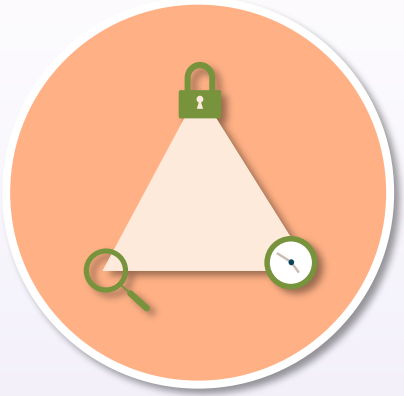
Welcome Back to the SSCP Bootcamp

Your instructor:

Michael J Shannon

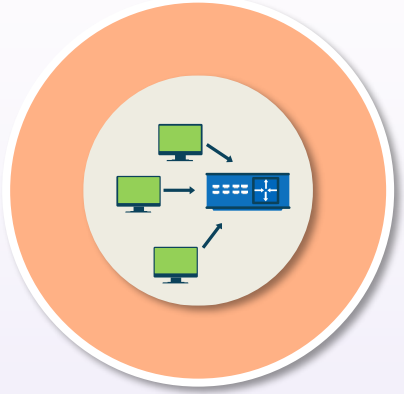
- **Class will begin at 10:00 A.M. Central Standard Time (CST)**

Systems Security Certified Practitioner (SSCP) Bootcamp



Session 3

Systems Security Certified Practitioner (SSCP)



Fundamental networking concepts

The OSI Reference Model

Number	Name	Description
7	Application	To accomplish a networked user task
6	Presentation	Expressing and translating data formats
5	Session	To accommodate multiple session connections
4	Transport	Connecting multiple programs on same system
3	Network (or internetwork)	Facilitate multihop communications across potentially different link networks
2	Link	Communication across a single link, including media access control
1	Physical	Specifies connectors, data rates, and encoding bits

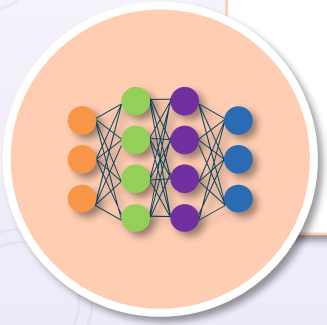
The OSI Reference Model

Number	Name	Description
7	Application	HTTP, FTP, SMTP, DNS, TELNET
6	Presentation	ASCII, PNG, MPEG, AVI, MIDI
5	Session	SSL/TLS, SQL, RPC, NFS
4	Transport	TCP, UDP, SPX, AppleTalk
3	Network (or internetwork)	IP, IPX, ICMP, ARP, BGP, OSPF
2	Link	PPP/SLIP, Ethernet, Frame Relay, ATM
1	Physical	Binary transmission, encoding, bit rates, voltages

The TCP/IP Reference Model

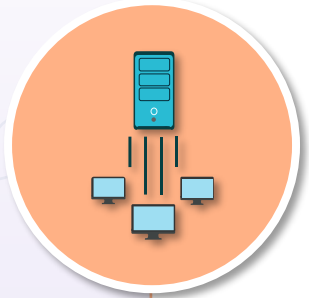
Number	OSI name	TCP/IP Model
7	Application	**Application**
6	Presentation	
5	Session	
4	Transport	**Transport** (host-to-host)
3	Network (or internetwork)	**Internet** (internetwork)
2	Link	**Network access**
1	Physical	

Network Topologies



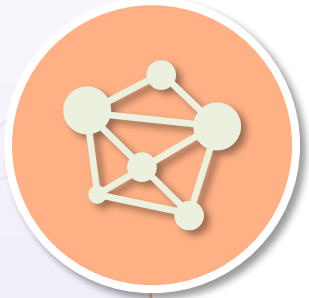
- Physical network topologies
  - Star
  - Full mesh = n(n - 1)/2
  - Partial mesh
  - Ring
- Logical network topologies
  - Star
  - Ring
  - Bus

Network Relationships



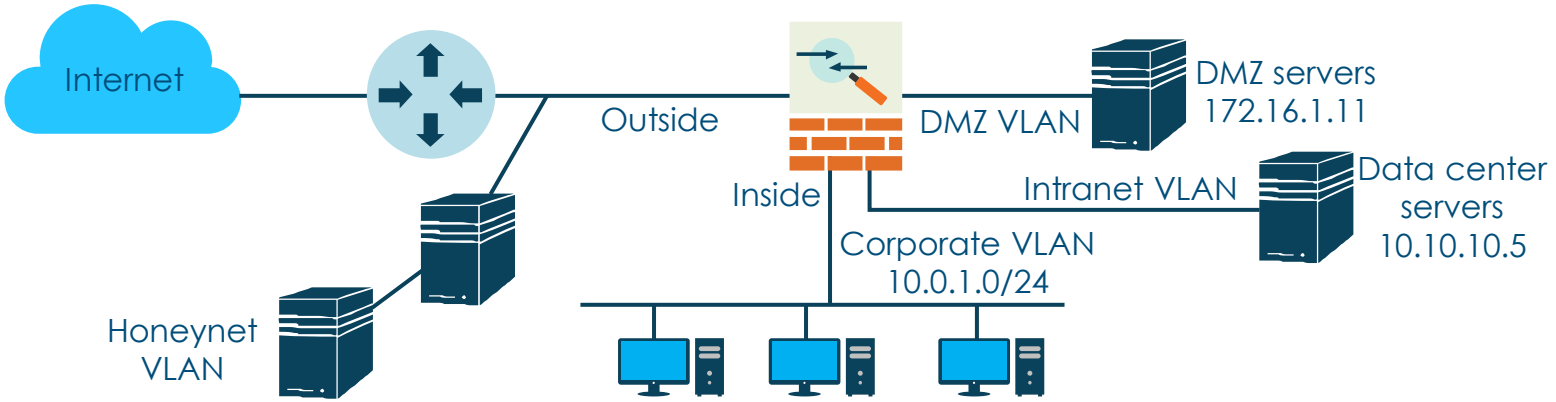
- Client-server – a relationship between cooperating programs in an application, composed of clients initiating requests for services and servers providing that function or service
- Peer-to-peer – a network relationship in which two or more computers are connected to a system in a way that they can access and share resources without having to go through the mediation of a different server computer
- Distributed – a form of peer-to-peer network configuration where every participant can communicate with one another without going through a centralized point

Network Media Types



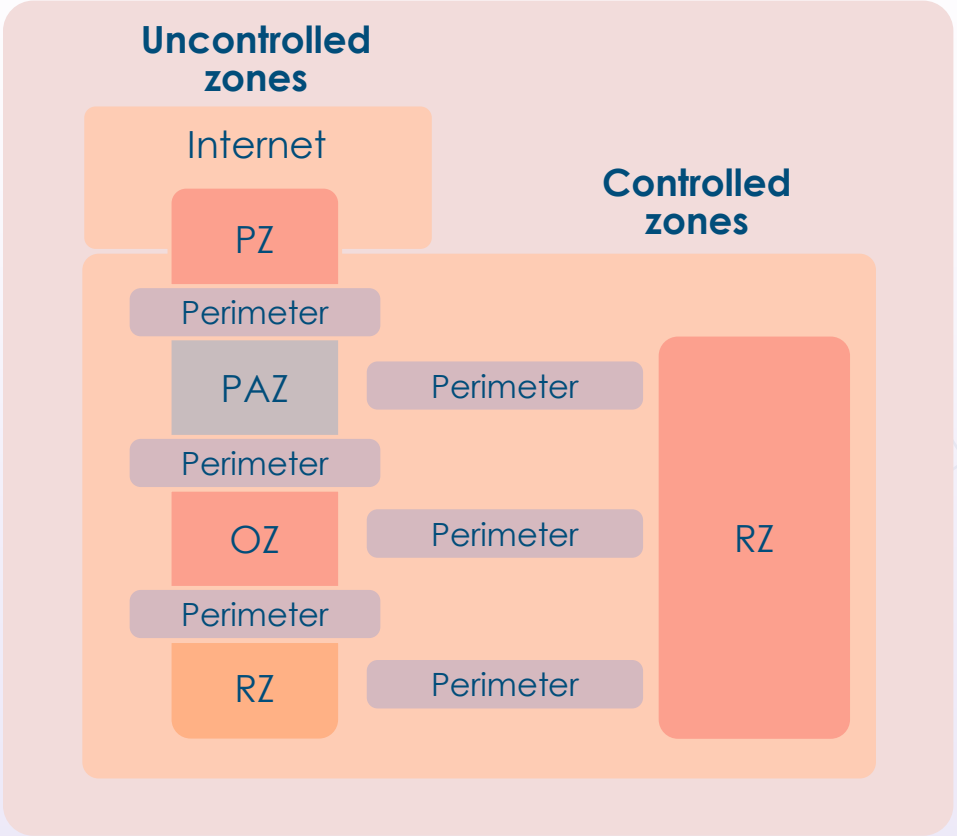
- Wired Ethernet
- Wired fiber optic
- Wired cable (DOCSIS)
- Wireless 802.11 (Wi-Fi)
- Wireless cellular
- Wireless satellite
- Wireless personal area network (PAN)
  - Bluetooth, infrared, Zigbee, RFID, NFC

Zones and VLANs



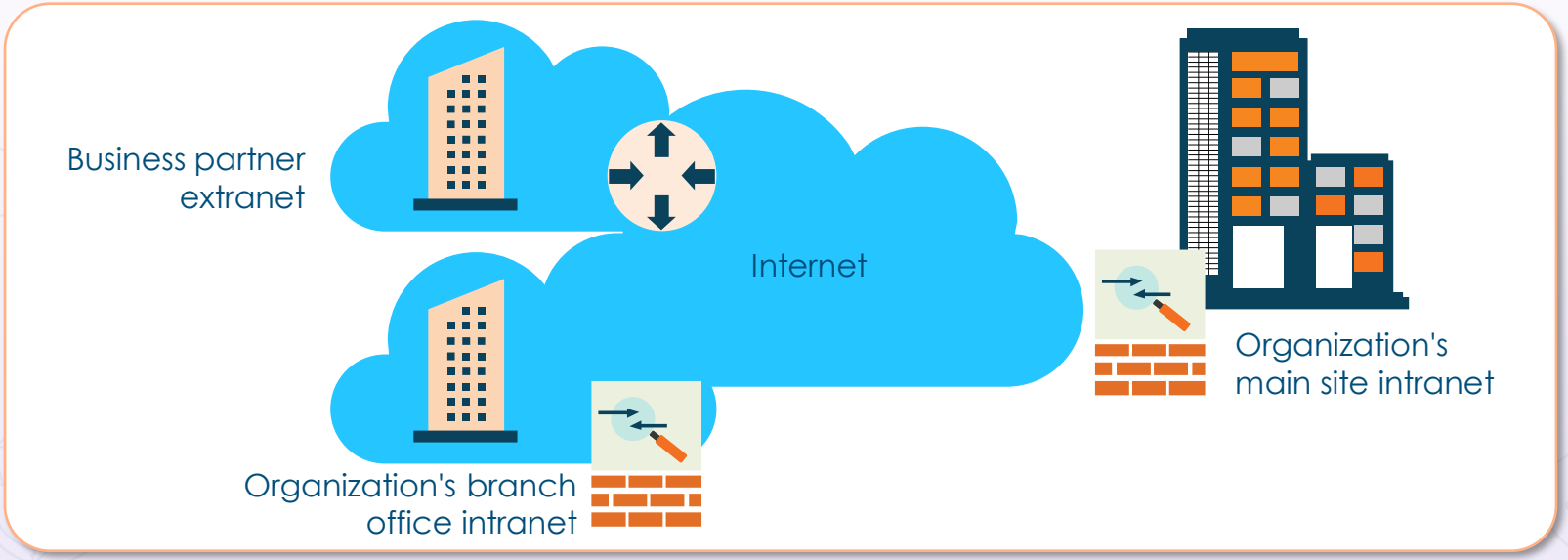
Zoning and Segmentation

- Zoning is used to mitigate the risk of an open network by segmenting infrastructure services
- Zoning is a logical design approach used to control and restrict access
- Each zone has fundamental characteristics, defined by the security assigned to it

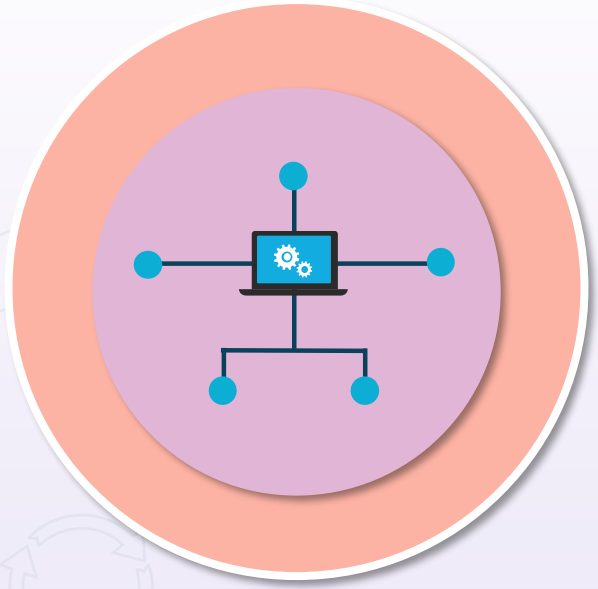


Extranet

- An extranet (e.g., PartnerNet) is a network with resources under the control of another organization that your organization needs access to
- It could be a strategic partner or a customer with a connection agreement

