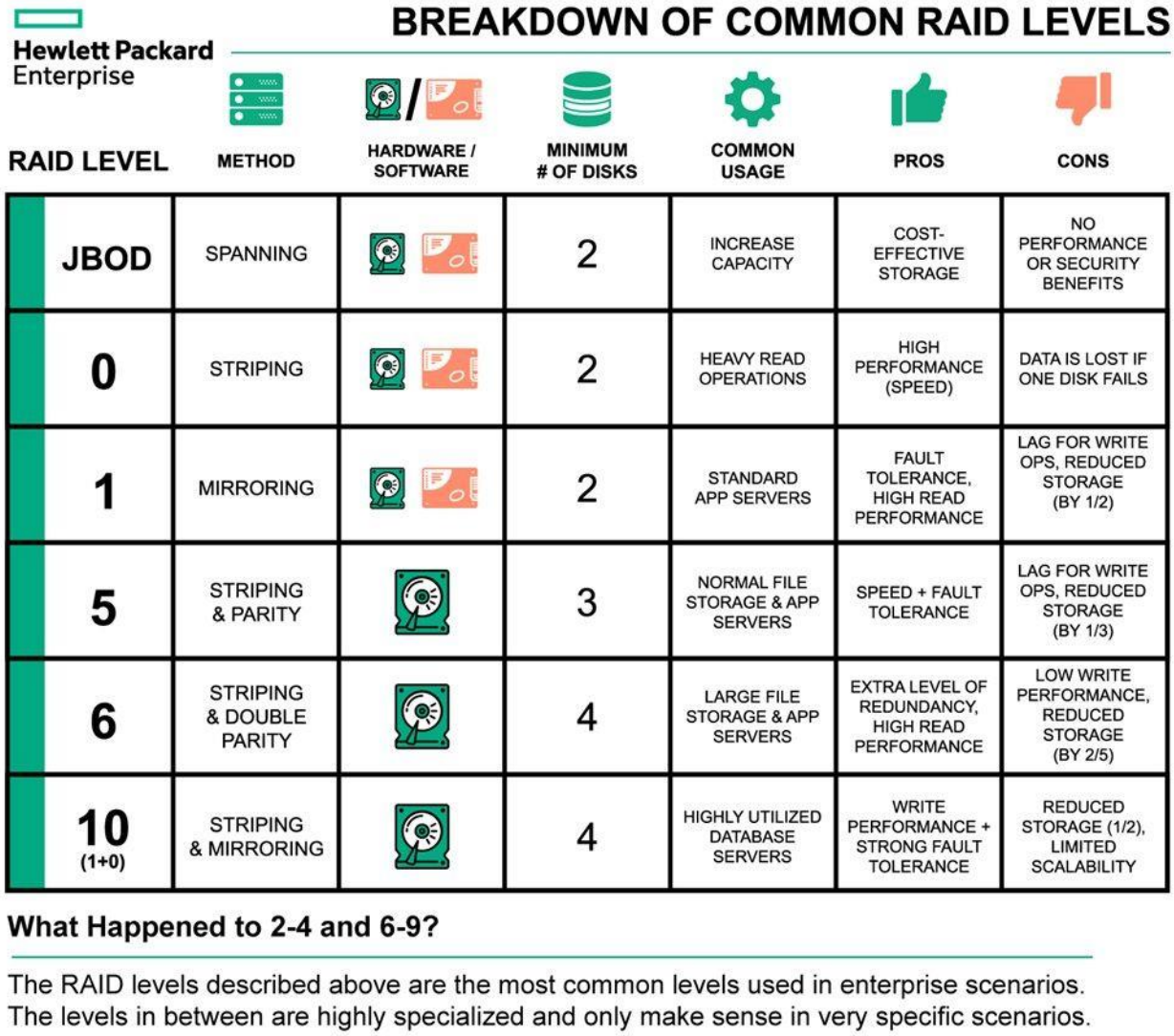
Redundancy- use of multiple, independent elements to perform a critical function, so that if one fails, there is another that can take over the work.

Fault tolerance- design objective to achieve high availability should a fault occur.

High availability- system or service that needs to remain operational with almost zero downtime

RAID

- **RAID 0-** striped disk. Great performance feature but if 1 drive fails, all fail.
- **RAID 1-** mirrored disk. If drive 1 fails, drive 2 continues writing.
- **RAID 5-** block-striped with error check. Provides High Availability because 3rd drive is a parity drive that has data building information
- **RAID 10-** stripe of mirrors



3.9 Physical Security Controls

Lighting- allows more people and activities to be observed.
Signs- visual cues. keep people away from restricted areas
Fencing/gate/cage- build a perimeter
Security guards
Alarms- set to provide accurate and useful alerts.
Safe
Secure cabinets/enclosures
Protected distribution/Protected cabling- physically secure cable to prevent tapping and DoS
Air Gap- a method of isolating an entity to effectively separate it from everything else. Provides physical isolation
Mantrap- prevents tailgating. Controls access to the data center.

Faraday Cage- prevents illicit monitoring of computer systems through Van Eck emissions. blocks electromagnetic fields.
Lock types- smart locks are a type of cipher lock that can be programmable. E.g. Keyscan system. Mechanical locks can be warded or tumbler. Combination lock requires correct combination.
Biometrics- Biometric features can change over time with medical conditions. Re-identification needed
Barricades/bollards- blocks vehicles
Tokens/cards- RFID badge. better than metallic keys because it can be revoked remotely
Environmental controls

- **HVAC-** provides cooling capacity
- **Hot and cold aisles-** provides cooling in the data center via proper air flow.
- **Fire suppression-** FM-200 is a Fire Extinguishing system. Water and soda acid are used in class A fire (paper, laminates, wooden furniture). Halon or CO2 was used for class C fire (electrical wiring & distribution boxes). Halon destroys Ozone. Use dry powder for combustible metal.

Cable locks- effective for small equipment
Screen filters
Cameras- can replace security guards.
Motion detection-
Logs
Infrared detection- detects changes in heat waves
Key management

4.0 Identity and Access Management

4.1 Identity and access management concepts

Identification, authentication, authorization and accounting (AAA)

- **Identification-** when users claim their identity with username, email etc.
- **Authentication-** when users prove their identity. E.g. password
- **Authorization-** grant access to resources based on the proven identity
- **Accounting-** track user activity and record in logs.

Multi-Factor authentication

- **Something you know-** password, PIN---------- Type I authentication
- **Something you have-** smart card, USB token----------Type II authentication
- **Something you are-** fingerprints, retina----------Type III authentication
- **Somewhere you are-** location
- **Something you do-** gesture in touch screen, signature, keyboard cadence (timing)

Federation

- provides central authentication between 2 or more nonhomogeneous environments by using a federated identity management system, often integrated as a federated database.
- Most significant disadvantage of federated identities is transitive trust. The security of federated identities is impacted by the security of others.

Single Sign-On (SSO)- enhances security by requiring users to use and remember only one set of credentials for authentication.

Transitive trust

- creates an indirect trust relationship.
- If A trusts B and B trusts C, A trusts C because of a transitive relationship.

4.2 Install and configure identity and access services

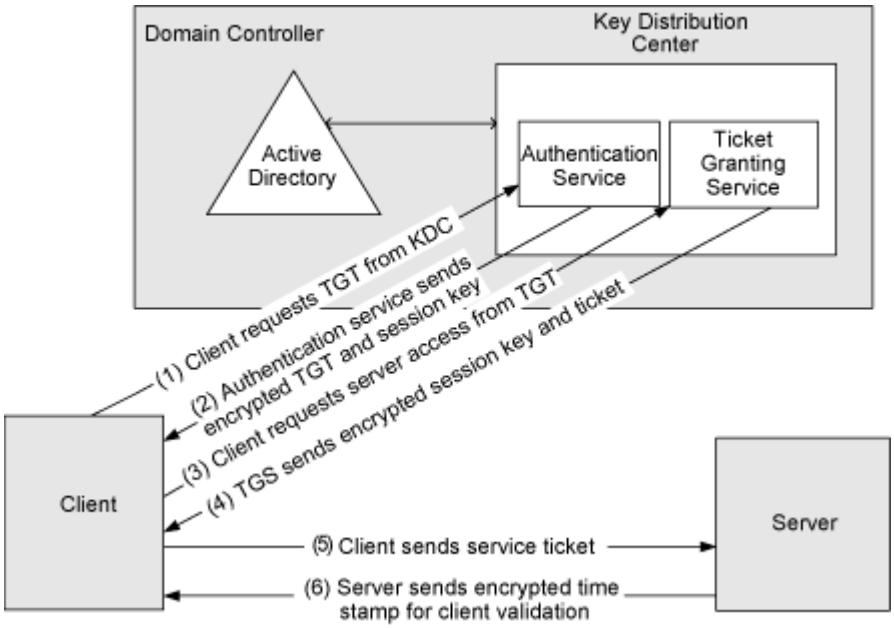
LDAP (X.500)-

- handles user authentication/authorization as well as control access to AD objects.
- Also specifies formats and methods to query directories.
- LDAP entries are contained in a directory information tree (DIT).
- AD is based on LDAP so AD queries also use LDAP format. E.g. CN=jsnow, CN=users, DC=google, DC=com
- LDAPS encrypt transmission with TLS.
- LDAPS uses port 636.

Kerberos-

- method of access, authentication and authorization that is more secure than RADIUS, TACACS or LDAP**.**

- In Kerberos 5, Authentication Service (AS) Exchange authenticates users and provides users with a ticket-granting ticket (TGT).
    1. When a user wants to gain access to a network resource, that user's TGT is sent to a computer that provides Kerberos Ticket Granting Service (TGS) Exchange.
    2. A TGS server uses a TGT to create a session key for the client requesting service and the server providing service.
    3. A client requesting service sends a session key to a server
    4. Client-Server (CS) exchange is used to enable a client and a server to authenticate one another.
    5. After these processes are completed, a client can gain access to services on a server.
- AS, CS, and TGS are the three main protocols used on a Kerberos network to provide authentication and authorization for use of resources.



- During the use of the Kerberos protocol, KDC stores, distributes and maintains both cryptographic session keys and secret keys.
- The master key is used to exchange the session keys.
- The keys are automatically distributed to the communicating client and the server.
- The KDC also provides the authentication services for the users.

Kerberos is a network authentication protocol in AD or Unix. Requires

1. A method of issuing tickets used for authentication- KDC: has 2 parts- Authentication Server (AS) and Ticket-Granting Server (TGS)
2. Time synchronization
3. A database of subjects or users.