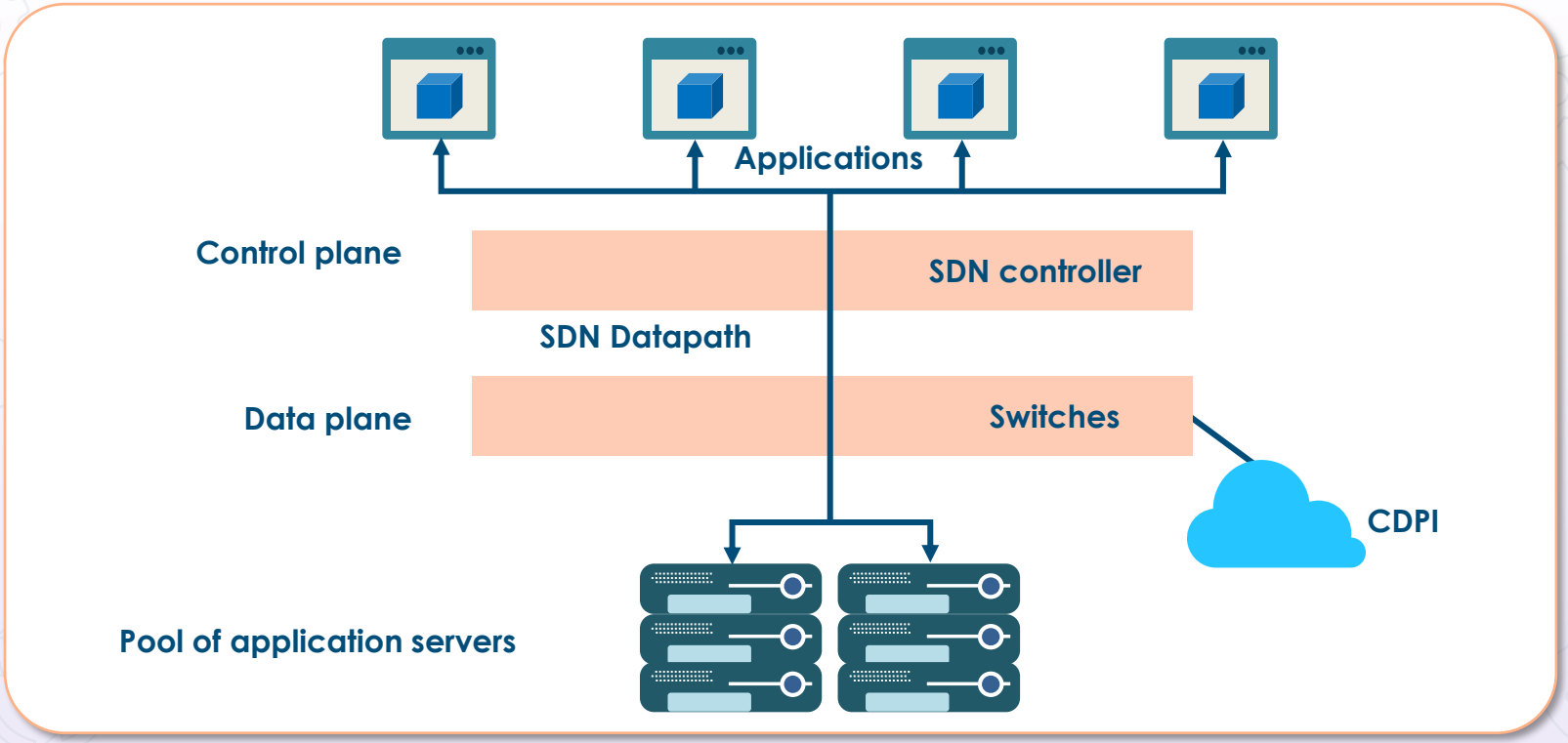


Software-defined Networking (SDN)

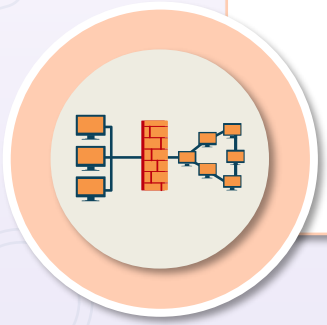


- Software-defined networking (SDN) virtualizes network functionality by separating the control and data planes and implementing the network intelligence in software – typically hypervisor or proprietary server solutions
- SDN can be applied to the existing physical infrastructure or as part of an evolving virtualization of switches, multilayer switches, routers, firewalls, and more

Software-defined Networking

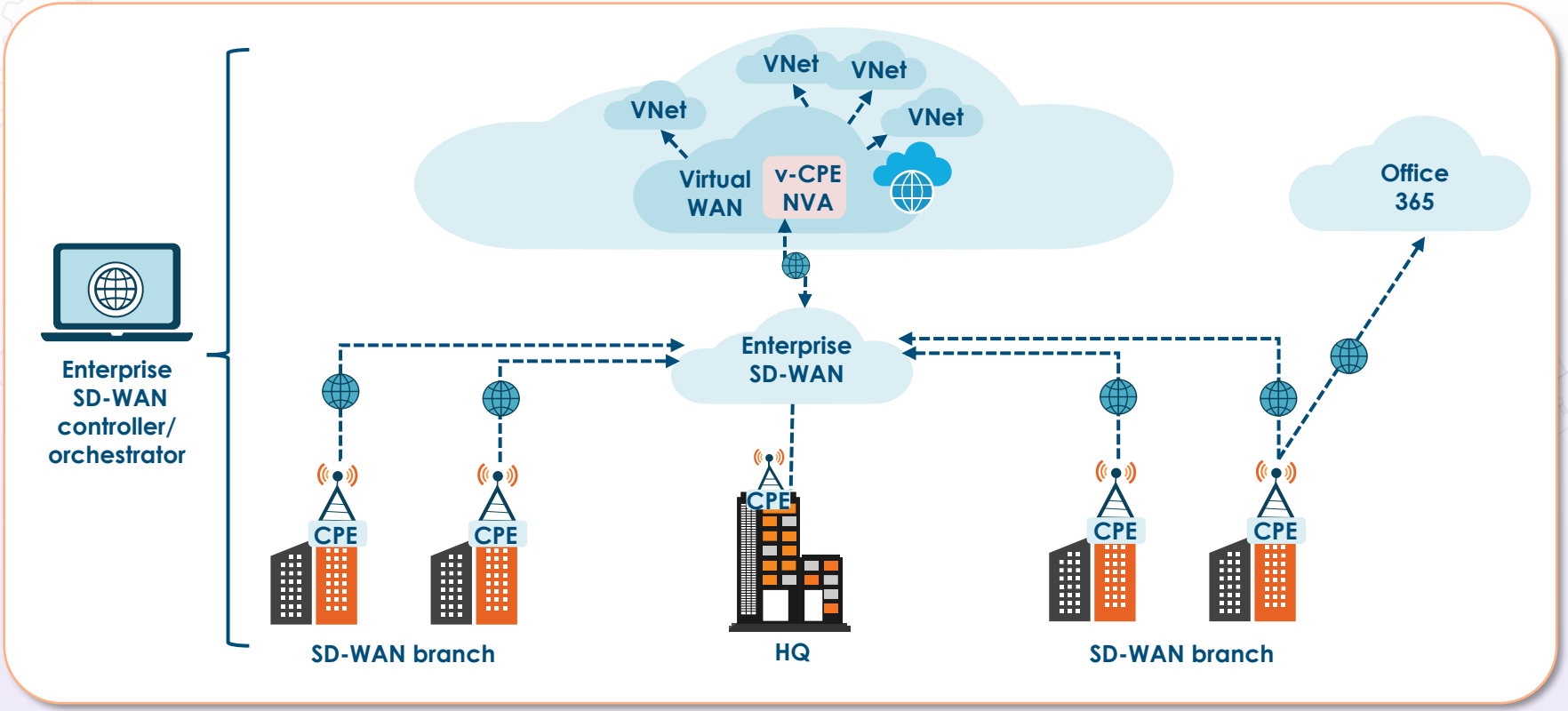


Software-defined Wide Area Network (SD-WAN)

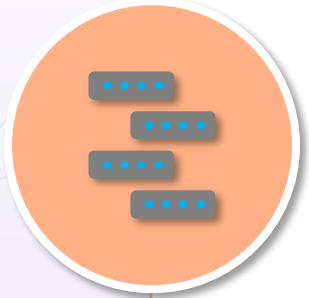


- SD-WAN is an SDN approach that raises network traffic management away from the hardware and premises to next-generation software in the cloud for superior agility, control, and visibility
- Incorporates a centralized control function with user-defined application and routing policies to deliver highly secure, robust, application-aware network traffic management

Microsoft SD-WAN Solution

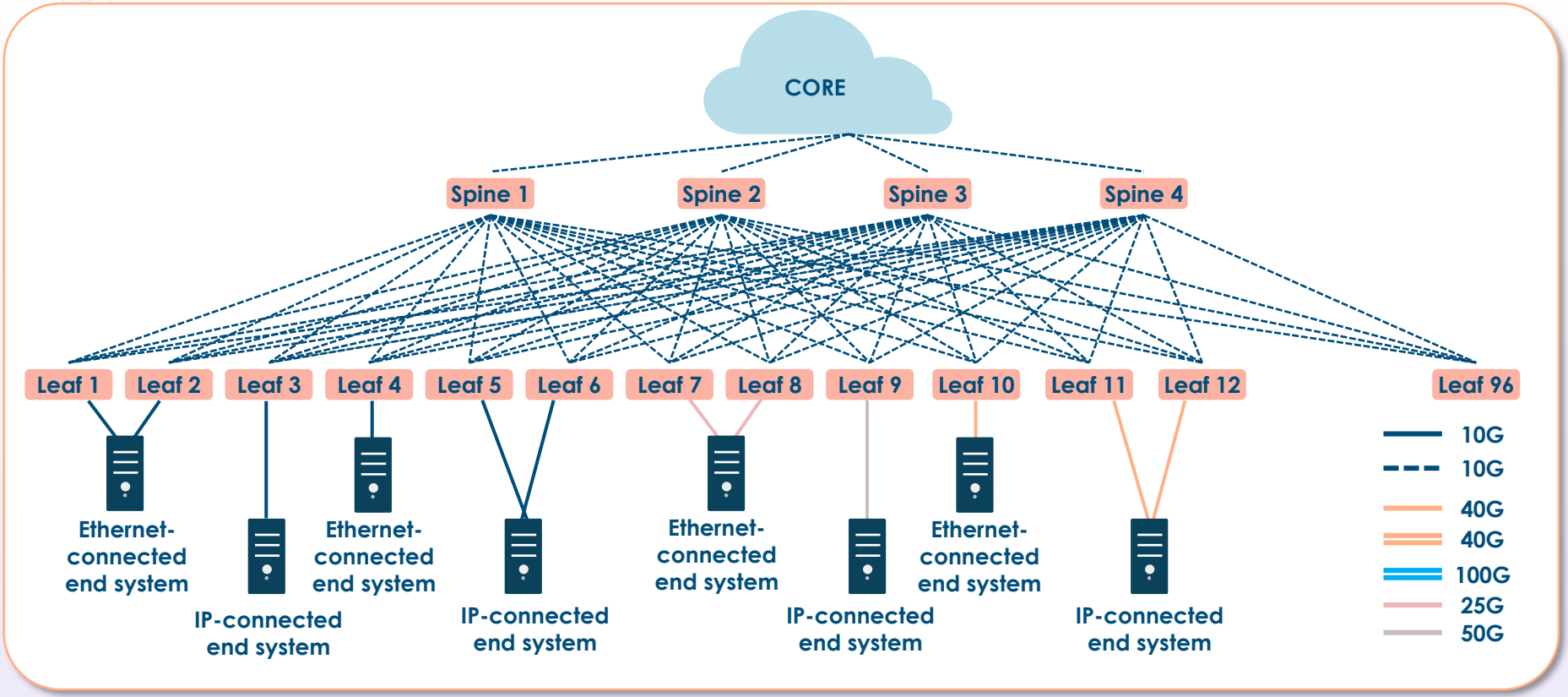


Virtual eXtensible Local Area Network (VXLAN)



- VXLAN solutions from a variety of vendors decouple the physical hardware from the network map in order to support virtualization
- This uncoupling allows the data center network to be deployed programmatically
- It allows both Layer 2 and Layer 3 transport between VMs and bare-metal servers
- Has a much larger scale than traditional VLANs

VXLAN Architecture



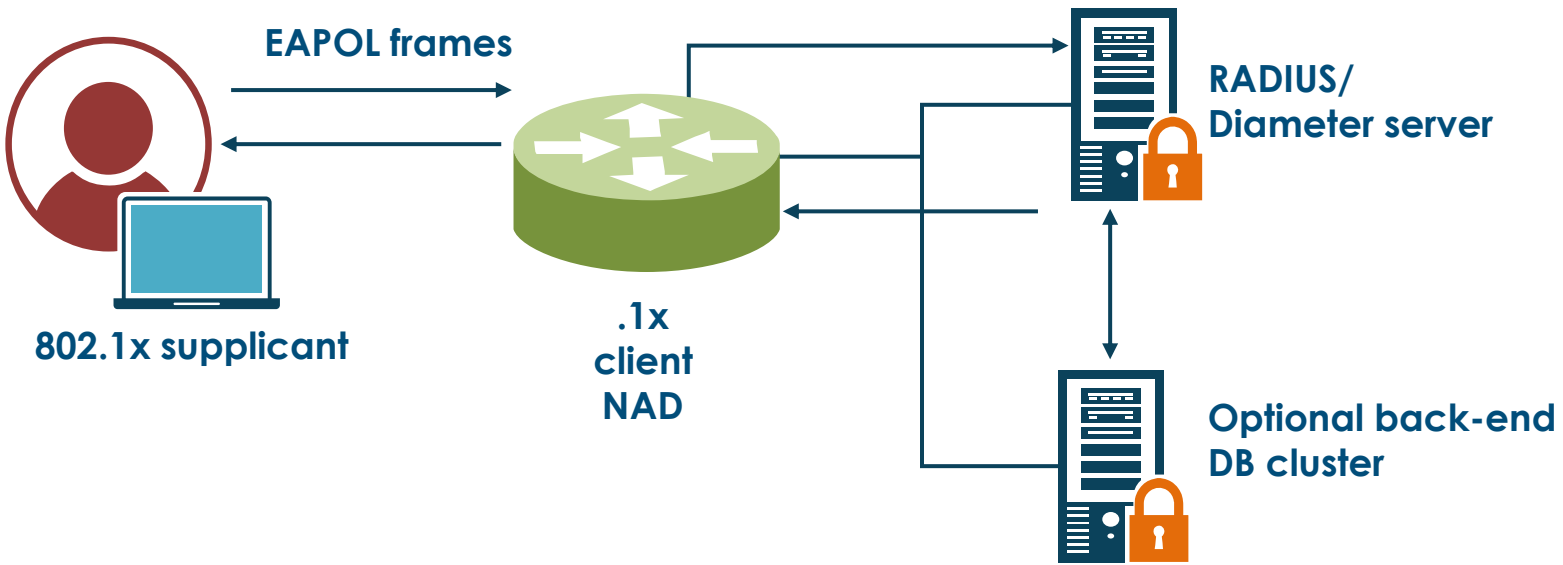
Remote Authentication Dial-In User Service (RADIUS)

- RADIUS is a popular and widely deployed IETF-based client-server protocol and software that enables a remote access server (RAS) to communicate with a central server to authenticate dial-in users and authorize their access to systems
- Transactions use a shared secret between the client and the RADIUS server for authentication
- The shared secrets are never sent over the network and only the password is encrypted

RADIUS

- Officially uses UDP ports 1812 (authentication) and 1813 (accounting)
- Earlier implementations used UDP ports 1645 and 1646
- Often preferred for its robust integrated accounting feature set
- Used with IEEE 802.1X (PNAC)
- The next generation is called Diameter

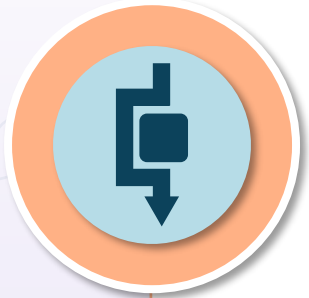
802.1X (PNAC)


EAPOL frames
802.1x supplicant
.1x
client
NAD
RADIUS/
Diameter server
Optional back-end
DB cluster

802.11 EAP Variants

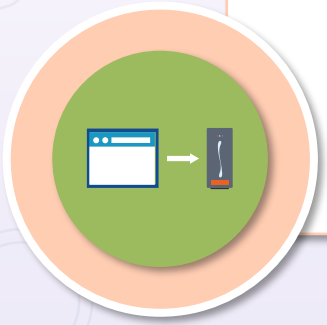
802.1x EAP types feature/benefit	MD5 … Message digest 5	TLS … Transport Layer security	TTLS … Tunneled transport Layer security	PEAP … Protected extensible authentication protocol	FAST … Flexible authentication via secure tunneling
Client-side certificate required	No	Yes	No	No	No (PAC)
Server-side certificate required	No	Yes	Yes	Yes	No (PAC)
Key management	No	Yes	Yes	Yes	Yes
Rogue AP detection	No	No	No	No	Yes
Provider	MS	MS	Funk	MS	Cisco
Authentication attributes	One-way	Mutual	Mutual	Mutual	Mutual
Deployment difficulty	Easy	Difficult (due to client certificate deployment)	Moderate	Moderate	Moderate
Wi-Fi security	Poor	Very high	High	High	High

Terminal Access Controller Access-Control System Plus (TACACS+)



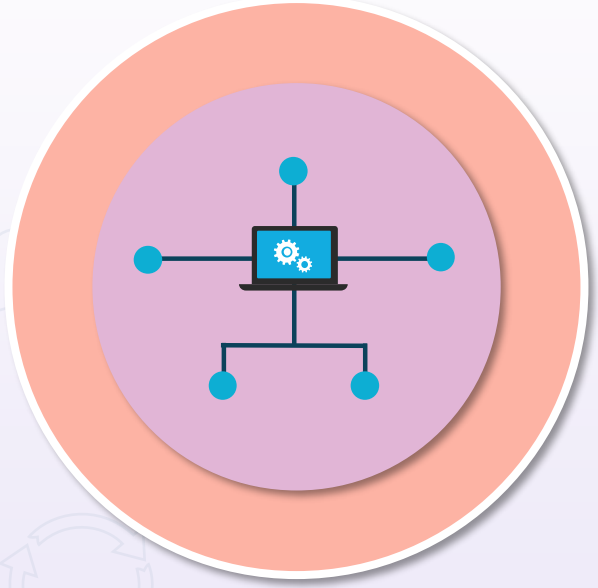
- Terminal Access Controller Access-Control System Plus (TACACS+) was developed by Cisco
- Now a standard client and server protocol for AAA services
- Dynamic authorization is on a per-user or per-group basis
- Offers separate and independent modular authentication, authorization, and accounting abilities
- Each service could be tied into its own database to take advantage of other services available on that server
- Commonly used with Cisco ACS 5.X and ISE 2.X for centralized administrative access control management for the enterprise

TACACS+



- It uses a two-factor password authentication mechanism
- The user can change the password
- It uses TCP port 49 and encrypts the entire payload
- TACACS+ services are in the public domain and can be bundled in the OS of network devices
- Routers can leverage per-command authorization for centralized management of privilege levels

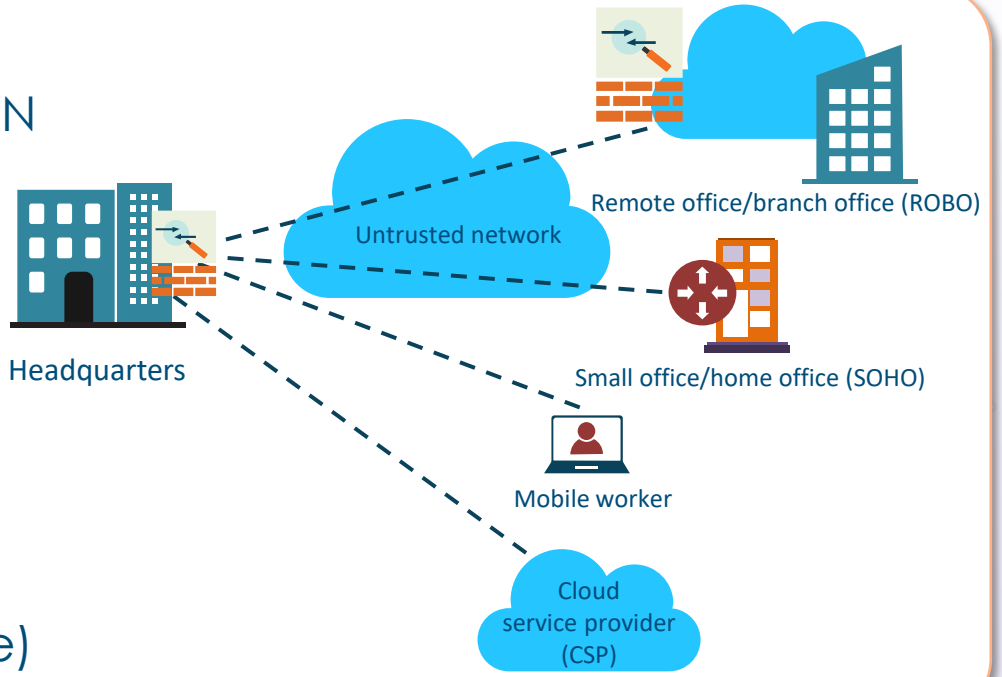
Virtual Private Networks (VPNs)



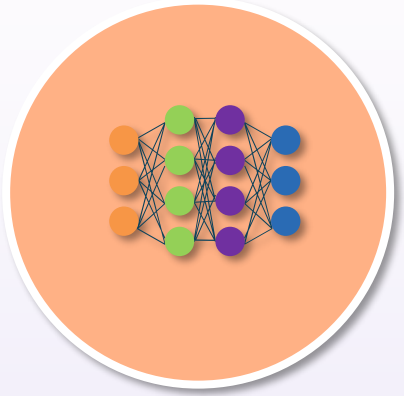
- VPN gateways are dedicated termination points (concentrators) for site-to-site and remote-access VPNs
- They can support IPsec IKEv1, IKEv2, and SSL/TLS protocol suites
- VPNs can be server or appliance-based and physical or virtual
- Routers and firewalls are common VPN gateways

VPN Connections

- Site-to-site or remote access VPN
  - Client or clientless
- IPsec IKEv1 or IKEv2
  - Tunnel mode or transport mode
  - AH or ESP
- Split tunnel vs. full tunnel
- Always-on VPN
- IPv4 and/or IPv6
- CSP-based (AWS, GCP, or Azure)

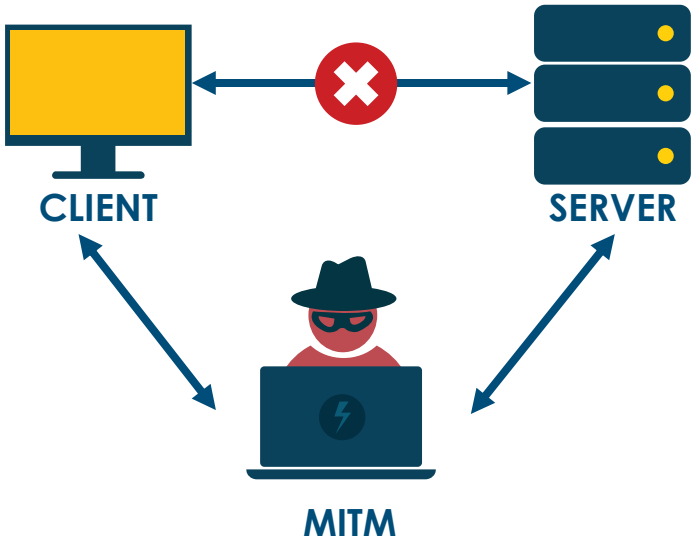


Systems Security Certified Practitioner (SSCP)



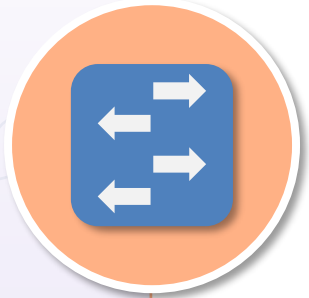
Network Attacks and Countermeasures

Man-in-the-Middle (MITM) Attacks



- A man-in-the-middle can be good (proxy, ALG, translators), or it can be dangerous (Proxy ARP, DHCP spoofing, poisoning)
- A system with the ability to view the communication between two (or more) hosts (frames, packets) injects itself in the path between the host systems
- They are complex attacks that can be simplex or duplex at different layers of the OSI model

ARP (Address Resolution Protocol) Poisoning



- A form of man-in-the-middle attack that exploits ARP
- Malicious hosts inject false frames in order to corrupt (poison) the ARP cache buffers on endpoints, switches, servers, firewalls, and routers
- Exploit kits have several scripts, modules, and tools to compromise the ARP protocol
- Only works in IPv4 networks – not IPv6
- It can be mitigated with port security, snooping binding databases on switches, and MACsec implementation 802.1AE

Domain Hijacking DNS Attack

- Domain hijacking or clickjacking is also called user interface redress attack, UI redress attack, and UI redressing
- Hacker uses several transparent layers to trick users into clicking on a button (or link) on another web page when they were trying to click on the top-level web page
- Attacker hijacks clicks meant for their page and routes them to another page, often controlled by another domain or application
- Keystrokes can also be hijacked with skillfully constructed iframes, CSS, and text boxes
- This can also be done through URL redirection

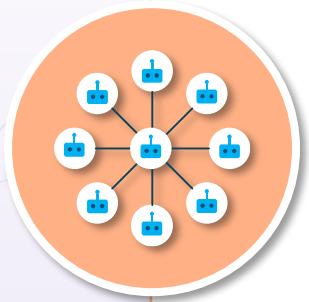
DNS Poisoning

- DNS poisoning is when an attacker changes the name resolution information that should be in a DNS server's cache so that client systems are redirected to incorrect web sites
- This is accomplished by name server misconfiguration, improper software design, and malicious exploits designed for the DNS system

DNS Poisoning

- When a DNS cache is poisoned, it is often changed in order to redirect requests for a domain to a different address and web site
- This other site could be performing phishing, pharming, or some other malicious activity

Denial of Service (DoS) Attacks



- Denial of service attacks are some of the oldest exploits that leverage inherent weaknesses in the TCP/IP stack
- DoS attacks try to consume a system's (or network's) critical resources, such as disk space, CPU cycles, memory (switch CAM tables), bandwidth, input queues, DHCP (Dynamic Host Configuration Protocol) leases, etc.
- DoS attacks are still common and a major risk because they can effectively interrupt business operations
- They are relatively simple to conduct with script kiddie tools

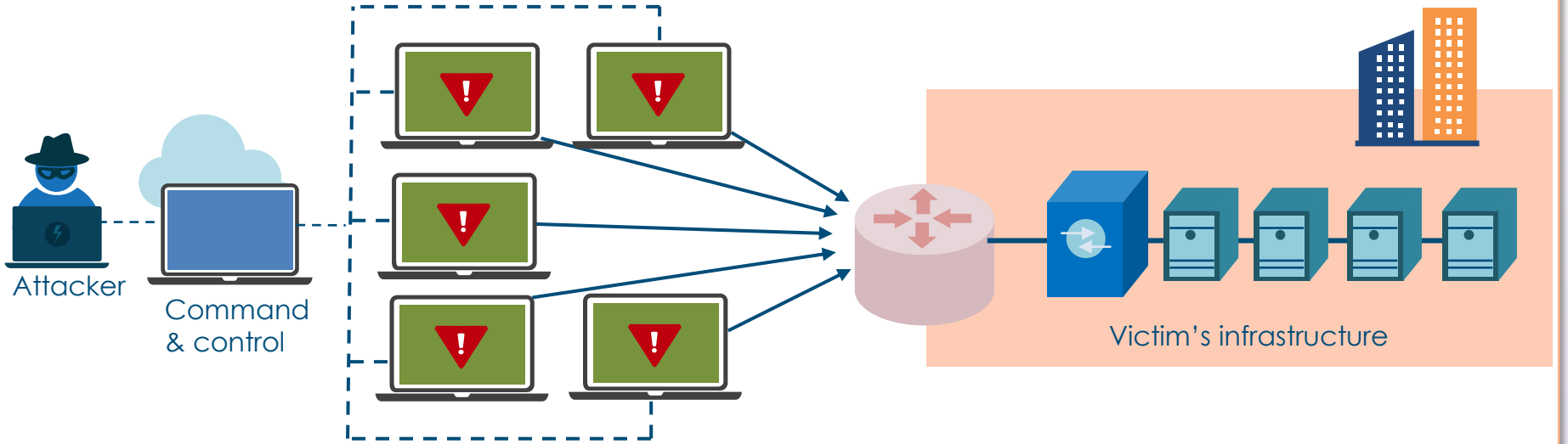
Botnets

- A botnet consists of a group of systems loaded with computer robot code (or bots)
- A command and control (C&C) server control mechanism directs the zombie computers remotely, often by using Internet Relay Chat (IRC), peer-to-peer, or even Twitter

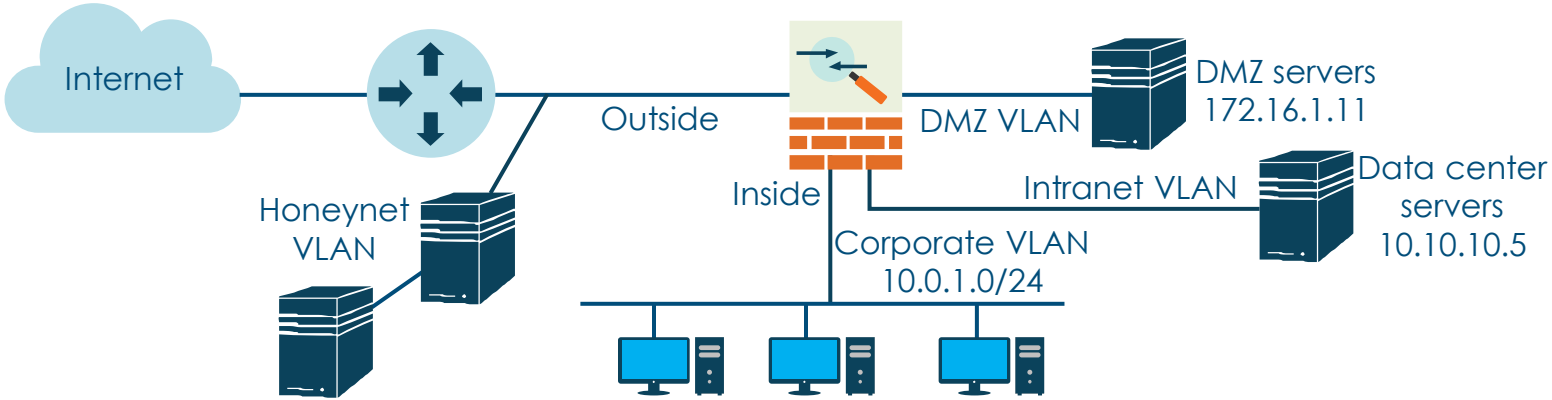
Botnets

- Malicious "zombiefied" hosts can also combine to flood a victim with many attack packets simultaneously from potentially thousands of sources
- This is a distributed DoS (DDoS) attack, which is often sourced from networks of compromised systems called botnets