#Kerberos by default does not provide SSO but can be enabled.

TACACS+

- alternative to RADIUS but cisco proprietary.
- TACACS is the first generation and combines the authentication and auditing process.
- XTACACS is the second generation and separates the authentication, authorization and auditing processes.

- TACACS+ is the 3rd generation and provides all the features of XTACACS along with extended two-factor user authentication.
- TACACS+ uses multiple challenge responses for authentication, authorization and auditing.
- It can interact with Kerberos and encrypts the entire authentication process which are its benefits over RADIUS.
- TACACS+ client sends START and CONTINUE packets and the server sends REPLY packets.

communications between a user (typically a PC) and the TACACS+ client are subject to compromise as they are usually not encrypted.

- Uses TCP 49

Figure 1: RADIUS vs. TACACS+

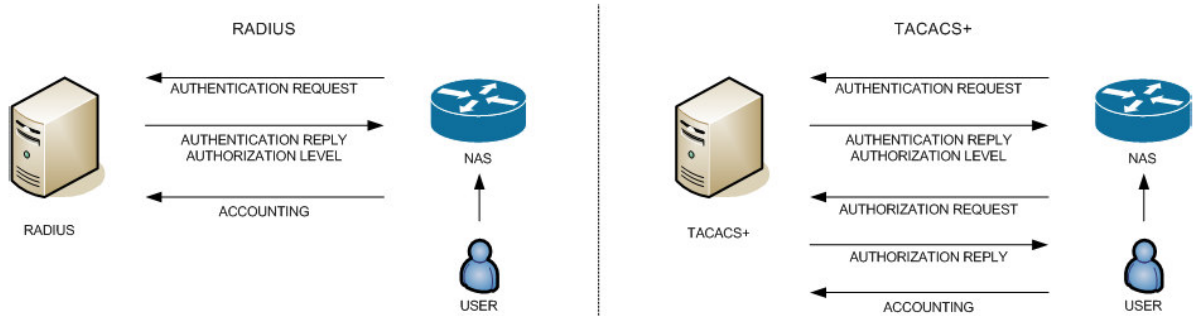


Table 1: RADIUS vs. TACACS+

RADIUS	TACACS+
Combines authentication & authorization.	Separates all 3 elements of AAA, making it more flexible.
Encrypts only the password.	Encrypts the username and password.
Requires each network device to contain authorization configuration.	Central management for authorization configuration.
No command logging.	Full command logging.
Minimal vendor support for authorization.	Supported by most major vendors.
UDP- Connectionless UDP ports 1645/1646, 1812/1813	TCP- Connection oriented TCP port 49
Designed for subscriber AAA	Designed for administrator AAA

CHAP-

- uses username and password combination to authenticate users.
- Used in PPP so its most common application is dial-up internet access user authentication.
- More secure than PAP.
- uses a 3-way handshake process to prevent replay attack where the server challenges the client.

- Client then responds with appropriate authentication information.
- Stops Session hijacking. RADIUS and PAP don't.

PAP-

- Password Authentication Protocol sends passwords in clear text.
- Use only as a last resort when the remote server does not support a stronger scheme such as CHAP or EAP.
- PPP uses PAP with dialup connection for authentication.

MSCHAP-

- Microsoft's CHAP is used by its client. Replaced by MSCHAPv2.
- It performs mutual authentication.
- Client authenticates to Server and Server authenticates to client.

RADIUS-

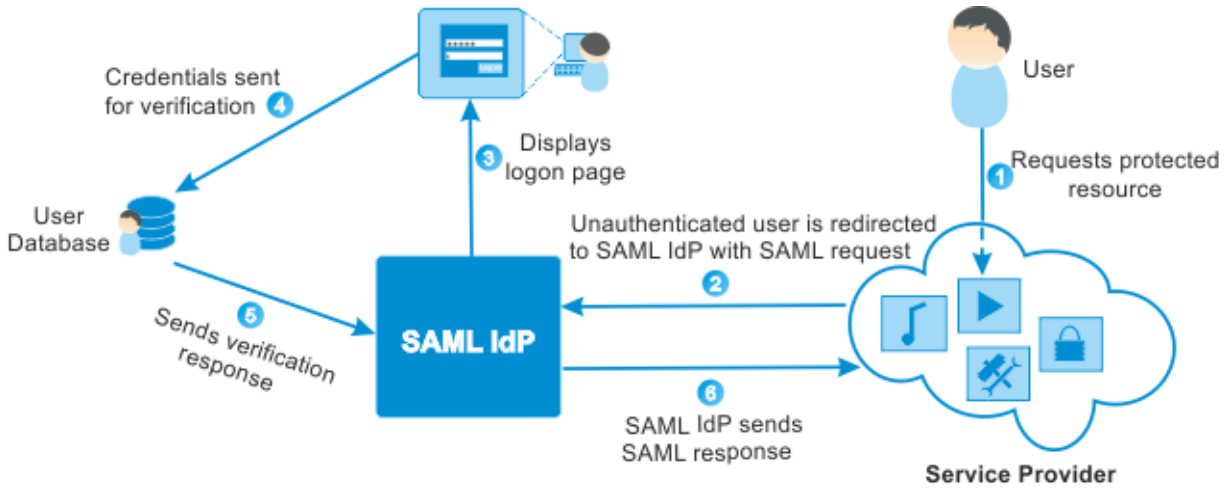
- Cross-platform remote access protocol
- Provides AAA.
- Centralized method of authentication for multiple remote access servers.
- RADIUS encrypts the password packets but not the entire authentication process.
- Uses UDP 1813 for accounting and 1812 for authenticating.

DIAMETER-

- An improvement over RADIUS
- Utilizes EAP, thereby providing better security than RADIUS
- Created to deal with VOIP and wireless services.
- Diameter was designed to be backwards compatible with RADIUS, some RADIUS servers have trouble working with Diameter servers.

SAML- (Security Assertion Markup Language)

- an XML based standard used to exchange authentication and authorization information between different parties.
- Not good for mobile.
    - Principal- user
    - Identity Provider (IdP)- source of identity information and authentication decision. authenticates principals and returns identity information to service providers. E.g. Auth0, ADFS, and Okta.
    - Service Providers (SP)- services that are requesting authentication and identity information about the principal.



OpenID Connect-

- allows clients to verify the identity of end users without managing their credentials.
- good for mobile. uses JWT Tokens.
- E.g. Many applications allow users to sign in using their Facebook credentials.
- OpenID works with OAuth and supports REST.
- OpenID connect is used for authentication while using OAuth for authorization

OAuth-

- Uses similar methodology as SAML to share login information
- SAML provides more control to enterprises to keep their SSO logins more secure, whereas OAuth is better on mobile.
- Many companies use it to provide secure access to protected resources.
- Ex. you can use the same account with Google, Facebook, PayPal, Twitter etc.

	SAML 2.0	**OpenID Connect**	**OAuth2**
Open standard for?	Federated Identity for authentication and authorization	Authentication	Delegated authorization
Primary use case	SSO for Enterprise	SSO for consumer apps	API authorization
Format	XML	JSON	JSON
History	Developed by OASIS in 2001	Developed by OpenID Foundation in 2004	Developed by Twitter and Google in 2006

Shibboleth-

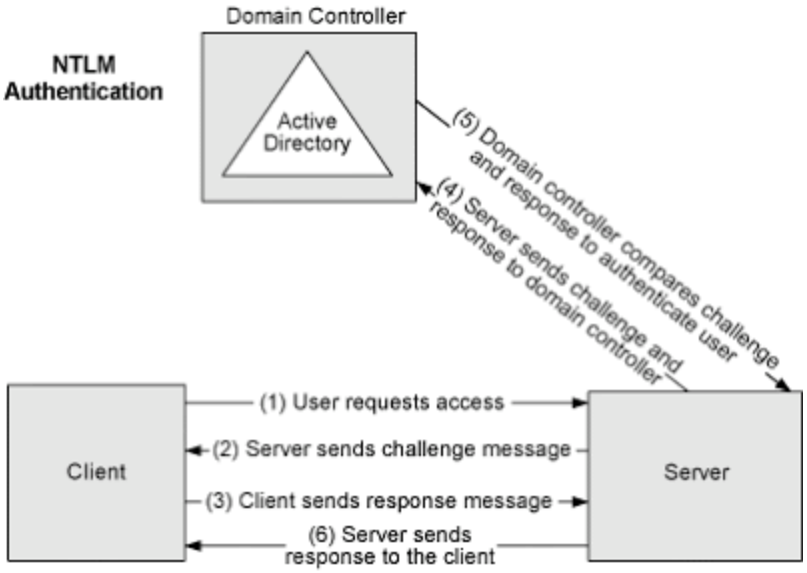
- open source and freely available federated identity solution.
- Includes open SAML libraries written in C++ and Java, making it easier for developers to expand its usefulness.

Secure token-

- provides for authentication across stateless platforms and
- can be used to identify the holder of the token to any service that uses the WS-Trust standard.
- Tokens are transportable.

NTLM-

- legacy proprietary SSO protocols that provide authentication, integrity and confidentiality within windows systems.
- Replaced by Kerberos
- They use a MD hashing algorithm to challenge users and check their credentials which is weak and ineffective.



4.3 Implement identity and access management controls

Access Control Models:

MAC-

- Uses (security) labels to determine access.
- Under MAC, a file, printer or computer would exist as an object. A user or group would exist as a subject.
- Highly secure than others.
- SELinux and Trusted Solaris are examples of OS specifically designed for MAC environments.
- E.g. enforce authorization rules by the OS. Users cannot override authentication or access control policies.

DAC-

- specifies that every object has an owner and the owner has full, explicit control of the object.
- More user friendly than RBAC.

ABAC-

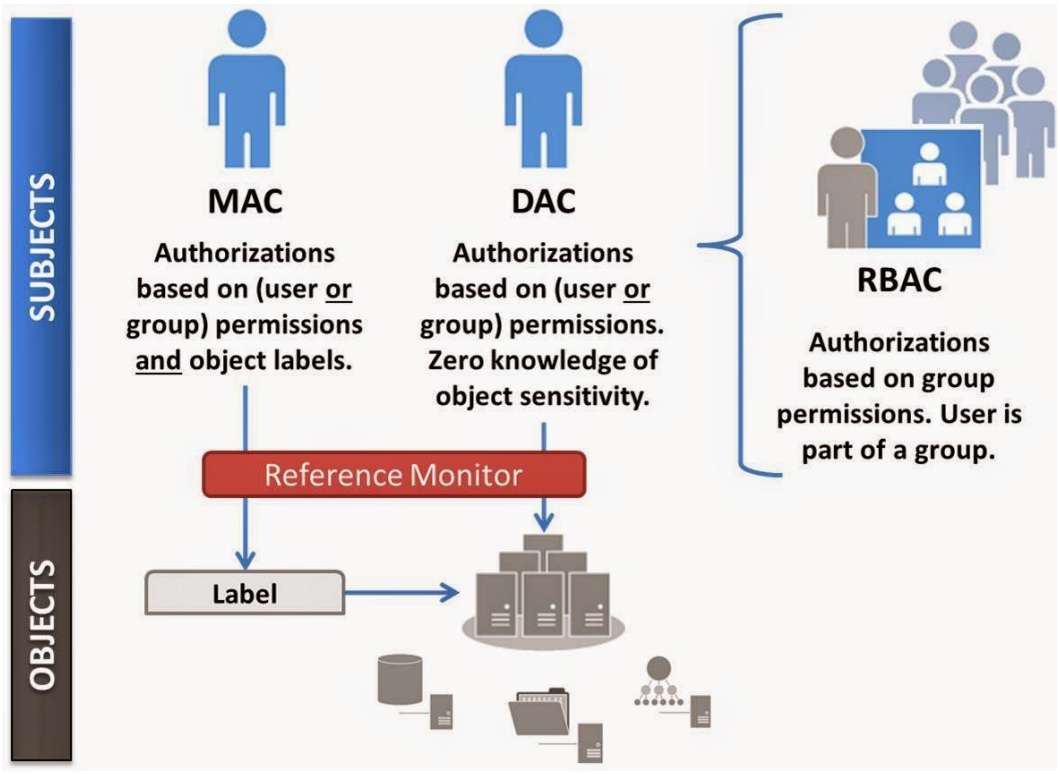
- uses attributes defined in policies to grant access to resources.
- dynamic and context-aware using IF-THEN statements.
- Commonly used in SDN
- E.g. you can use geographical location as an attribute.

Role-based access control-

- create a role for users
- assign access to the role instead of users.
- Has low security cost and easier to implement.

Rule-based access control-

- based on a set of approved instructions such as an ACL.
- E.g. A user needs access to the resource that he doesn't have access to.
- Ex. IPS can block traffic from the attacker when it detects an attack.

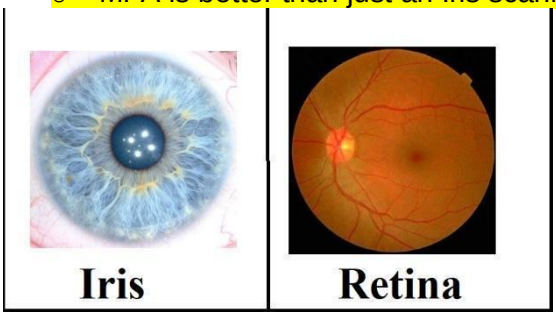


Physical access control

- **Proximity cards-** contactless card
- **Smart cards-** has embedded microchips and a certificate. The embedded certificate holds users' private key and is matched with a public key.

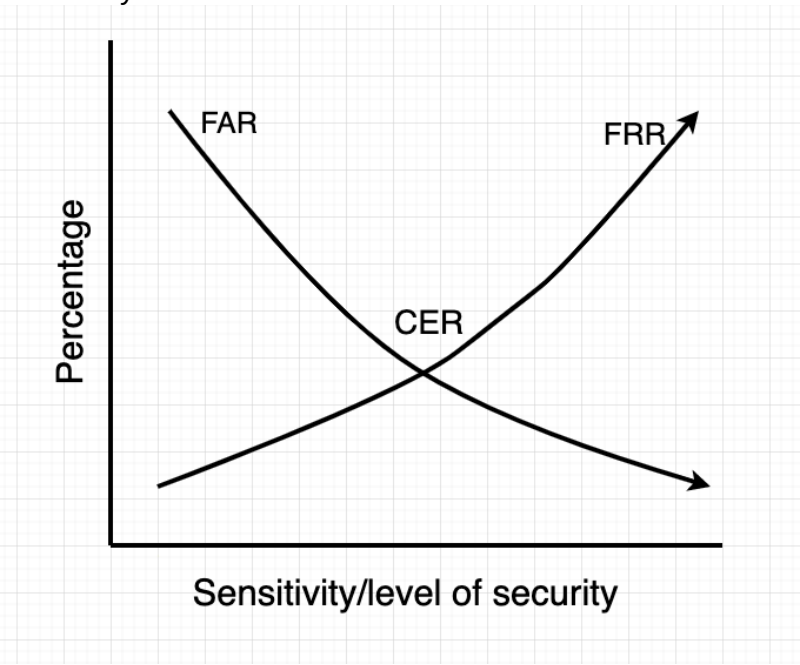
Biometric factors

- **Fingerprint Scanner-** For authentication and identification
- **Retinal Scanner-** use the pattern of blood vessels at the back of the eye. Most intrusive.
- **Iris Scanner-** pattern of the iris around the pupil. Compares the picture of the iris.
    - MFA is better than just an Iris scanner.



- **Voice recognition-** uses speech recognition to identify acoustic features. Least intrusive.
- **Facial recognition-** based on facial features
- **False acceptance rate (FAR)-** biometric system incorrectly identifies unauthorized users as authorized users.
- **False rejection rate (FRR)-** incorrectly rejects authorized users. Ex. 1 in 50 fingerprint scans of authorized users gets rejected.

- **Crossover error rate (CER)-** point where FAR and FRR meet. A lower CER indicates that the biometric system is more accurate.



Tokens- key fob with LCD that displays a number for a one time use and changes periodically. Uses one-time password authentication. can store digital certificates.
Token is provided with each request to the server. No session information is stored on the server.

- **Hardware-** Key fob like token
- **Software-** ex. Google Authenticator
- **HOTP- (**HMAC-based One-Time-Password)
    - Combines a secret key and an incrementing counter and uses HMAC to create a hash of the result. It then converts the result into an HOTP value of 6-8 digits.
    - Usable for 1 use.
- **TOTP- (**Time based OTP)
    - uses a timestamp instead of a counter.
    - Typically expires after 30 seconds.

Certificate-based authentication

- **CAC (Common Access Card)**
    - used by DOD to military personnel and contractors.
- **PIV (Personal Identity Verification)**
    - used by non-military federal employees and contractors.
    - specialized smart cards that include photo identification.
    - used to gain access into secure locations.
- **IEEE 802.1x-**
    - port based authentication protocol.
    - Requires users or devices to authenticate when they connect to specific wireless AP or a physical port.
    - User's identity is based on their credentials or certificate, which is confirmed by the RADIUS server.

File system security- NTFS supports user-level access differentiation FAT32 doesn't.
Database security-

- Data Control Language (DCL) implements security through access control and granular restrictions.
- Database views are used to limit user and group access to certain information based on the user privileges and the need to know.
- Two-phase commit ensures that the entire transaction is executed to ensure data integrity. If a portion of a transaction cannot complete, the entire transaction is not performed.
- Concurrency ensures that the most up-to-date information is shown to database users. To ensure concurrency, locks are often implemented at the page, table, row, or field level.
- Savepoints ensure that the database can return to a previous state if a system failure occurs.
- Database Activity Monitoring Prevention (DAMP) system is an active device that prevents unauthorized access. ABAC is not designed for databases.

4.4 Differentiate common account management practices

Account types

- **User accounts-** for regular users
- **Shared and generic accounts/credentials-** should not be used otherwise IAAA cannot be implemented
- **Guest accounts-** limited access to computer or network. Shared logon.
- **Service accounts-** used by the service or application and not an end user.
- **Privileged accounts-** has additional rights and privileges beyond a regular user

General concepts

- **Least privilege-** technical control where users or processes are granted only those rights and permissions needed to perform their assigned tasks or functions.
- **Onboarding/Offboarding**
- **Permission auditing and review**
- **Usage auditing and review**
- **Time-of-day restrictions-** Specifies when users can log on to a computer.
- **Recertification**- process of examining a user's permissions and determining if they still need access to what was previously granted. also ensures users are still employed and still require accounts.
- **Standard naming convention-** for servers, emails etc. Don't use jsmithAdmin for an admin account. Just use jsmith…. Always!!!
- **Account maintenance-** run script to list users inactive for more than 30 days and disable them.
- **Group-based access control-** put user accounts into security groups and assign privileges to the groups. E.g. use of security groups in AD to manage access to folders.
- **Location-based policies-** restricts access based on the location of the user

Account policy enforcement

- **Credential management-** Users are able to add credentials into the Credential manager in the Control Panel which stores them securely in special folders called vaults. Then, when users access web sites needing credentials, the system automatically retrieves the credentials from the vault and submits them to the web site.
- **Group policy-** to create password policies and implement within a domain.
- **Password complexity-** 7 characters of letters, symbols and numbers is stronger than 8 characters of just letters.
- **Expiration-** change regularly
- **Recovery-** verify user identity before resetting
- **Disablement-** disable account as soon as possible. Disabling the account ensures that user security keys (cryptographic keys) are retained. If the keys are deleted (such as when the account is deleted), it might not be possible to access files that the user encrypted.
- **Lockout-** prevent users from guessing password
- **Password history-** implement system to remember password history and prevent user to reuse
- **Password reuse-** prevent reuse of password
- **Password length-** enforces character length. More significant than password history or password age.