Botnets



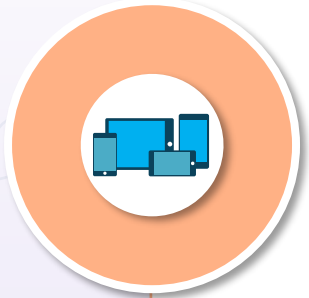
Network Device Placement



Access Control Lists

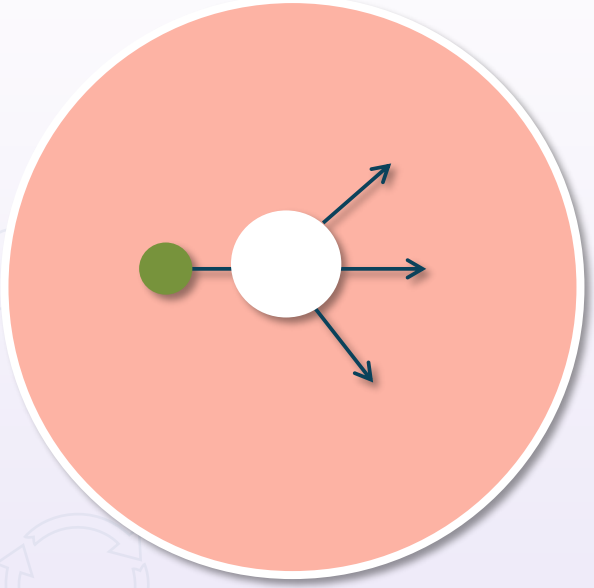
In this demo…

Secure Device Management



- Use secure management protocols, such as SSH2 and TLS 1.2 or 1.3
- Utilize mediated access with bastion services or hardened jump hosts
- For privileged access, use multi-factor authentication and strong identity management services
- Authorization is best centralized with services such as LDAPS, TACACS+, RADIUS, or Diameter
- Use separation of duties, least privilege, and dual operator whenever possible

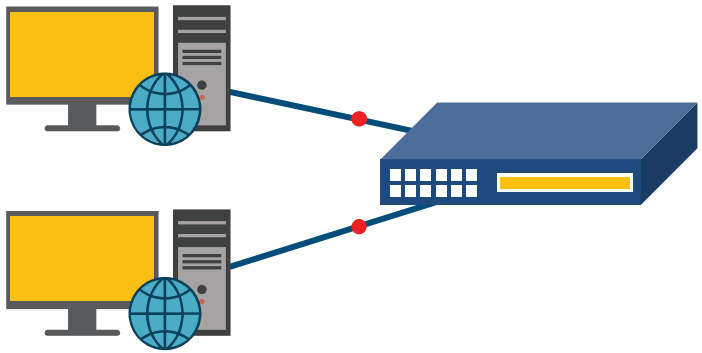
Load Balancing



- Devices are popular due to the usage of intensive applications and services
- They can optimize application availability and performance
- They distribute TCP, UDP (User Datagram Protocol), HTTP, and TLS traffic across multiple servers in order to efficiently allocate resources and offer failover solutions

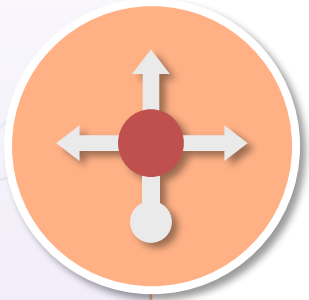
Load Balancing

- Dedicated load balancing appliances and modules have become a standard component in the physical and virtual network
- All the major network equipment vendors offer load balancing solutions to basically "put traffic in its place"
- These systems can optimize application availability and performance, distribute traffic across multiple servers, and offer failover solutions



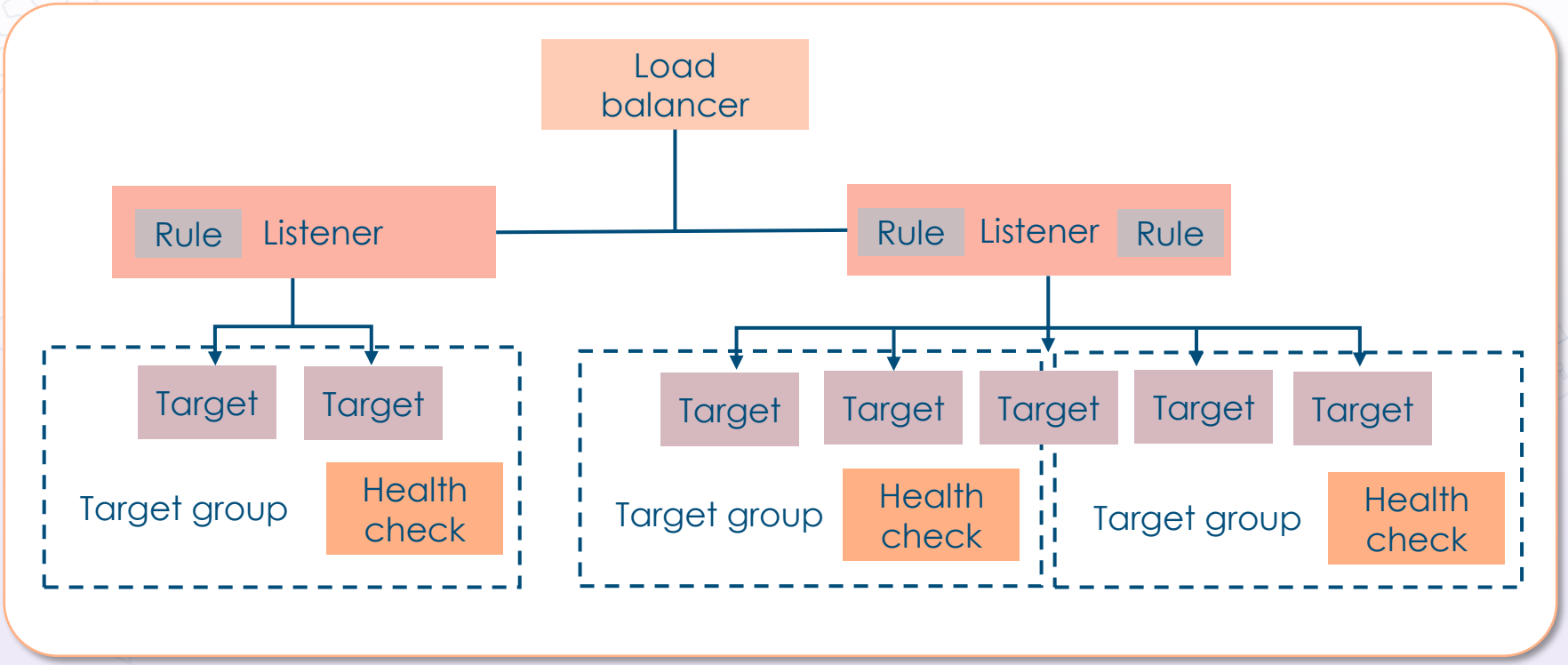
Load balancer

Load Balancing at Cloud Service Providers

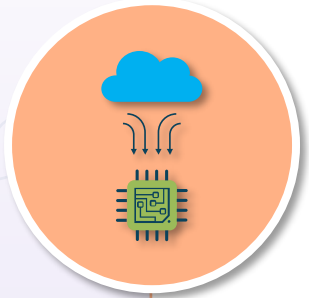


- Network or application load balancing
- Often represents virtual network to the public based on IP address or public domain name
- Performs health checks on back-end instances and containers
- Produces flow logs for other threat management services
- Runs the TLS listener to decrypt traffic
- Can also have layer 3/4 and web application firewall (web ACL – web access control list)

Load Balancing at Cloud Service Providers

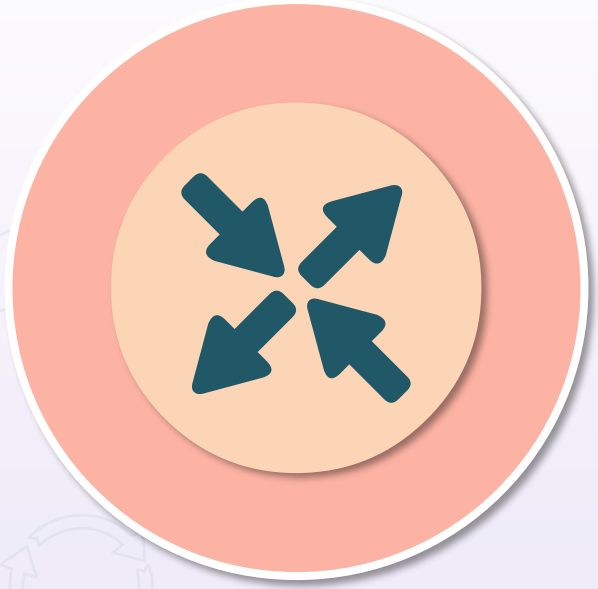


Content Distribution (Delivery) Network (CDN)



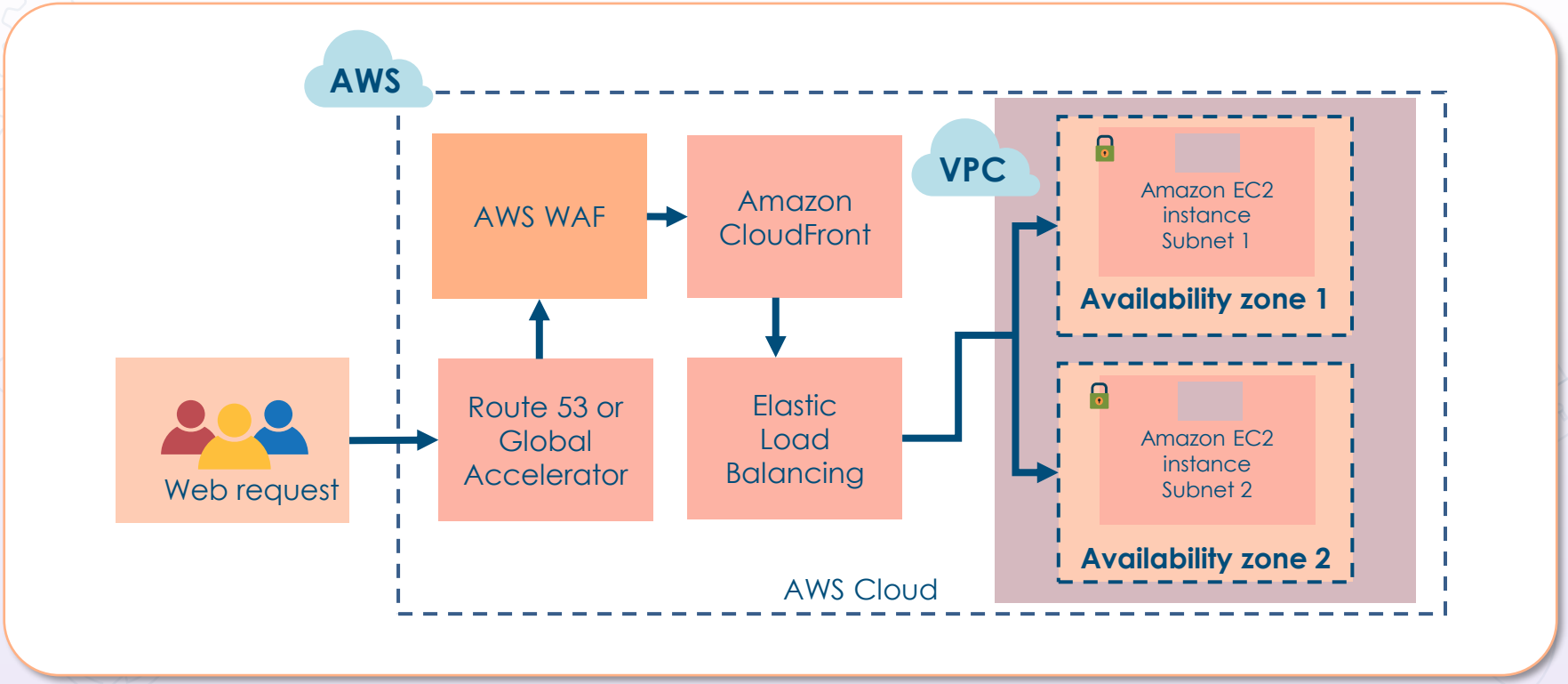
- A CDN is a highly-distributed platform of servers that reduces delays in loading web page content
- It reduces the physical distance between the server and the users around the world
- Without a CDN, origin servers would have to respond to every end-user request, resulting in substantial traffic to the origin and subsequent load
- By responding to end-user requests using modern edge computing and elastic caching, the CDN offloads traffic from content servers to metro edge locations
- Examples are Cloudflare, Akamai, Fastly, and AWS CloudFront

AWS CloudFront



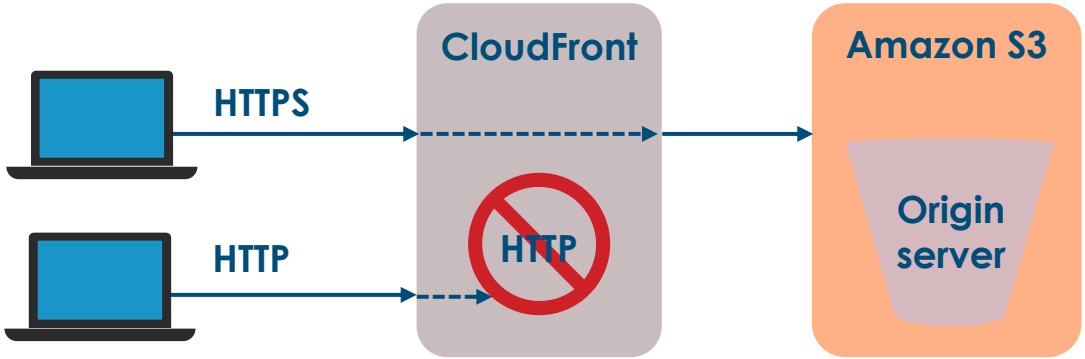
- Amazon CloudFront is a fast CDN service, like Akamai, that securely delivers data, videos, applications, and APIs to customers at metro edge computing locations with low-latency, high-transfer speeds within a developer-friendly environment
- CloudFront is often integrated with AWS Redis ElastiCache at global provider partner locations and various service endpoints
- Functions seamlessly with Route 53, S3 object storage, Elastic Load Balancing, EC2 instances, AWS WAF (web application firewall), and AWS Shield for DDoS protection

CloudFront at Amazon Web Services

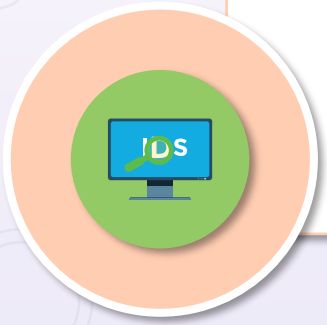


AWS CloudFront Security

- High-level data center physical security is in place
- Uses TLSv1.1 and TLSv1.2 protocols for HTTPS connections between CloudFront and the custom origin web server
- Cipher suites use the ECDHE protocol on all connections
- Private content feature controls who can download content from CloudFront
- Origin access identities can control access to original copies of objects



Intrusion Detection and Prevention

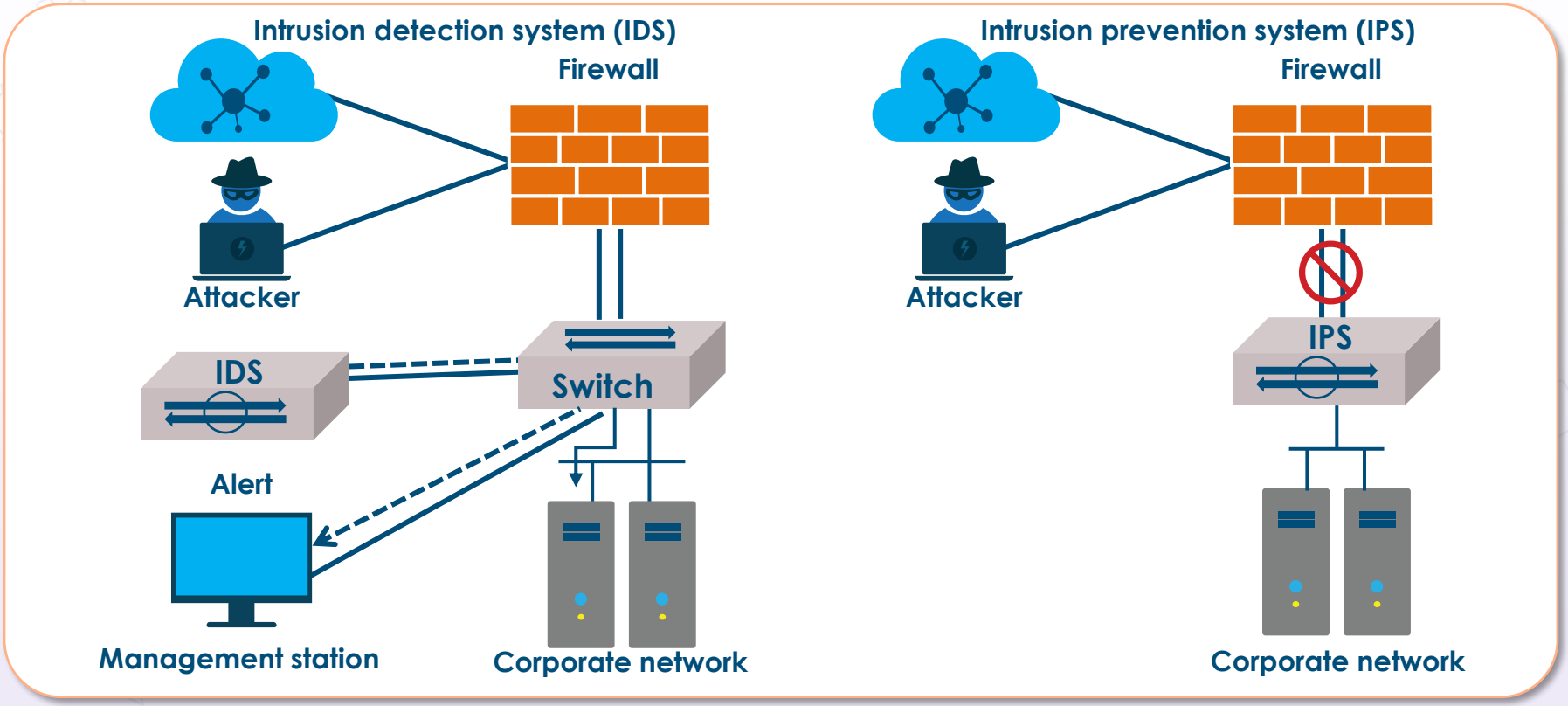


- A combination of hardware and/or software to get visibility into existing attacks and malware on the network or individual hosts
- Snort intrusion detection system (IDS) running on Unix machines was the original intrusion detection daemon and has evolved into advanced next-generation solutions

Intrusion Prevention System (IPS)

- Inline IPS or monitor (passive mode)
- In-band vs. OOB (out-of-band)
- Signature-based
- Anomaly-based
- Heuristic/behavioral-based (ML)
- Cloud-based (NGIPS – next-gen intrusion prevention system)

IDS vs. IPS


Intrusion detection system (IDS)
Firewall
Attacker
IDS
Switch
Alert
Management station
Corporate network
Intrusion prevention system (IPS)
Firewall
Attacker
IPS
Corporate network

IPS Actions

- Alerts and alarms
- Verbose dumps
- TCP resets
- Drop packets or addresses
- Blocking (shun) on firewalls and routers
- SNMP (Simple Network Management Protocol) traps
- Logging to syslog and SIEM systems
- Flows to NetFlow collectors

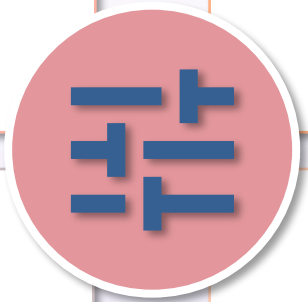
IPS Tuning

True positive

True (accurate) + positive (action taken)

False positive

False (error) + positive (action taken)



True negative

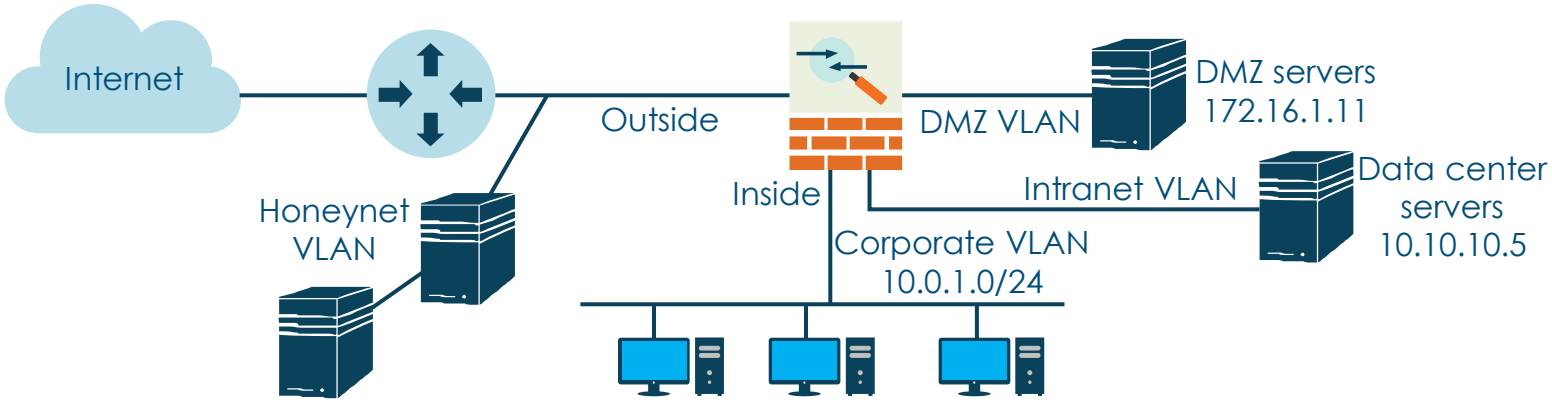
True (accurate) + negative (action not taken)

False negative

False (error) + negative (action not taken

Honeypots and Honeynets

- Honeypots and honeynets are isolated systems, sites, and services with data that appears to be valuable to an attacker
  - Entice potential malicious users to connect (internal or external)
  - Track and log all traffic to and from the honeypot
  - Run IDS services and other next-generation cloud-based analysis
  - Perform active defense procedures

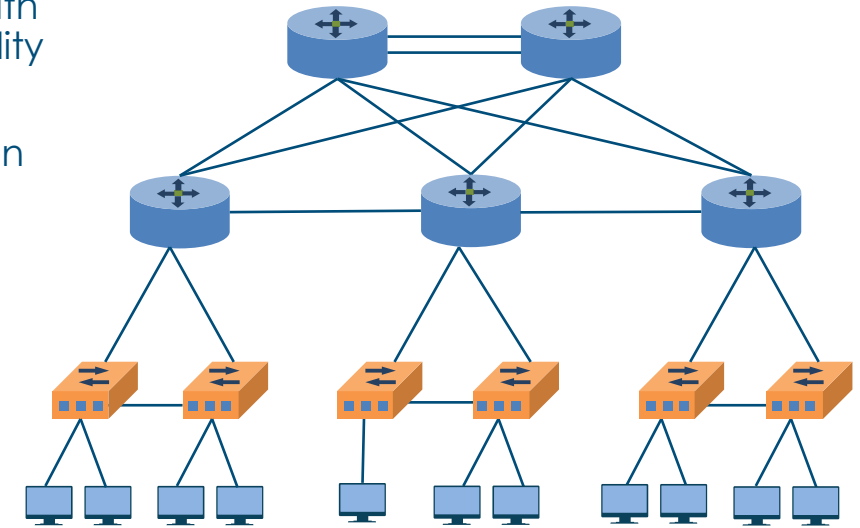


Active Defense

- DECEPTION
- ATTRIBUTION
- COUNTERATTACK

Switch Port Security

- Switches function at layers 2-4 with extensive capabilities and flexibility
- Access switches and aggregate (multilayer) switches are common
- Can be physical or virtual (SDN)
- Switch port security should be a base configuration for MAC filtering
- Infrastructure as code can contribute to secure switch configuration to reduce configuration errors



Switch Security

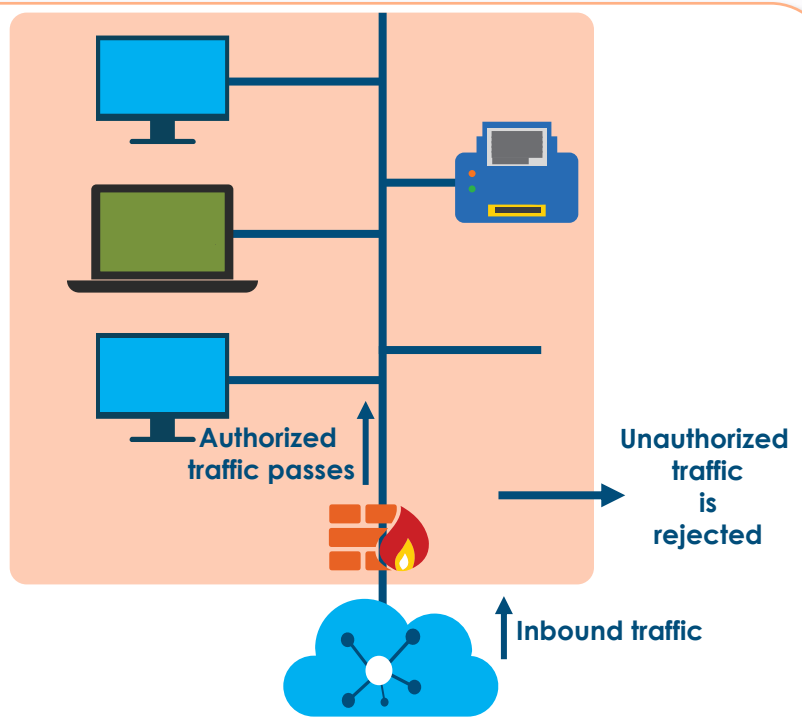
- Loop prevention, flood guard with BPDU (Bridge Protocol Data Unit), and root guard configurations
- DHCP (Dynamic Host Configuration Protocol) snooping for Dynamic ARP inspection and IP Source Guard
- VLANs and PVLANs help to enforce a layer 2 trust model and compartmentalization
- Protect any dynamic trunking protocol, like VTP (VLAN Trunk Protocol)
- 802.1X PNAC offers EAP-TLS (Extensible Authentication Protocol-TLS), PEAP (Protected EAP), and EAP-FAST (EAP-Flexible Authentication via Secure Tunneling)
- MACsec offers AES-GCM-128/256 with GMAC (Galois Message Authentication Code)

Secure Routers

- Network Address Translation (NAT)
- Infrastructure access control lists (ACLs)
- Unicast and Multicast Reverse Path Forwarding
- Integrated and modular L2-7 next-generation firewall and intrusion detection/prevention systems (IDS/IPS)
- VPN gateways for TLS and IPsec
- URL filtering and caching
- Integration with various cloud security services (web, email, DLP, anti-malware)
- Coordinate with managed security service providers (MSSPs)

Next-generation Firewalls

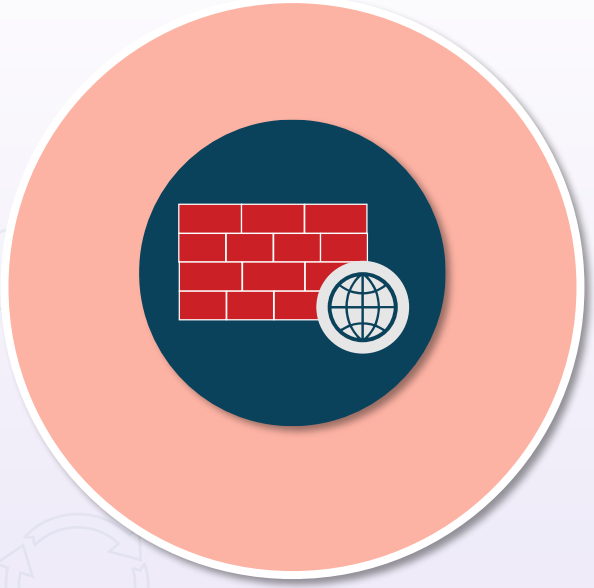
- Layer 5-7 policies (DPI and AVC)
- Authentication proxy (interactive or transparent)
- Identity services (ABAC)
- Integrated IDS/IPS
- Unified threat management (UTM)
  - Content security and advanced malware protection with cloud services
- URL filtering
- Botnet filtering
- Vendor cloud correlation and reputation filtering



Web Application Firewall (WAF)

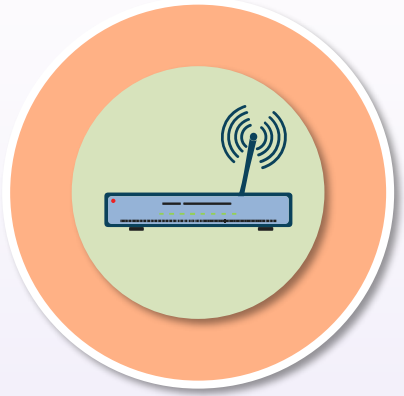
- An appliance, server plugin, or CSP service that applies a set of rules to an HTTP/S connection
- Web ACLs (access control lists) filter for common attacks, such as
  - cross-site scripting (XSS)
  - SQL injection
  - cross-site request forgery (CSRF)
  - buffer overflows
  - DDoS and botnets, and
  - custom web ACL rules

Common WAF Solutions



- Akamai
- Fortinet
- Cloudflare
- Cisco Cloud Web Security
- StackPath
- AWS WAF on CloudFront, API Gateway, and Application Load Balancers in ELB (Elastic Load Balancing)

Systems Security Certified Practitioner (SSCP)

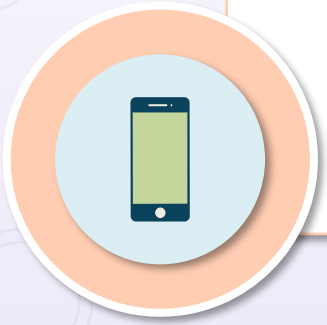


Secure wireless communication

Wi-Fi Technology

Release Date	Standard	Frequency Band	Bandwidth	Transmission Scheme	Max Modulation	MIMO	Max Data Rate
1997	802.11	2.4 GHz	20 MHz	DSSS, FHSS	QPSK	N/A	2 Mb/s
1999	802.11b	2.4 GHz	20 MHz	DSSS	QPSK	N/A	11 Mb/s
1999	802.11a	5 GHz	20 MHz	OFDM	64QAM	N/A	54 Mb/s
2003	802.11g	2.4 GHz	20 MHz	DSSS, FHSS	64QAM	N/A	54 Mb/s
2009	802.11n	2.4 GHz 5 GHz	20 MHz 40 MHz	OFDM	64QAM	4X4	600 Mb/s
2013	802.11ac	5 GHz	20 MHz 40 MHz 80 MHz 160 MHz	OFDM	256QAM	8X8	6.93 Gb/s
2018	802.11ad	60 GHz	2160 MHz	SC,OFDM	256QAM	Beamforming	6.93 Gb/s

Cellular Technologies

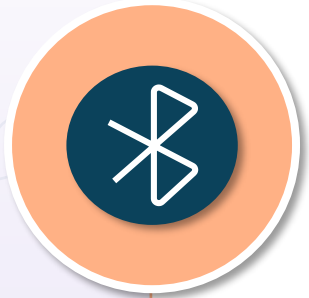


- Multiple access technology where multiple voice or data connections are placed into a single radio channel
- Involves having many small, inter-connected transmitters instead of one large one
- The major enhancements of 4G were mobile broadband Internet services offered to laptops, wireless modems, etc.