5.0 Risk Management

5.1 Importance of policies, plans and procedures

Standard Operating Procedure- step by step instructions employees can use to perform common tasks

Agreement types

- **BPA-** relationship between 2 partners including their obligations toward the partnership. Helps settle conflict when they arise. Just establishes expectations. Includes profit/loss sharing and addition/subtraction of partners.
- **SLA-** performance expectations from vendors such as minimum uptime and maximum downtime levels.
- **ISA-** Interconnection Security Agreement. Technical and security requirements for planning, establishing, maintaining and disconnecting a secure connection between 2 or more entities.
- **MOU/MOA-** defines responsibilities of both parties. Not as strict as SLA or ISA
    - not as formal as a traditional contract but still has a level of importance to all involved parties

Personal management

- **Mandatory vacations-** helps to discover malicious activities while the employee is away.
- **Job rotation-** ensures employees cannot continue malicious behavior.
- **Separation of duties-** prevents one person from controlling all critical functions.
- **Clean desk-** no sensitive paper
- **Background checks-** history of an individual
- **Exit interviews-** for feedback and collecting items.
- **Role-based awareness training**
    - **Data owner-** ensure data are classified correctly and ensure that the data is labeled to match the classification.
    - **System administrator-** responsible for overall security of a system.
    - **System owner-** high level executive with overall responsibility for the system. should receive training on how to manage particular systems.
    - **User-** train them not to click
    - **Privileged user-** with more rights and permissions than typical end users.
    - **Executive user-** need high-level briefings related to the risk that the organization faces
- **NDA-** ensures that proprietary data is not disclosed to unauthorized entities.
- **Onboarding-** granting individual access to an organization's computing resources.
- **Continuing education**
- **Acceptable use policy/rules of behavior-** purpose of IT equipment for users and their responsibilities when they access the systems.
- **Adverse actions-** actions against employees when wrongdoing has been found. E.g. Josh is a bank manager and has suspicions that one of his tellers has stolen money

from their respective station. After talking with his supervisor, he places the employee on leave with pay, changes their computer account to suspended, and takes their prox card and building keys

General security policies

- **Social media networks/applications**
- **Personal email-** can introduce malware to the corporate network.

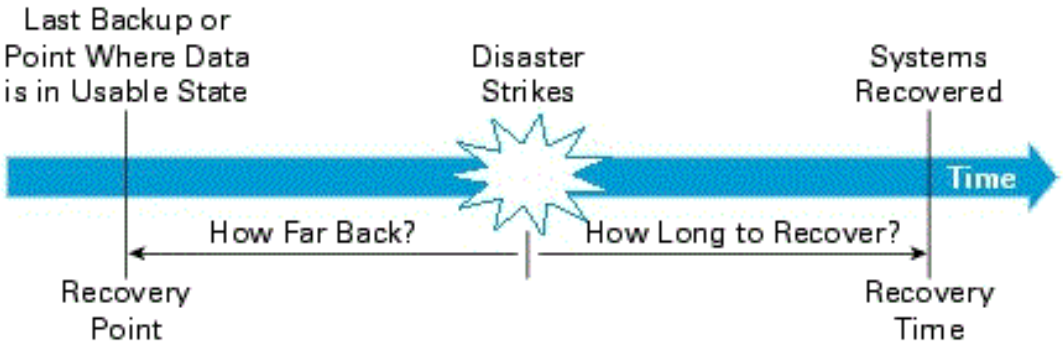
5.2 Business impact analysis concepts

RTO- (Recovery Time Objective)-

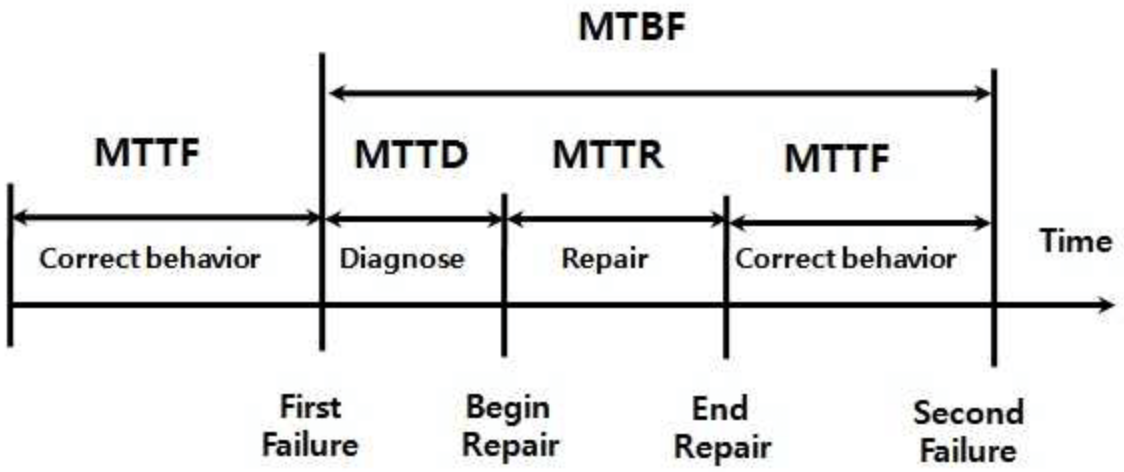
- how long can it take to restore a system after an outage.
- Refers to time not data.
-

RPO- (Recovery Point Objective)

- a point in time where data loss is acceptable.
- If you cannot lose more than 1 weeks worth of data (RPO is 1 week), your backup should be able to recover documents from 1 week.



MTBF- Mean Time Between Failures is a prediction of how often a repairable system will fail.
MTTR- Mean Time to Restore/Repair identifies the average time to restore a failed system
MTTF- expected lifetime of a non-repairable system.



Mission-essential functions
Identification of critical systems
Single Point of Failure- weakness which can enable one fault to cause a whole system to stop operating. A configuration can be a SPoF. A cluster is not SPoF because it has several systems connected together to rely on each other.
Impact- cost associated with a realized risk

- **Life**
- **Property**
- **Safety**
- **Finance**
- **Reputation**

Privacy impact assessment-

- Identifies potential risks related to PII
- ensures the organization is complying with laws and regulations.

Privacy threshold assessment-

- analysis of whether PII is collected and maintained by a system.

5.3 Risk management processes and concepts

Threat assessment- structured analysis of threat. Evaluates potential dangers that can compromise the CIA of data or system.

- **Environmental-** Threats from hurricane, earthquake etc.
- **Man Made-** from attacker or by authorized personnel by mistake.
- **Internal vs. External-** within organization vs outside

Risk assessment- analyze potential risk based on statistical and mathematical models.

- **SLE-** Single Loss Expectancy.
  - Product of Exposure Factor (EF) and Asset Value.
- **ARO-** Annual Rate of Occurrence
- **ALE-** Annual Loss Expectancy= SLE*ARO
- **Asset Value-** amount of money required to replace the asset.

- **Risk register-** comprehensive document listing known information about risks. Typically includes risk scores along with recommended security controls.
- **Likelihood of occurrence-** chance that a particular risk can occur
- **Supply chain assessment-** everything needed to produce and sell a product.
- **Impact-** measure of the actual loss when a threat exploits a vulnerability.
- **Quantitative-** measures risk using a specific monetary amount.
- **Testing**
  - **Penetration testing authorization**
  - **Vulnerability testing authorization-** Tools: Password crackers, network scanners (ping, SYN stealth, port, service OS), Network mapping, wireless scanner/cracker, rogue system detection, banner grabbing
- **Risk response techniques**
  - **Accept-** low cost or low impact risk can be accepted.
  - **Transfer-** purchasing insurance, outsourcing or contracting a third party.
  - **Avoid-** by not participating in risky activity. Ex. avoiding an application that requires too many ports open in the firewall.
  - **Mitigate-** implement controls. Using antivirus to mitigate risk of malware.

Change management

5.4 Incident response procedures

Incident response plan

- **Documented incident types/category definitions-** define what needs to be responded. E.g. interruption of service, malware delivery, malicious communication, data exfiltration, phishing attack etc.
- **Roles and responsibilities-** Senior management with enough authority to get things done, network admin with technical expertise to understand the issue, security expert who knows how to collect and analyze evidence, communication expert to relay information to the public.
- **Reporting requirements/escalation-** notify the executives about a serious incident and inform the supervisor about the incident while working on it.
- **Cyber-incident response teams-** skilled with how to identify and validate an incident, how to collect evidence and how to protect the collected evidence.
- **Exercise-** drill

Incident response process

- **Preparation-** establish and maintain an incident response plan and incident response procedure.
- **Identification-** weed out false positives to identify actual incidents.
- **Containment-** isolate/quarantine the device or system
- **Eradication-** remove malicious components
- **Recovery-** return a system to normal operation
- **Lessons learned-** Perform a root cause analysis and document any lessons learnt.

5.5 Basic concepts of forensics

Order of volatility- start collecting evidence that will disappear faster first.

1. CPU cache & CPU register
2. Routing tables, ARP cache, process tables, kernel statistics
3. Live network connections and data flows
4. RAM,
5. Temporary file, swap or paging file,
6. hard drive data,
7. logs stored on remote systems,
8. archived media.

Chain of custody-

- Assures that the evidence has been controlled and handled properly after collection.
- Documents who handled the evidence and when they handled it.
- Governs the collection, analysis and preservation of the evidence before the evidence is produced in a court of law.

Legal hold- once you realize your organization needs to preserve evidence, you must properly preserve any and all digital evidence related to a potential case.

Data acquisition

- **Capture system image-** forensic image is a bit-by-bit copy of the data and does not modify the data during the capture.
- **Network traffic and logs-** helps recreate events leading up to and during the incident.
- **Capture video-** cctv
- **Record time offset-** difference between the system clock and the actual time.
- **Take hashes-** provides integrity of the captured images.
- **Screenshots-** take pictures before analysis. shows the state of a computer at the time it was collected by law enforcement
- **Witness interviews-** for first hand report

Preservation

Recovery- restoring of lost data

Strategic intelligence/counterintelligence gathering-

- use of all resources to make determinations.
- Deals with collecting information to be used during prosecution, as well as locating information that may be used by the opposition against you.

Active logging- allows you to document access to the evidence, including photographic or video records showing the manner in which the evidence is secured. E.g. enable more logging in the firewall if attack is discovered.

Track man-hours

5.6 Disaster recovery and continuity of operation

BCP- identifies critical systems and components that need to be protected.

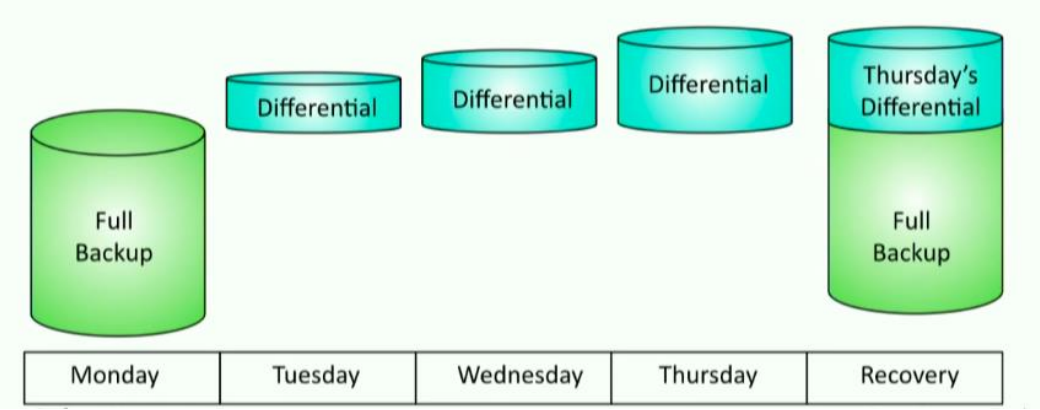
DRP- has information relating to the disaster recovery strategy such as how the company will require with minimal lost time and money.