5G

- The fifth generation of wireless cellular mobile networking
- All 5G devices in a cell are linked to the Internet and telephone network by radio waves through a local antenna in the cell
- The goal is to deliver bandwidths up to 10 Gbps by using higher-frequency radio waves than current cellular networks

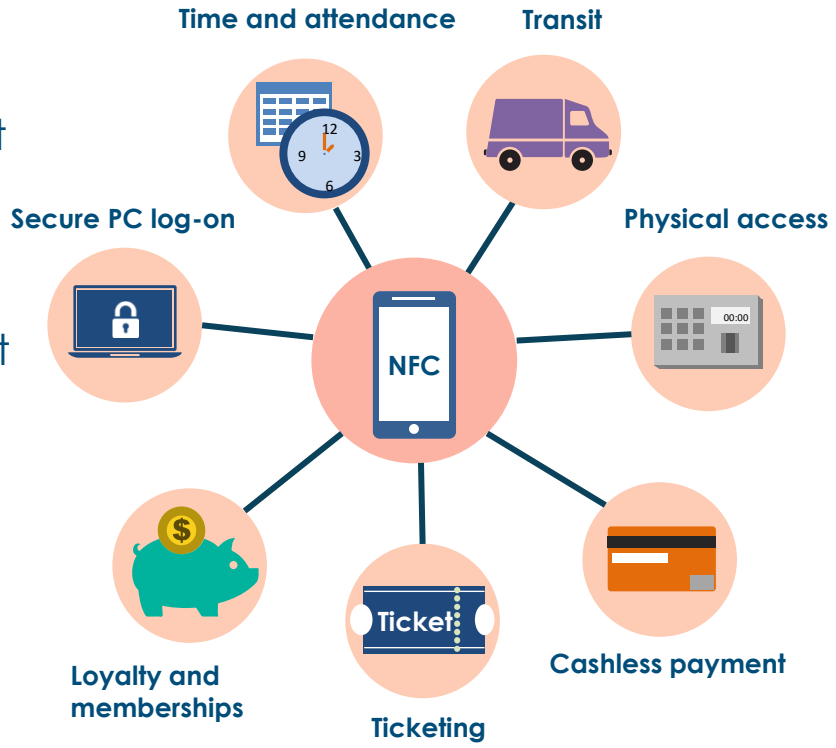
Bluetooth



- Method of creating personal area networks (PAN) with many applications
- Telephones, speakers, tablets, media players, robotics systems, handheld devices, laptops, console gaming equipment, high-definition headsets, modems, watches, and wearable tech
- Bluetooth is both an IEEE radio-frequency standard UHF in the 2.4 to 2.485 GHz ISM and an agreement protocol
- Bluetooth delivers confidentiality, authentication, and key generation with custom algorithms based on the SAFER+ block cipher

Radio Frequency Identification (RFID)

- Radio Frequency Identification (RFID) technology digitally encodes data in RFID tags or smart labels that are captured by a reader through radio waves
- The benefits of rapid and contactless payments and entry/exit without long waiting times are very tempting
- RFID is used for inventory management, asset and personnel tracking, access control, ID badges, supply chain management, and counterfeit prevention



Near Field Communication (NFC)

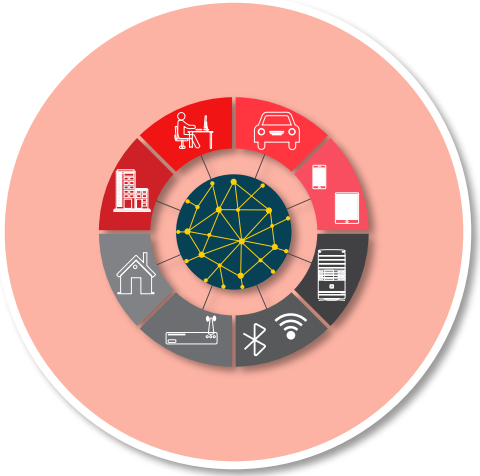
- ISO/IEC 14443 defines the ID cards used to store information, such as that found in NFC tags
- ISO/IEC 18000-3 specifies the RFID communication used by NFC devices
- 18000-3 is an international standard for all devices communicating wirelessly at the 13.56MHz frequency using Type A or Type B cards

Near Field Communication (NFC)

- Attendance tracking
- Asset identification and tracking
- Identity validation/access control
- Payments/transactions
- Wireless pairing

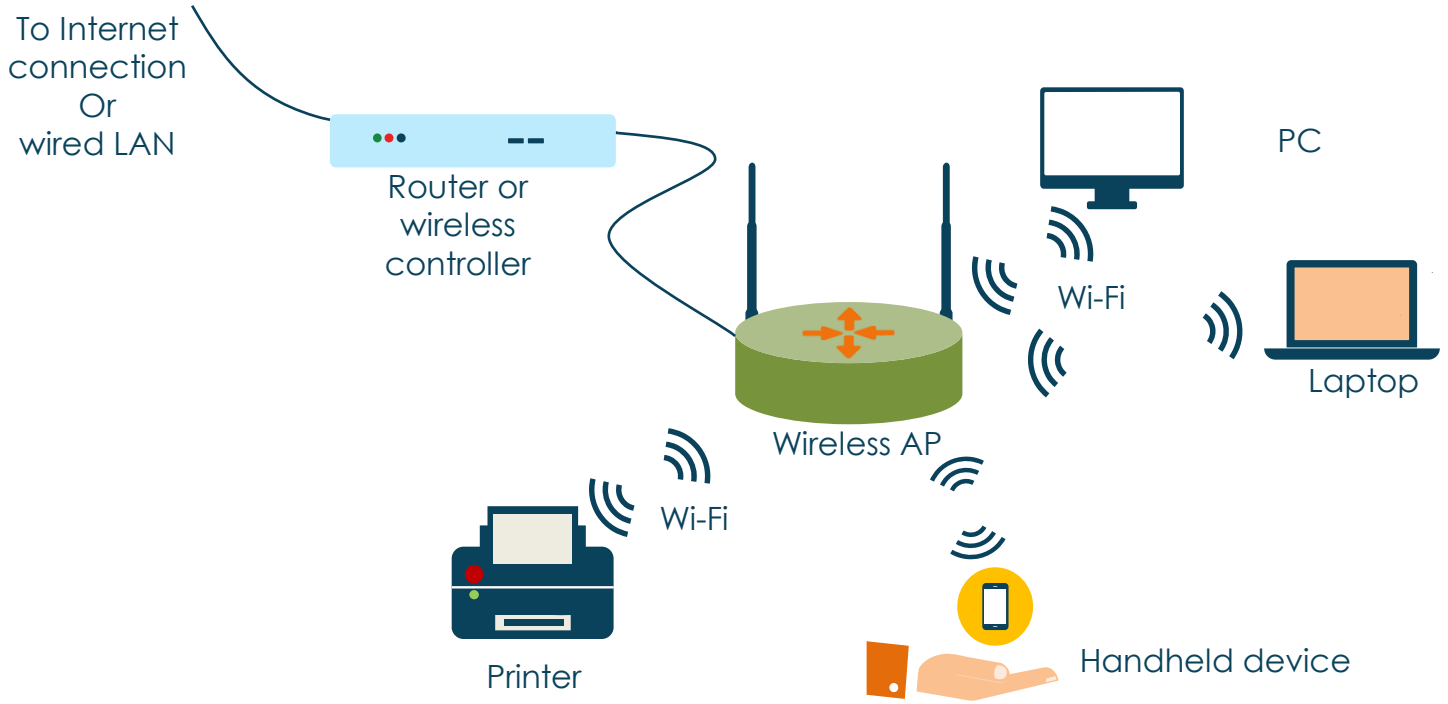
Zigbee (IEEE 802.15.4-2011)

PAN Technology

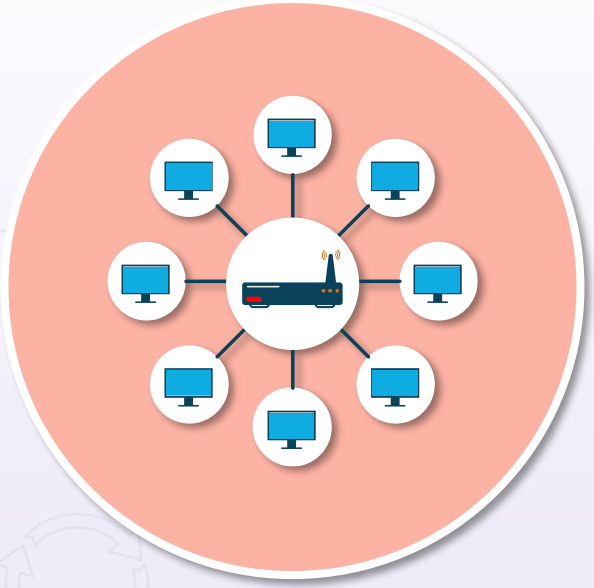


- Zigbee components can connect and communicate using the same IoT language
- Millions of Zigbee products are already deployed in smart homes and commercial buildings
- The network topology is a self-forming and self-healing mesh
- Ranges are up to 300+ meters (line of sight) and up to 75-100 meters indoors
- Supports AES-128 (Advanced Encryption Standard-128) at the network layer and application layer

Wireless LANs

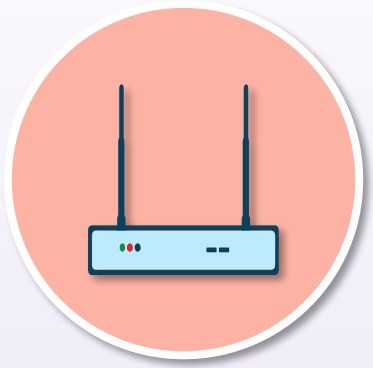


Distinctive Wi-Fi Characteristics



- Wireless LANs have many more planning considerations than wired LANs due to
  - wireless analysis
  - power output
  - RF channel selection
  - antenna strength and placement
  - interference, and
  - rogue station and WAP detection

Wireless Installation Considerations

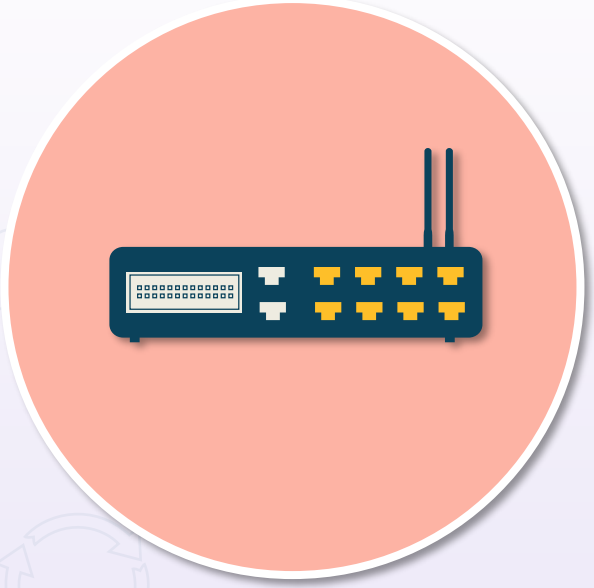


- Conducting site surveys with scanners and analyzers
- Generating visual heat maps and topologies
- Analyzing power outputs and interference
- Designing the channel overlays and DHCP roaming
- Strategically placing WAPs and internal/external antennas

Wireless Captive Portals

- Graphical web interfaces used in 802.1X to force EAP (Extensible Authentication Protocol) supplicants to upgrade, remediate, or get a certificate as part of Change of Authorization (CoA)
- Also used in hotels, airports, and other commercial scenarios to gather credentials or registration profiles before users can access a public Wi-Fi

Wireless LAN Controller (WLC) Security



- WLCs have a "session level" access control for management protocols and MFP features
  - All interactive management traffic to the controller will be done through HTTPS/SSH (encrypted)
- Control Plane Policing and CPU ACLs control the control plane and which devices can talk to the main controller processor
- Network IDS/IPS solutions
- SIEM and log event correlation
- Locate rogue radios and access points

Wi-Fi Protected Access (WPA)

- Wi-Fi is the commercial implementation of 802.11b/g/n/ac
- A temporary fix to WEP shortcomings (2003)
- Uses Temporal Key Integrity Protocol (TKIP) for encryption and integrity
- Supports PSK (pre-shared key) and enterprise authentication
- Deprecated (should not be used) but still available on products for SOHO deployments

WPA2

The de facto standard

- Replacement for WPA (2004)
- Devices require testing and certification from Wi-Fi Alliance (2006)
- Uses Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) for security
- Supports PSK and enterprise authentication
- Has been widely used for over 17 years and is still the most common solution

WPA2 Modes

Common solutions in today's wireless networks

WPA-PSK (Personal)

- Shared secret key is used
- Manually configured on devices and AP
- Local access controls
- AES used for encryption

WPA2-Enterprise (802.1X)

- Authentication server is required
- RADIUS used for authentication and key distribution
- Centralized access control with EAP (Extensible Authentication Protocol) variants
- AES used for encryption

CCMP

- Counter Mode Cipher Block Chaining Message Authentication Code Protocol
- Part of 802.11i wireless standard designed for WiMAX technology
- Algorithm based on AES
- Uses 128-bit keys and a 48-bit IV for replay attacks
- Includes a MAC for data integrity and origin authentication