IT contingency plan- specifies alternate procedures for disruptions of service.
Recovery Sites- alternate processing site to be used after a disaster

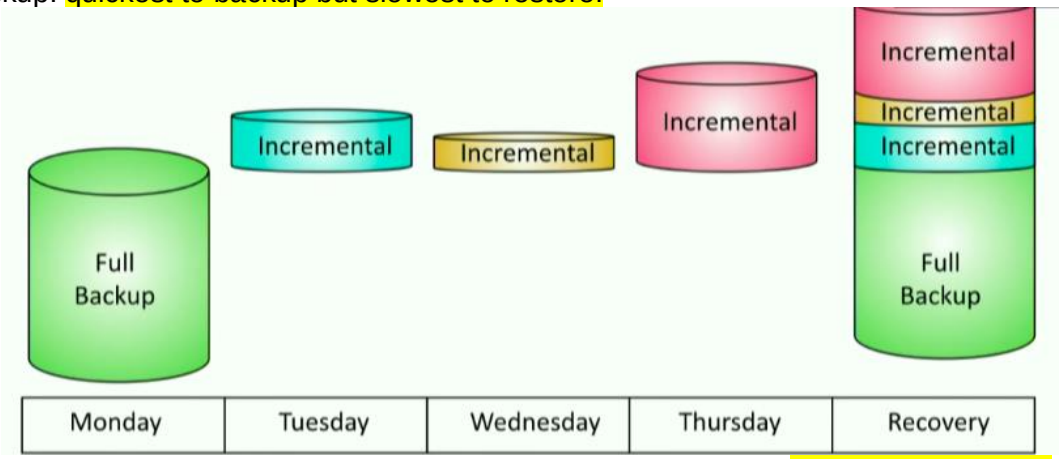
- **Hot Site-** would be up 24/7 and be able to take over functionality. Expense and administration are disadvantages.
- **Cold site-** has power and connectivity needed for a recovery site. Least expensive and hardest to test.
- **Warm Site-** compromise between 2.

Order of restoration- bring back the least critical function to the primary site. Keep the critical functions as long as necessary
Backup concepts

- **Differential-** backs up data that changed since last full backup.



- **Incremental-** backs up all the data that has changed since the last full or incremental backup. quickest to backup but slowest to restore.



- **Snapshots-** captures the data at a point in time. Image backup. If a system crashed, restoring the snapshot would be the fastest way to restore the system.
- **Full-** backs up all selected data

Geographic considerations

- **Off-site backups-** copy of backup in a separate geographic location
- **Distance-** some needs to be really close so that backups can be easily retrieved. Some need to be far away so that it is saved from geographical disaster.
- **Location selection**

- **Legal implications-** PII and PHI should be protected according to HIPAA.
- **Data sovereignty-** data stored within their borders is subject to their laws. Data originating within their borders must be stored there.

Continuity of operation planning

- **Exercises/tabletop**
- **After-action reports**
- **Failover-** process for moving from a normal operational capability to the continuity-of-operations version of the business.
- **Alternate processing sites-** involve contracting with a third party, who provides a location and equipment to be used in the event of an emergency.
- **Alternate business practices-** new sites might not have everything needed for normal operations so seek for alternate business practices. Ex. work from home, revert to paper and pen.

5.7 Various types of controls

Deterrent- discourage the attacker. E.g. law, warning sign, login banner (only authorized user can login)
Preventative- prevents specific actions from occurring. E.g. mantrap prevents tailgating, firewall, configures OS to lockout after 5 minutes of inactivity.
Detective- detects physical breach. E.g. IDS, motion detector
Corrective- post event effort to minimize the extent of damage
Compensating- restores using different methods. E.g. backup, warm site, UPS
Technical- use of technology to control risk. Also called Logical control.
Administrative- policy and procedure used to limit security risk.
Physical- prevents physical action from occurring.

5.8 Data security and privacy practices

Data destruction and media sanitization

- **Burning-** for sensitive papers
- **Shredding-** repeatedly overwriting the space where the file is located with 1s and 0s.
- **Pulping-** reduces the shredded paper to mash or puree
- **Pulverizing-** physically destroying with a sledge hammer.
- **Degaussing-** passing a disk through powerful electromagnet
- **Purging-** general term for removing sensitive data from a device
- **Wiping-** bit level overwriting process. DoD standard 5220.22-M recommends 7 wipes to completely wipe data.

Data sensitivity labeling and handling

- **Confidential-** secret among a certain group of people
- **Private-** information about an individual that should be remain private
- **Public-** available to anyone

- **Proprietary-** data related to the owner.
- **PII-** Personally Identifiable Information like Full name, birthday etc.
- **PHI-** personal Health information

Data roles

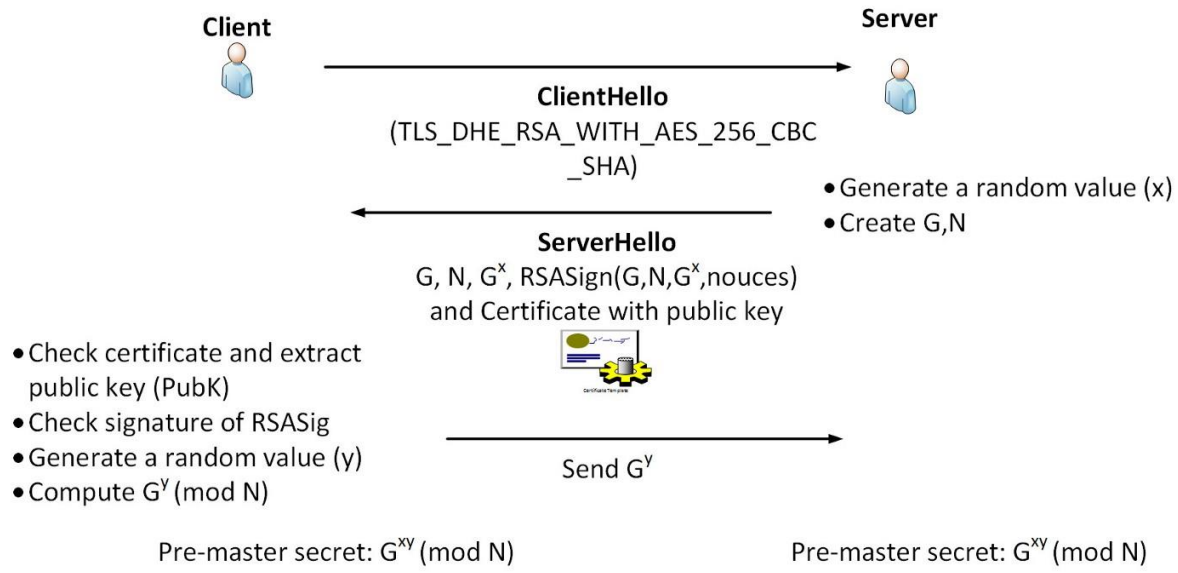
- **Owner-** has overall responsibility for the protection of data. makes business decisions regarding the data.
- **Steward-** responsible for data accuracy, privacy and adding sensitivity labels to the data.
- **Custodian-** handles routine tasks to protect data. manages access rights and sets security controls to the data

A human resource employee would be an example of a security role. These individuals maintain access to data as well as integrity.

- **Privacy officer-** responsible for ensuring the organization complies with relevant laws. sets privacy policies and implements privacy processes and procedures.

Data retention- how long should data be kept before destroying
Legal and compliance- follow law like HIPAA, GLBA, SOX, GDPR for handling data

6.0 Cryptography and PKI



Part of Client Hello in TLS encryption:

TLS_DHE_RSA_WITH_AES_256_CBC_SHA

TLS- Tunneling protocol
DHE-RSA- Key Exchange method
AES-256- Symmetric Encryption method
CBC- Cipher Mode
SHA- Hashing algorithm

6.1 Basic concepts of cryptography

Symmetric algorithms- Uses the same key to encrypt and decrypt the data. E.g. RADIUS
Modes of operation- ECB, GCM etc.
Asymmetric algorithms- Uses public and private key combinations to encrypt and decrypt data. Requires a certificate and a PKI.
Hashing- string of characters created with a hashing algorithm to verify integrity of data. One-way function.
Salt- extra character added in the password before hashing them to make it strong
IV- fixed size random or pseudo-random number that helps create random encryption keys. Should be large enough so that the algorithm doesn't reuse the same IV and recreate the same encryption key.
Nonce- Number that is used once. Algorithms use Nonce as a seed or starting number
Elliptic curve- requires less computing power. used with small wireless devices. Serves as an alternative to the RSA algorithm and provides similar functionalities, but ECC has a higher strength per bit than RSA.
Weak/deprecated algorithms- already cracked algorithms
Key exchange- like Diffie-Hellman. Used for exchanging symmetric key.

Digital signatures- provides integrity, authentication and non-repudiation in email. creates hash for the data and encrypts the hash with its private key to ensure authenticity.
Diffusion- effective diffusion should ensure significant change in ciphertext when there is a small change in plaintext.
VS.
Confusion- when the ciphertext is significantly different from the plaintext, it creates confusion which is a good thing.
Collision- when 2 passwords create the same hash.
Steganography- hides messages within a file. Watermark is a commercial application of steganography. E.g. hide message within the white space of a JPEG or GIF. (size on disk -size)
Obfuscation- hides data or makes something unclear. Does not necessarily convert plaintext to ciphertext.
Stream vs. block-

- Stream cipher encrypts data as a stream of bits or bytes.
- Block cipher divides large files into a block of 64-bit, 128-bit etc. and then encrypts this block.
- Stream cipher is efficient if data is sent in a continuous stream like streaming audio, video over the network.
- One-time pad works like stream ciphers

Key strength- larger key has more entropy. AES-256 is better than AES-128
Session keys- symmetric key used for encrypting messages during a communication session.
Ephemeral key- lasting for a very short time and re-created for each session.
Secret algorithm- privately kept algorithm but also prevents review from experts.
Data-in-transit- data sent over the network. Use secure protocols like HTTPS.
Data-at-rest- data stored on media. Individual field in database (SSN), folder, individual files or the full disk.
a process of deleting data by sending an eraser to clear the instruction in an address of nonvolatile memory.
Data-in-use- data used by the computer for processing. Encrypt data after use and purge memory of sensitive data
Random/pseudo-random number generation- used to generate cryptographic keys. PRNG is used in symmetric algorithms such as AES, DES and Blowfish. RNG is used in asymmetric ciphers such as RSA, Diffie-Hellman, and ECC.
Key stretching- Techniques used to increase the strength of stored passwords by salting it. OR, Perform multiple rounds of password hashing.
Helps prevent brute force and rainbow table attacks
Implementation vs. algorithm selection

- **Crypto service provider-** software library of cryptographic standards and algorithms. E.g. Active Directory Certificate Services.
- **Crypto modules-** set of hardware, software/firmware that implements cryptographic functions. This includes algorithms for encryption and hashing, key generation, and authentication techniques such as a digital signature. E.g. Microsoft Kernel Mode Cryptographic Module.