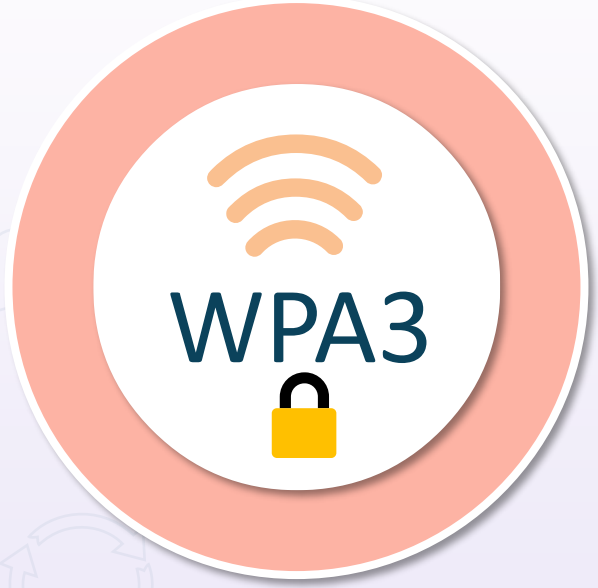
WPA3

- All WPA3 networks use the latest security methods, disallow outdated legacy protocols, and require the use of Protected Management Frames (PMF)
- PMF enhances privacy protections already in place for data frames with mechanisms to improve the resiliency of mission-critical networks

WPA3

- Authenticated encryption – GCMP-256
- Key derivation and confirmation – 384-bit HMAC with Secure Hash Algorithm (HMAC-SHA384)
- Key establishment and authentication – ECDH exchange and ECDSA using a 384-bit elliptic curve
- Robust management frame protection - 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)

WPA3 Personal



- Natural password selection – lets users choose passwords that are easier to remember
- Ease of use – provides enhanced protections with no change to the way users connect to a network
- Forward secrecy – protects data traffic even if a password is compromised after the data was transmitted

Simultaneous Authentication of Equals (SAE)

- Password-based authentication
- Password-authenticated key agreement
- Originally implemented as 802.11s
- WPA3 replaces PSK with SAE
- More secure initial key exchange

Dragonblood Attack

- Vulnerability in WPA3 discovered by the same researcher who discovered the KRACK attack on WPA2
- Exploit of the Dragonfly handshake protocol of WPA3
- If successful, an attacker within the range of a victim's network could recover the Wi-Fi password and infiltrate the target network
- Is, in fact, a collective of 5 attacks: 1 DoS, 2 downgrade attacks, and 2 side-channel information leaks

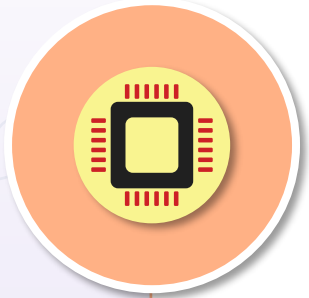
Extensible Authentication Protocols

- Extensible Authentication Protocol (EAP) is an authentication framework, not a specific authentication mechanism, that has evolved from Point-to-Point Protocol (PPP)
- It is frequently used in wireless networks and point-to-point connections. It provides some common functions and negotiation of authentication methods called EAP methods
- The EAP protocol can support multiple authentication mechanisms without having to pre-negotiate a particular one. There are currently about 40 different methods defined

802.1x EAP Variants

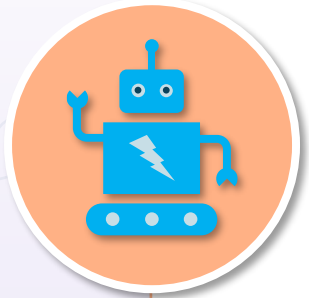
802.1x EAP types – Feature/benefit:	MD5 --- Message Digest 5	TLS --- Transport Layer Security	TTLS --- Tunneled Transport Layer Security	PEAP --- Protected Extensible Authentication Protocol	FAST --- Flexible Authentication via Secure Tunneling
Client-side certificate required	No	Yes	No	No	No (PAC)
Server-side certificate required	No	Yes	No	Yes	No (PAC)
WEP key management	No	Yes	Yes	Yes	Yes
Rogue AP detection	No	No	No	No	Yes
Provider	MS	MS	Funk	MS	Cisco
Authentication attributes	One-way	Mutual	Mutual	Mutual	Mutual
Deployment difficulty level	Easy	Difficult (due to client certificate deployment)	Moderate	Moderate	Moderate
Wi-Fi security	Poor	Very high	High	High	High

IoT and Embedded System Challenges



- Complete embedded source code is often not available
- Many of the device drivers and other components are simply binary sites with no source code at all
- Even if a patch is available, it is rarely applied in a consistent manner
- Hundreds of millions of devices are sitting on the Internet, unpatched and unsecured, for the last ten years or so

Raspberry Pi

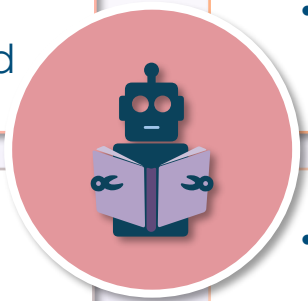


- Sequence of small, single-board computers developed by the UK Raspberry Pi Foundation
- Originally designed to teach computer science in schools and developing countries
- System exploded in popularity, especially for robotics
- No peripherals or cases included, although some accessories are included in several bundles

Securing Raspberry Pi

- Keep your system updated
- Don't use auto-login or empty passwords
- Change the default password

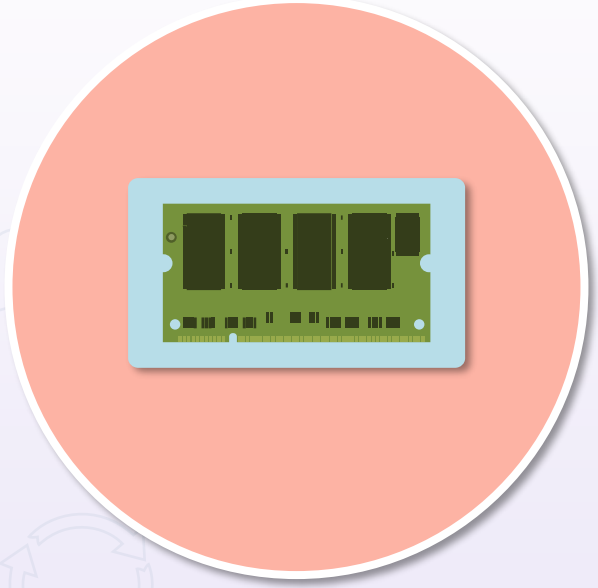
- Make sudo require a password
- SSH: prevent root login
- SSH: change the default port (SSH default port is 22)



- Disable the Pi user
- Stop unnecessary services

- SSH: use SSH keys instead of passwords
- Install Fail2ban tool to detect and block brute-force attacks

Arduino Security



- Open-source electronic prototyping platform enabling users to create interactive electronic objects
- The same security measures that are taken with IoT and Raspberry Pi apply to Arduino solutions

Securing Embedded Devices

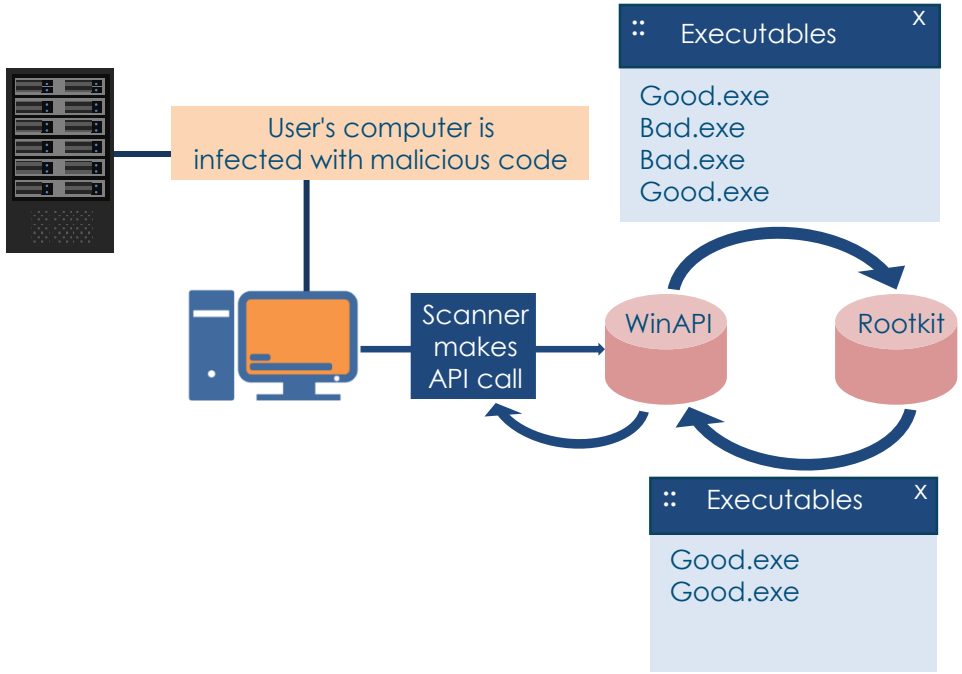
- Test in cloud before deployment
- Employ change and configuration management
- Initiate a patch management program
- Utilize digitally signed code
- Deploy trusted OS and firmware
- Hire skilled systems/security practitioners

Systems Security Certified Practitioner (SSCP)

Malware and countermeasures

Rootkit Malware

- Rootkits are malicious modules that are placed in unauthorized areas (root volumes) to
  - access data
  - monitor actions
  - escalate privileges
  - modify programs, and
  - conduct further exploits



Spyware

- Spyware is software that gathers data about a computer user without the user's permission or knowledge
- Spyware can show advertisements, track information, and make modifications to endpoints without user knowledge
- Malware, adware, and spyware are often found among P2P networks, download sites, and bit torrents
- Alexa, Echo, and similar "smart" things can be spyware

Scareware

- Scareware is a malware approach that influences users to believe they need to get or download malicious, often impractical, software
- The tactic is most often delivered with a pop-up ad that uses social engineering to leverage a user's fear, tricking them into installing fake anti-virus tools
- Scareware goals can vary from selling useless utilities to downloading harmful code that exposes sensitive data
- It has also been known to influence users to download ransomware

Ransomware

- Malware encrypts key files and holds them for "ransom", usually for a cryptocurrency such as Bitcoin
- Ransomware evolved from misleading "fix" apps to fake AV tools to bogus "fine" web sites
- CryptoLocker toolkits have exploded since Gpcoder in 2005
- The average ransom demand has more than doubled, and over 30% of victims are in the U.S.
- Newest trend is Ransomware as a Service (RaaS) on dark net, which is a subset of Malware as a Service (MaaS)

Ransomware Campaigns

1. INSTALLATION

Crypto-ransomware installs itself after bootup

2. CONTACTING HEADQUATERS

Malware contacts a server belonging to an attacker or group

3. HANDSHAKE AND KEYS

The ransomware client and server "handshake," and the server generates two cryptographic keys

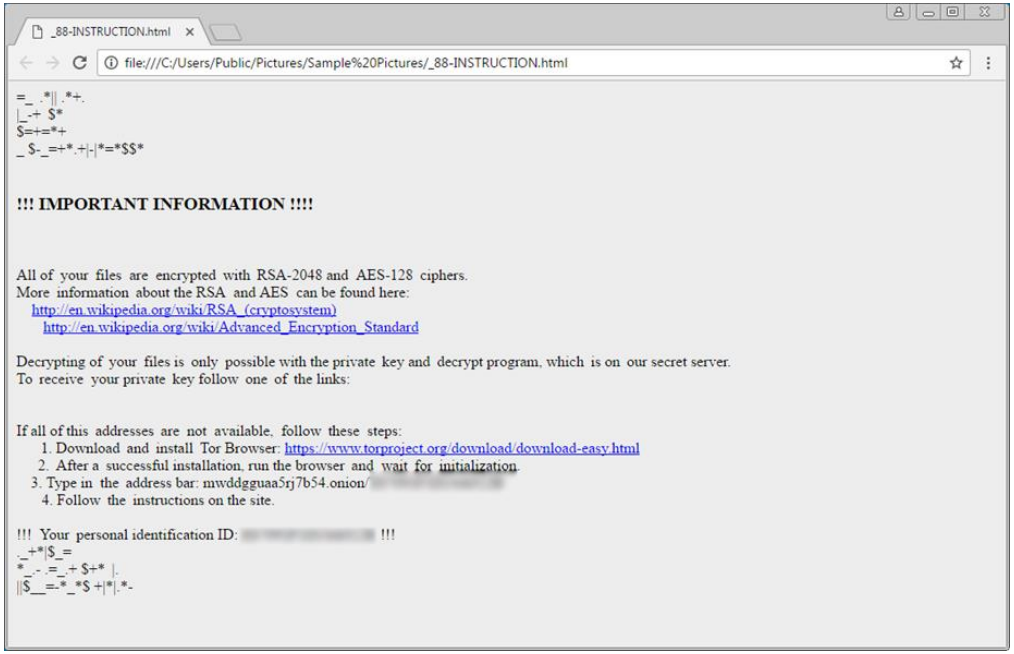
4. ENCRYPTION

The ransomware starts encrypting any files with common file extensions that it finds

5. EXTORTION

A screen displays giving a time limit to pay up before the criminals destroy the key to decrypt the files

Ransomware Campaigns



Viruses and Worms

- Viruses are malware that attach to a host program or file to deliver the payload
- Worms are a special form of self-replicating virus (malware) that generally spread without user action
- They distribute complete copies (possibly modified) of themselves across networks
- A worm can consume resources, infiltrate data, or simply cause the CPU on the system to waste cycles, resulting in a computer becoming unresponsive
- Viruses and worms can be file-based or fileless code that resides only in Random Access Memory (RAM)

Fileless Viruses

Fileless viruses operate in memory without being stored in a file or installed directly on a machine