Perfect forward secrecy-

- Feature of specific key agreement protocols that gives assurances your session keys will not be compromised even if the private key of the server is compromised.
- protects past sessions against future compromises of secret keys or passwords.
- By generating a unique session key for every session a user initiates, even the compromise of a single session key will not affect any data other than that exchanged in the specific session protected by that particular key

Security through obscurity- concept that security can be achieved by hiding what is being secured.

Common use cases:

Low power devices- ECC is used for low-power application. Use it for wireless devices, handheld computers, smart cards etc.
Low latency- Stream ciphers have low latency
High resiliency- addresses the issue of data leakage from a side-channel attack.
Supporting confidentiality- use encryption
Supporting integrity- use hashing
Supporting obfuscation- accomplished through encryption and steganography
Supporting authentication- validating that the message originator is indeed who they say they are. Often implemented using digital certificates.
Supporting non-repudiation- use digital signatures
Resource vs. security constraints- resource constraints include available bandwidth, financial constraints etc. Security constraints would deal with the limitations of the particular cryptography chosen.

6.2 Cryptography algorithms and their basic characteristics

Symmetric Algorithms:

Algorithm	Block size	Key size	Characteristics
AES	128-bit	128, 192, 256	Fast, Strong, Efficient (less resource intensive)
DES	64	56-bit	Uses 16 rounds of computation. Can be broken with Brute Force Attack
3DES	64	56, 112, 168	Triple DES; Uses 48 rounds of computation. Used in legacy hardware that does not support AES
RC4	Stream Cipher	1-2048	Rivest Cipher; Susceptible to weak keys. Used in WEP.
Blowfish	64	32-448	Faster than AES-256
Twofish	128	128, 192, 256	2 times Blowfish

Cipher modes

ECB (Electronic Code Book)

- simplest cipher mode so deprecated.
- It divides the plaintext into blocks and encrypts each block using the SAME key.

CBC (Cipher Block Chaining)

- Encrypts first block with an IV.
- Combines subsequent block with previous block using XOR operation.
- Suffers pipeline delays.
- Vulnerable to POODLE attack.

CTR/CM/CTM (Counter Mode)

- combines an IV with a counter to encrypt each block.
- Converts a block of cipher (block of data) into a stream cipher (one bit at a time).

GCM (Galois/Counter Mode)

- combines CTM with hashing techniques for integrity.
- Uses a special binary field (called a Galois field) to provide authenticated encryption.
- Recognized by NIST and is used in 802.1AE standard

Stream vs. block- Stream cipher process one bit at a time and block cipher process one block of bits at a time. Block cipher example- DES, AES, IDEA, Blowfish, RC5

Asymmetric algorithms

Offers easy key exchange and key management.
Very strong but very resource intensive. Normally used for exchanging symmetric keys and the rest of the encryption is done with a symmetric key.
Uses 2 keys in a matched pair.

- If the public key encrypts information, only the matching private key can decrypt it
- If the private key encrypts information, only the matching public key can decrypt it

RSA

- Provides both encryption and authentication.
- uses the product of 2 very large prime numbers. It is difficult to factor large prime numbers. Therefore, it is difficult to break the encryption.
- Requires higher processing power due to the factorability of numbers but ensures efficient key management.
- TPMs and Hardware Security Modules (HSMs) provide secure storage for RSA keys.
- Based on Diffie-Hellman key exchange concepts using static keys.
- Used as a de facto standard for Digital Signatures.
- Can prevent MITM attack by providing authentication before the exchange of public and private keys.
- Lacks Forward Secrecy so if an attacker records the encrypted packet and steals the private key, data is exposed.
- Use RSA and DH together for authentication and perfect forward secrecy.

DSA

- Digital signature standard for the US government.
- Published by NIST and NSA.

Diffie-Hellman

- A key exchange algorithm. privately shares symmetric keys over the public network. Supports both static and ephemeral keys. Commonly used for TLS.
- Does not encrypt actual data.
- Vulnerable to MITM because DH does not have an authentication mechanism. Use RSA with DH for authentication.
- **Groups-** more than 25 groups: DH Group 1, DH Group 2 and so on. Higher means more secure. E.g. DH group 1 uses 768 bits, DH group 2 uses 3072 etc.
- **DHE-** Diffie-Hellman Ephemeral. Generates different keys for each session.
- **ECDHE-** Elliptic Curve Diffie-Hellman Ephemeral. Uses ephemeral keys generated using ECC.

ELGamal is an asymmetric public key encryption algorithm based on the Diffie-Hellman key agreement.
Elliptic curve- requires less processing power but is difficult to crack. Used for low-power devices like small wireless devices.
PGP/GPG-

- PGP establishes a web of trust between users which means the users generate and distribute their public key.
- These keys are signed by users for each other, establishing a community of users who trust each other for communication.
- Every user has a collection of signed public keys stored in a file known as a key ring.
- A level of trust and validity are associated with each key in that list.
- For example, if A trusts B more than C, there will be a higher level of trust for B compared to C.
- PGP does not use either CA servers or formal trust certificates. The users trust each other. In a PKI, CAs are arranged in a hierarchy and sign public key pairs.
- If a user wants to receive a file encrypted with PGP, the user must first supply the public key.
- Some PGP follows S/MIME standards and some follow OpenPGP. GNU Privacy Guard (GPG) is a free software based on the OpenPGP standard. GPG is an alternative to the PGP.

PGP can encrypt, decrypt and digitally sign email. Flexible use of both symmetric and asymmetric algorithms. PGP provides following functionalities:

- Confidentiality through IDEA (International Data Encryption Algorithm)
- Integrity through MD5
- Authentication through public key certificates
- Non-repudiation through encrypted signed messages

Hashing algorithms:

MD5- 128-bit hash represented in hexadecimal. least secure hashing algorithm.
SHA- SHA-0: not used, SHA-1: 160-bit hash, SHA-2 (SHA-224,256,384,512-bit hash), SHA-3 (SHA-224,256,384,512-bit hash)
HMAC (Hash-based Message Authentication code)

- Uses a secret key and a part of the hash to create MAC.
- Verifies not only the integrity but also the authenticity.
- If only hashing (MD5, SHA) is used, attackers can change the message, create a new hash and include the new hash with an altered message. But with HMAC, a key is used which the attacker would not know to create a HMAC.
- E.g. IPsec and TLS use HMAC-MD5 and HMAC-SHA1

RIPEMD- RACE Integrity Primitives Evaluation Message Digest was based on MD4 and was replaced by RIPEMD-160. Newer versions are RIPEMD-128,256,320

Key stretching algorithms:

Techniques used to increase the strength of stored passwords by salting it. Helps prevent brute force and rainbow table attacks.
BCRYPT- adds additional salt before encrypting with Blowfish. Uses on UNIX and Linux.
PBKDF2- Password-Based Key Derivation Function 2. Adds a salt of at least 64 bits. Used in WPA2, Apple iOS and Cisco OS.

Obfuscation:

XOR- eXclusive OR uses a binary key to create a cipher text. By itself, XOR does not provide a high level of security. Consequently, it is used in combination with symmetric ciphers.
ROT13- rotates 13 places.
Substitution ciphers- replaces plaintext with ciphertext using a fixed system. E.g. ACE to BDF has a 1 letter fixed system.

6.3 Install and configure wireless security settings

Cryptographic Protocols:

WPA-
- improved wireless security by giving alternatives to WEP with existing hardware.
- Susceptible to password cracking attacks.
- Attacker uses protocol analyzer to capture the authentication traffic and then uses an offline brute force attack to discover the passphrase.
- Supports older devices.

WPA2-
- permanent replacement for WPA.
- supports CCMP (based on AES) which is much stronger than the older TKIP protocol.

CCMP-
- Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
- Mode in which the AES cipher is used to provide message integrity.
- much more secure than TKIP.
- WPA2 with CCMP only uses a PSK, not usernames.

TKIP-
- Temporal Key Integrity Protocol
- Used with WPA.
- Not secure anymore.

Authentication protocols:

IEEE 802.1x-
- Port based authentication.
- More secure than simply disabling unused ports or MAC filtering.
- Secures the authentication process prior to a client gaining access to the network. Can be implemented with RADIUS or DIAMETER, LDAP, TACACS+ etc.

- 802.1x is a network-based authentication protocol that opens ports for network access when an organization authenticates a user's identity and authorizes them for access to the network.
- The user's identity is determined based on their credentials or certificate, which is confirmed by the RADIUS server.
- The RADIUS server is able to do this by communicating with the organization's directory, typically over LDAP or SAML protocol.
- When a user is authenticated via 802.1x for network access, a virtual port is opened on the access point allowing for communication.

EAP(Extensible Authentication Protocol)-

- only an authentication framework to send identifying information over-the-air.
- Not an actual encryption method.
- Used to pass the authentication information between the supplicant and the authentication server.
- The EAP type actually handles and defines the authentication.
- The AP acting as authenticator is only a proxy to allow the supplicant and the authentications server to communicate.

PEAP-

- encapsulates EAP within TLS. Hence, protected EAP.
- EAP was designed assuming a secure communication channel.
- Authenticates Wi-Fi clients using only server-side certificates.

EAP-FAST-

- EAP Flexible Authentication via Secure Tunneling.
- Cisco's proposal to replace LEAP. Retains the "Lightweight" implementation.
- Uses PAC (Protected Access Credentials) to establish the TLS tunnel in which the client's credential is verified.
- Consists of 3 phases- provisioning, establishment of a tunnel and authentication.

EAP-TLS-

- Relies on client-side and server-side certificates to perform authentication
- Advantage: a compromised password is not enough to break EAP-TLS. Intruder still needs info on the client-side certificate.
- One drawback is that the certificates must be managed on both the client and server side.
- Unlike most TLS implementations of HTTPS, such as on the World Wide Web, the majority of implementations of EAP-TLS require client-side X.509 certificates without giving the option to disable the requirement, even though the standard does not mandate their use. Some have identified this as having the potential to dramatically reduce adoption of EAP-TLS and prevent "open" but encrypted access points.

EAP-TTLS-

- TTLS encapsulates the TLS session, allowing for ANY authentication of the client.
- Authenticates clients using only server-side certificates.
- encrypts user credentials when users enter their usernames and passwords. Implemented in Enterprise mode and would use an 802.1x server.

RADIUS Federation-

- a group of RADIUS servers that assist with network roaming.
- The servers will validate the login credentials of a user belonging to another RADIUS server's network.
- The use of SSL-based tunneling and EAP packets makes the distributed authentication of RADIUS possible.

Methods:

PSK vs. Enterprise vs. Open-

- PSK uses a pre-shared key and does not provide individual authentication.
- Open mode doesn't use any security and allows all users to access the AP.
- Enterprise mode uses 802.1x server (implemented as RADIUS) to add authentication.

WPS-

- allows a wireless AP to broadcast an 8-digit PIN, which connecting devices use for authentication.
- Susceptible to brute force attack and packet sniffing.

Captive portals-

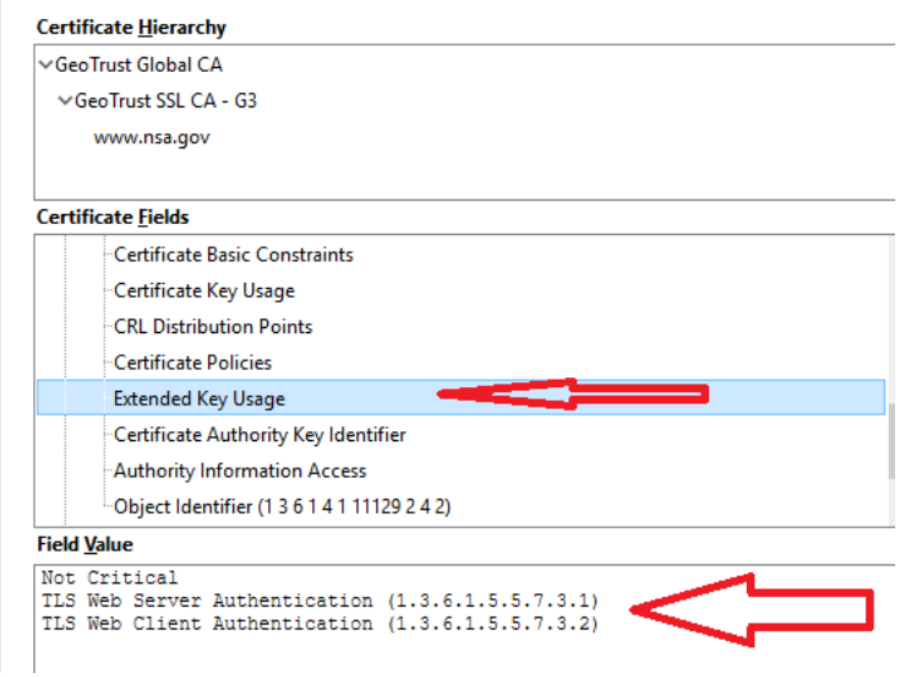
- a technical solution that forces clients using web browsers to complete a specific process before it allows them access to the network.
- It could be as simple as checking a box indicating they agree to terms and conditions.

6.4 Implement public key infrastructure

Components:

PKI- group of technologies used to request, create, manage, store, distribute, and revoke digital certificate.
Issuer signs the certificate. Principal possesses a public key. Verifier verifies a public key chain. Subject seeks to have a certificate validated.
CA- Certificate Authority. Issues, manages, validates and revokes certificates. E.g. VeriSign, GoDaddy.
Intermediate CA- Issues certificates that have been issued by a root authority or by another higher-level intermediate authority. Organizations frequently take the root CA offline for security reasons and allow the intermediate CA to actually issue certificates.
CRL- list of revoked certificates and is publicly available. Typically cached so not up-to-date. Has a latency period of 24-48 hours. Is slowly being replaced by OCSP.
Revoked certificates cannot be renewed. If a certificate is revoked, you must create a new certificate and key pair.

OCSP- Online Certificate Status Protocol. If CA revokes a certificate, the client using OCSP will know immediately. Generates a lot of real-time traffic.
CSR- Certificate Signing Request is a message sent from a user or application to a CA to apply for a digital certificate. Create RSA-based private key
Certificate- digital document that includes public key and information on the owner of the certificate: serial number, issuer, validity dates, subject, public key, usage etc.
Public key- publicly available.
Private key- should be kept secret. If the private key is exposed, a new public-private key should be created.
Object identifiers (OID)- optional extensions for X.509 certificates. They are dotted decimal numbers that would assist with identifying objects. E.g. 2.5.4.9 would identify a street address.



Concepts

Online vs. offline CA- Online CS is always connected, accessible and vulnerable. An offline CA is isolated from the network which reduces the likelihood that it could be compromised. For this reason, organizations frequently take the root CA offline and allow the intermediate CA to actually issue certificates.
Stapling (timestamp)- Web server staples timestamped OCSP response to a certificate to prevent traffic for each OCSP request to CA.
Pinning (host)- helps identify a fraudulent certificate. Once a certificate is associated with a certain host, that certificate is "pinned" to the host. In the event that another certificate is presented for the same host, it is likely that the new certificate is not valid.
When configured with public key pinning, the server responds to client HTTPS requests with an extra header which includes a list of hashes derived from valid public keys used in the website. Also includes a max-age field specifying how long the client should store and use the data.
Trust model- defines how various CAs trust each other. Also defines how the client of a given CA would trust the certificate from another CA. E.g.

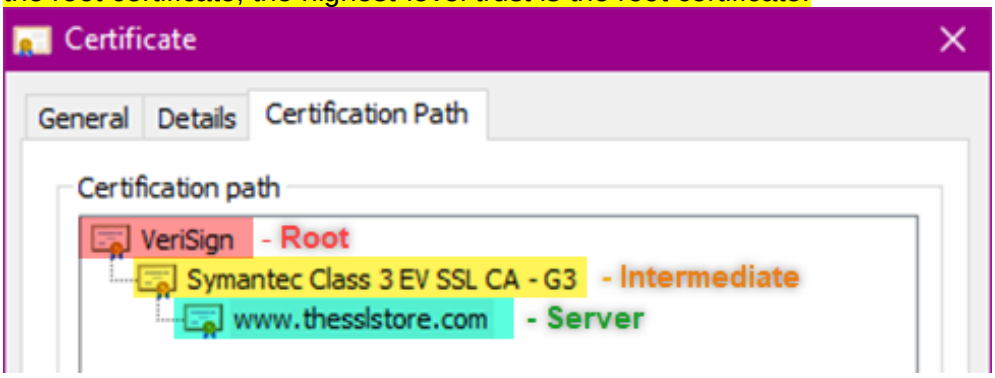
- PGP uses the Web of Trust model.
- Kerberos uses KDC.

- PKI uses CA.

Key escrow

- addresses the issue that a key might be lost.
- It's a proactive approach where copies of the private keys are held in escrow (stored) by a third party.
- The third party (key recovery agent) manages access to and use of the private keys.

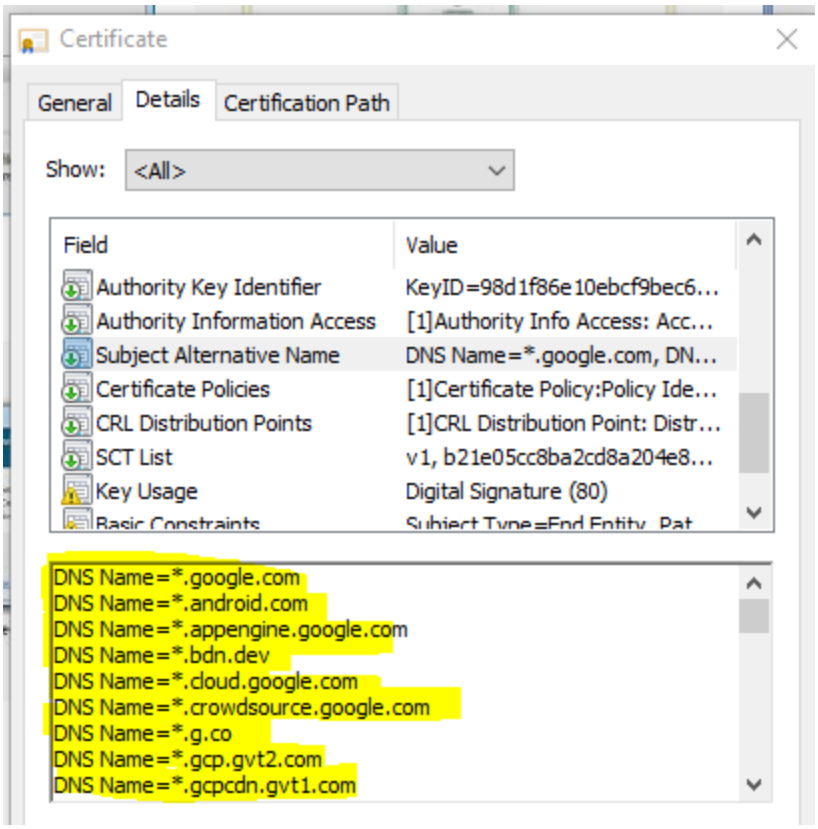
Certificate chaining- refers to the trust relationships between CAs and helps determine which certificate has the highest-level trust. For example, if you get a certificate from “A” and “A” trusts the root certificate, the highest-level trust is the root certificate.



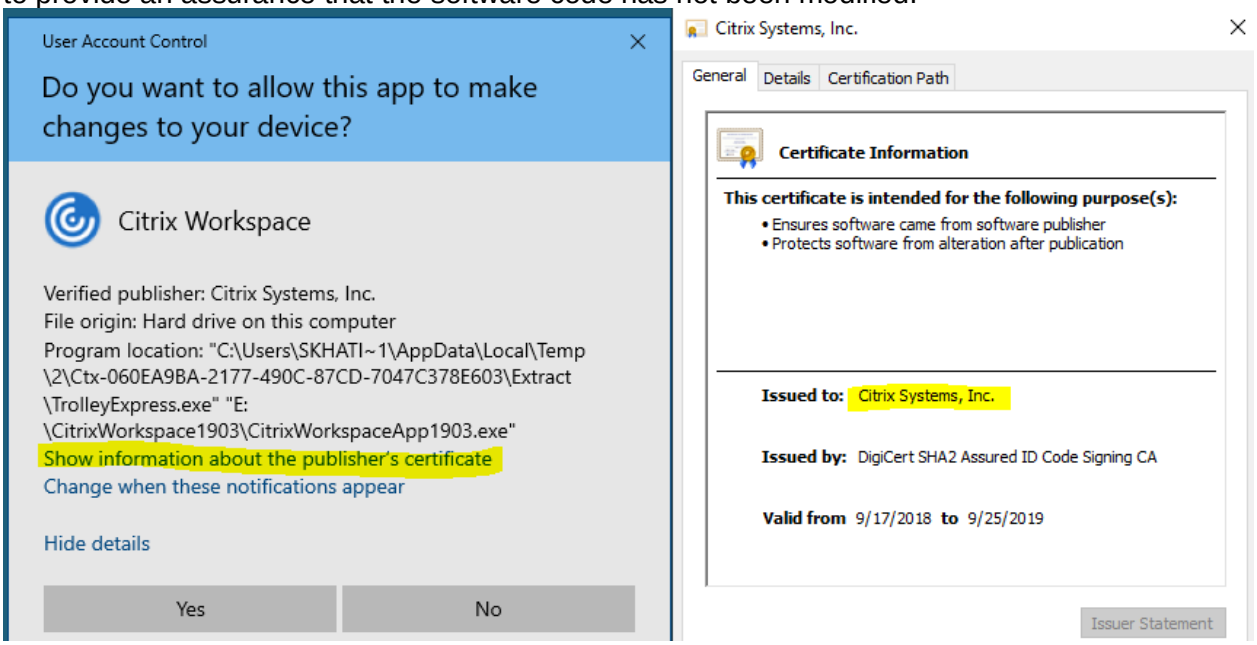
Types of certificates

Wildcard- can be used for multiple domains provided the domain name has the same root domain. *.google.com

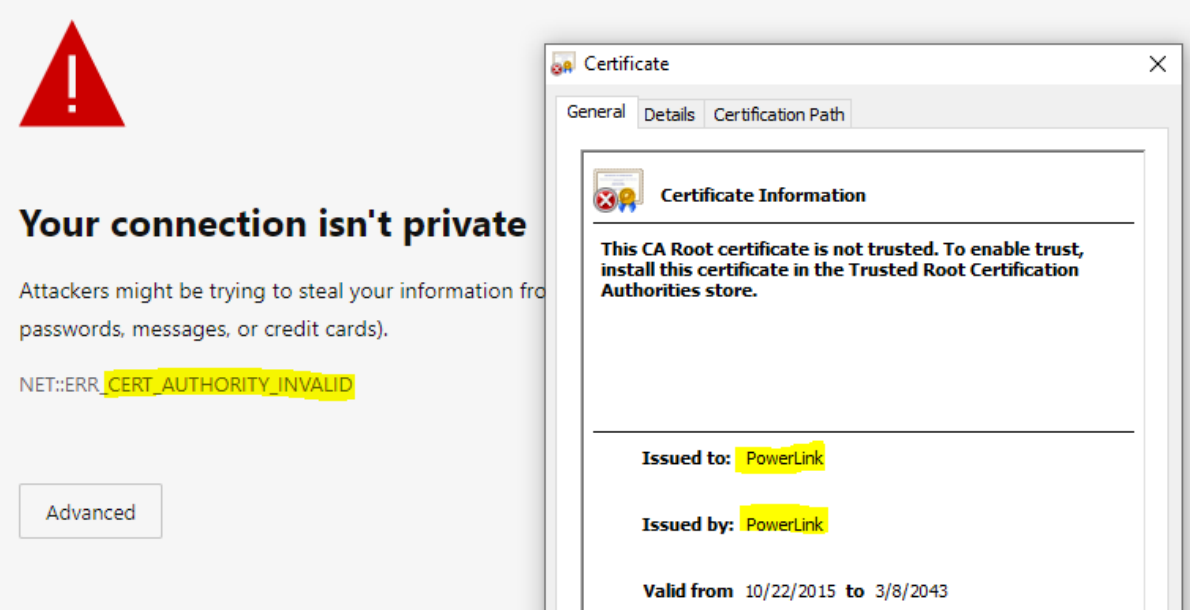
Subject Alternate Name (SAN)- allows you to add additional information such as an IP, host name associated with the certificate. also used for multiple domains that have different names. E.g. Google uses SANs of *.google.com, *.android.com, *cloud.google.com



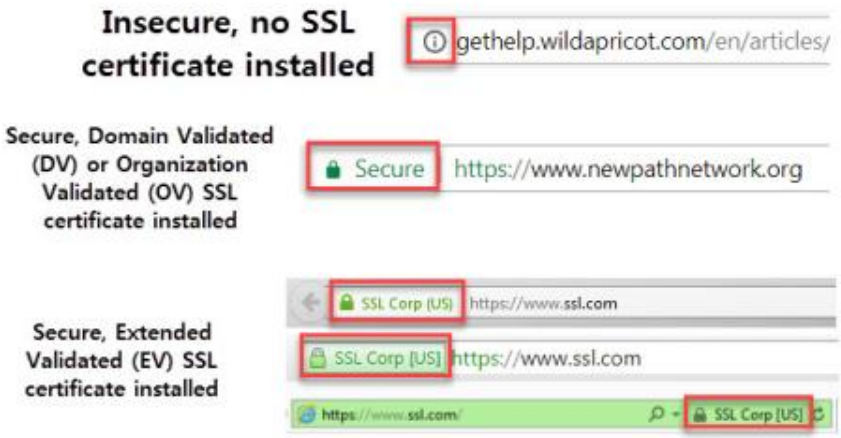
Code signing- process of assigning a certificate to code (executables). Uses digital signatures to provide an assurance that the software code has not been modified.



Self-signed- digitally signed by users. Often provided by IIS. a self-signed certificate will transmit a public key but that key will be rejected by browsers.



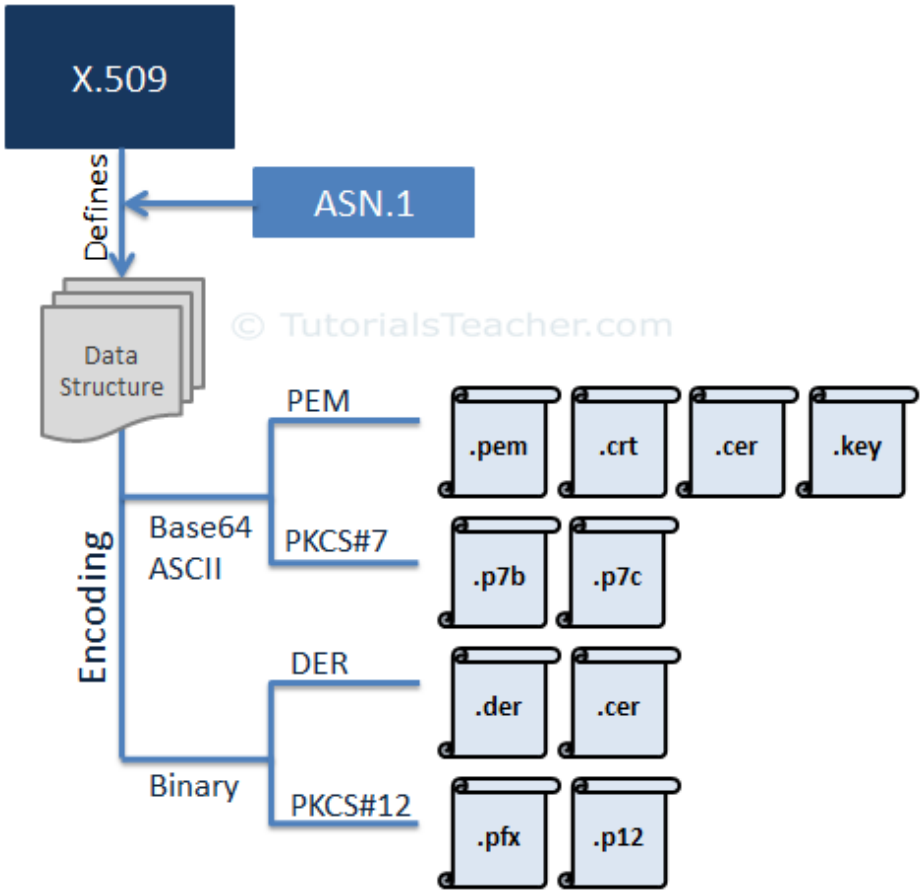
Machine/Computer- issued to a device or a computer. Identifies the computer within a domain.
Email- encryption of email and digital signature uses email certificate. E.g. S/MIME
User- can be issued to users. Used for encryption, authentication, smart cards, and more.
Root- first certificate created by the CA that identifies itself. If the CA's root certificate is placed in the store, all certificates issued by this CA are trusted.
The root CA must certify its own public key pair.
Domain validation- low-cost and are often used by web admins to offer TLS to a domain. They are validated using only the domain name.
Extended validation- provides additional validation for HTTPS web sites. The certificate provides the name of the legal entity responsible for the website. Provides a higher level of trust than domain validation because they are validated using more than the domain information.



Certificate formats

CER

- contains the certificate encoded in encrypted Base64.
- Storage of a single certificate. Does not support storage of the private key or certification path.
- Can be read by Windows servers.



PEM (Primary Enhanced Mail)

- Primarily used by open-source software like Apache. Unix/Linux based web servers.
- Can be read in a text editor.
- contains the "BEGIN CERTIFICATE/END CERTIFICATE" statements. DER doesn't

P7B (PKCS#7)

- Only contains certificates and chain certificates, not the private key
- Open standard used by Java (Tomcat) and supported by Windows.

DER

- The parent format of PEM.
- Think of it as a binary version of the base64-encoded PEM file.
- Storage of a single certificate. Does not support storage of the private key or certification path.
- By default, Windows exports certificate files as DER encoded files.

- Not routinely used very much outside of windows.

PFX (PKCS#12)

- Provided enhanced security versus the plain-text PEM format.
- Supports storage of private and public keys and all certificates in the path in one encrypted file.
- Preferably used by Windows and can be freely converted to PEM through use of openSSL.