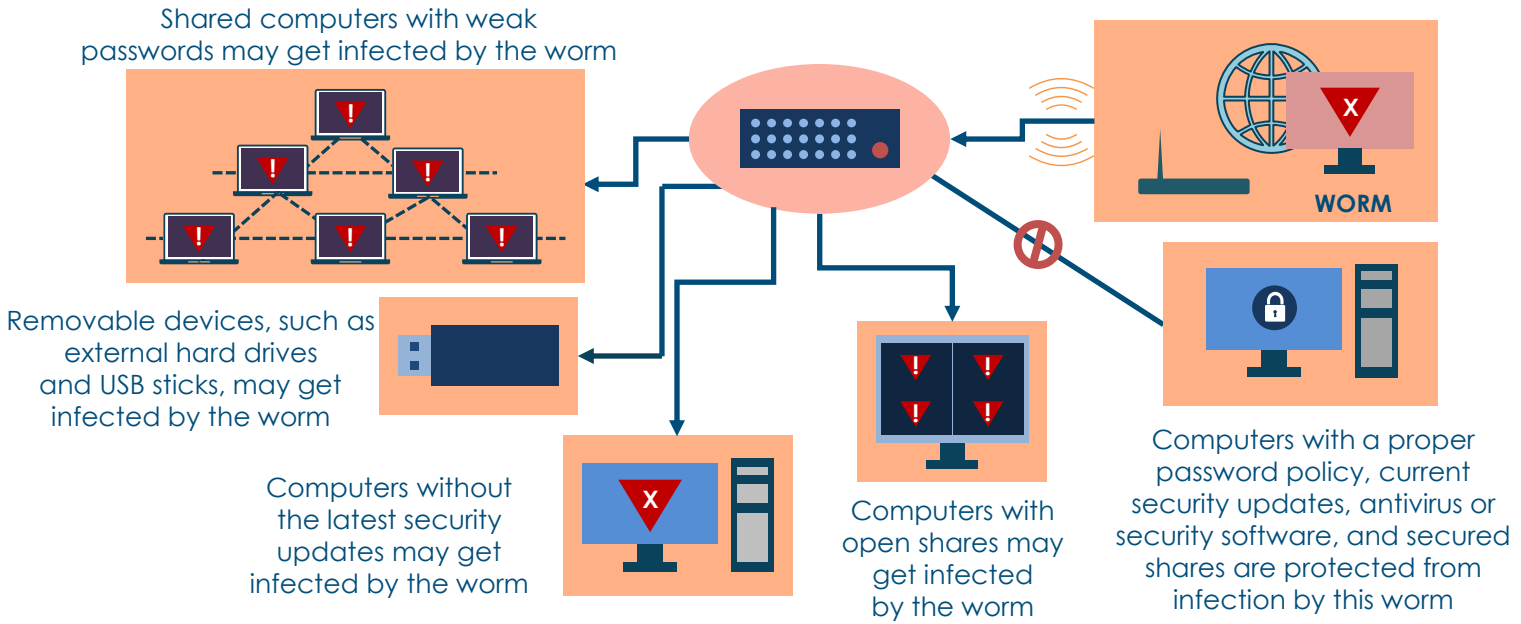
They go directly into memory and the malicious content never reaches a hard drive

An evolutionary strain of malicious software

Banks, telecoms, and government agencies are top targets

Frodo and Dark Avenger

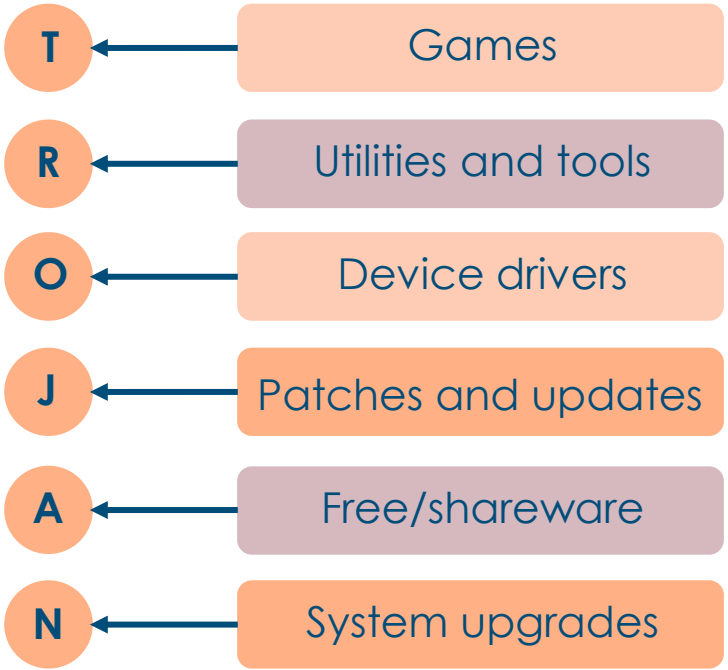
Worms


Shared computers with weak passwords may get infected by the worm
WORM
Removable devices, such as external hard drives and USB sticks, may get infected by the worm
Computers without the latest security updates may get infected by the worm
Computers with open shares may get infected by the worm
Computers with a proper password policy, current security updates, antivirus or security software, and secured shares are protected from infection by this worm

Trojan Malware

- Trojan horses have no replicating abilities like viruses or worms
- They are malicious code and programs that masquerade as legitimate applications or are embedded in real, operable programs and tools

Trojan Malware

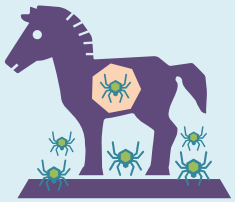


Remote Access Trojans (RATs)

Specific forms of Trojan horse malware – often part of multi-staged exploits

Create backdoors

Use Command and Control (C&C) servers

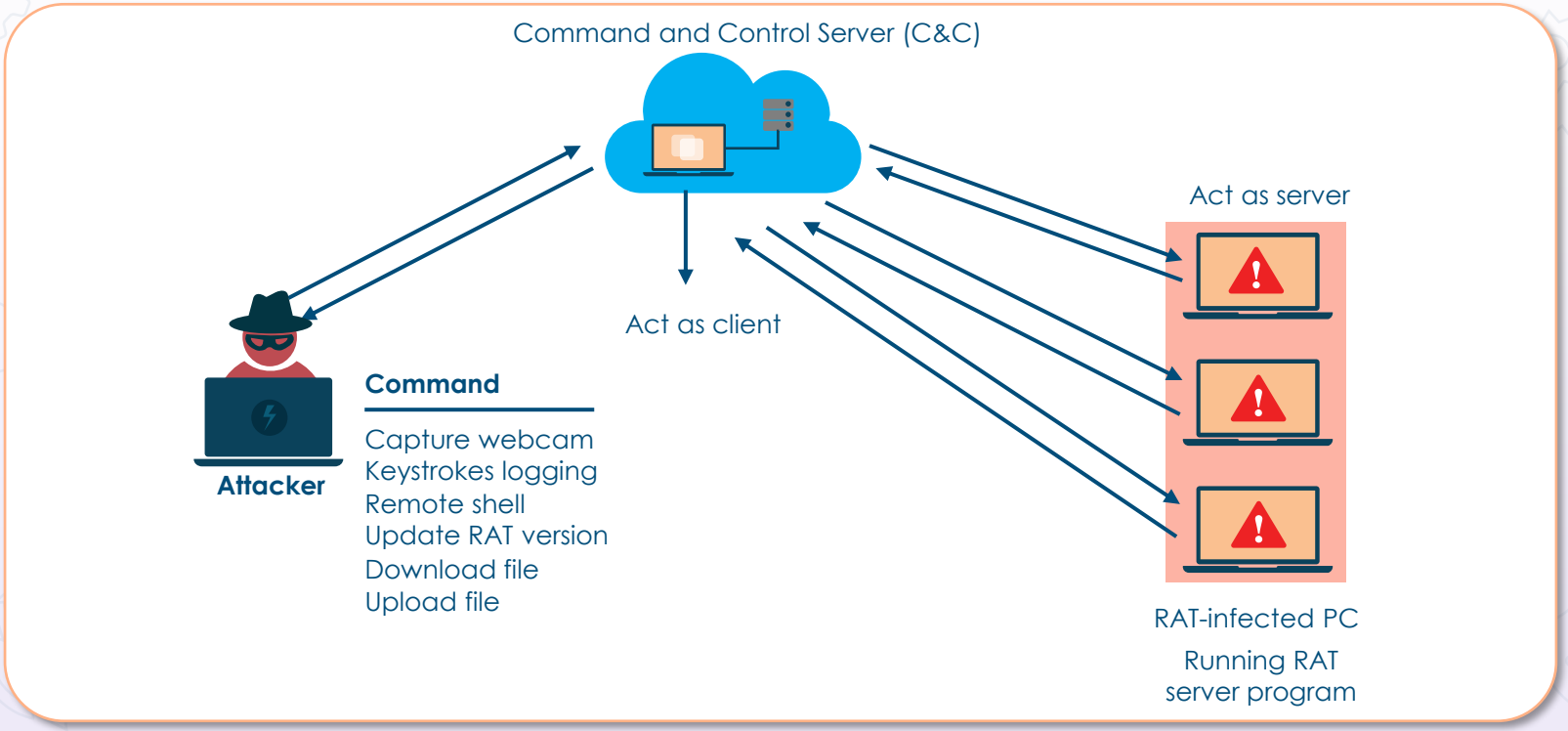


RATs

Now on mobile devices

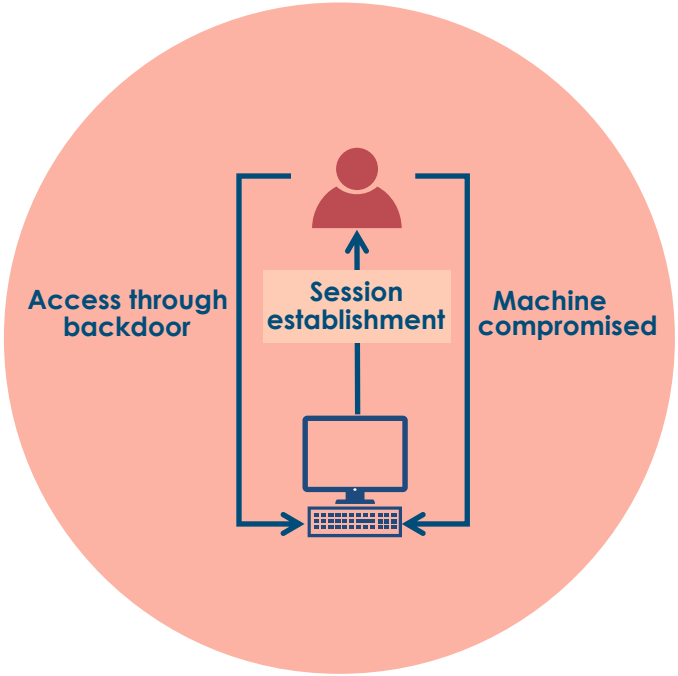
Gh0st, PlugX, Sakula

RATs and C&C Servers



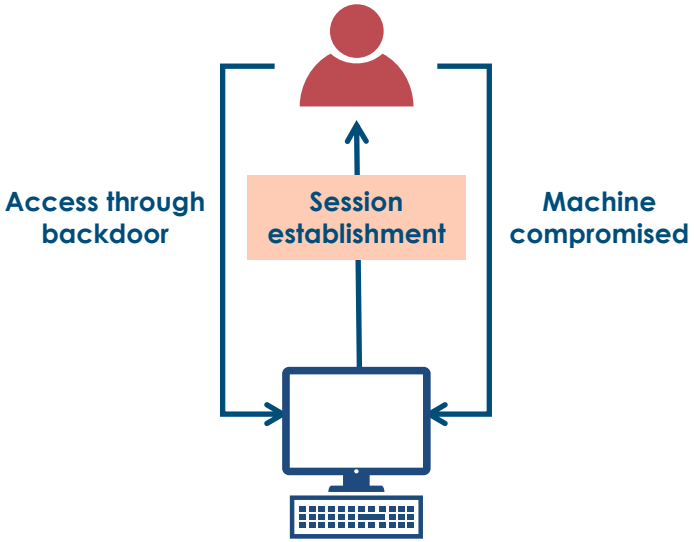
Backdoors

- Backdoors are Trojan programs
- Closely related to results of a botnet attack
- Generates a covert channel
- Remote attacker controls systems
- Common on mobile devices



Backdoor Exploits

- Collect system and personal data from the system and even attached storage devices
- Perform denial of service (DoS) attacks on other systems (Distributed DoS and botnet)
- Run and terminate tasks and processes
- Download additional files for multi-phased attack
- Upload files and other content
- Audit system status
- Open remote command line shells
- Modify computer settings
- Shut down or restart system



Vulnerability Scanning Terminology

- Vulnerability scanning is the process of identifying known and unknown weaknesses in systems, applications, services, and policies using tools
- Vulnerability scanning is an easier and often more focused process looking for unpatched systems, misconfigurations, and open ports
- It is typically automated and done on a routine basis (weekly, quarterly), taking at most a few hours
- Tuning must be performed in order to reduce false positives and false negatives

Vulnerability Scanning Sources

- Various logs (system, application, firewall, etc.)
- Simple Network Management Protocol (SNMP) traps and informs
- NetFlow v5 and v9 collection
- Security Information and Event Management (SIEM) systems

Vulnerability Scanning Sources

- Security Orchestration, Automation, and Response (SOAR)
- Next-Generation Intrusion Prevention System (NGIPS) alerts and logs
- Cloud-based machine learning (ML) and artificial intelligence (AI) visibility/analysis

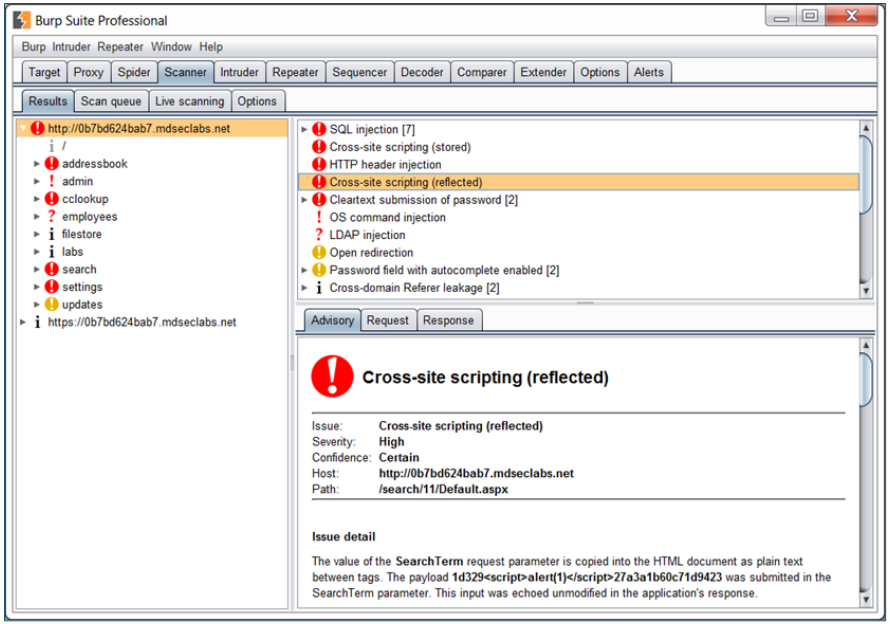
Web Vulnerability Scanning

- The most common vulnerability scanners will test web applications and services to look for
  - cross-site scripting and request forgery
  - SQL and other command injection
  - broken authentication and session management
  - insecure direct object references
  - insecure server configuration (XML, PHP, etc.), and
  - exposed sensitive data

Vulnerability Scanning Tools

- Nessus
- OpenVAS
- Core Impact
- Nexpose
- GFI LanGuard
- QualysGuard
- OWASP ZAP
- Burp Suite

Web Vulnerability Scanning



Vulnerability Databases

Common vulnerabilities and exposures (CVE)

- A list of entities from MITRE.org that represent publicly known cybersecurity vulnerabilities
- Consists of an ID number, description, and public references
- Used by the national vulnerability database (NVD)

Common vulnerability scoring system (CVSS)

- Open standard for weighing the severity of computer system vulnerabilities
- Uses a uniform and consistent scoring method ranging from 0 to 10, with 10 being the highest severity

Anti-malware Programs and Suites

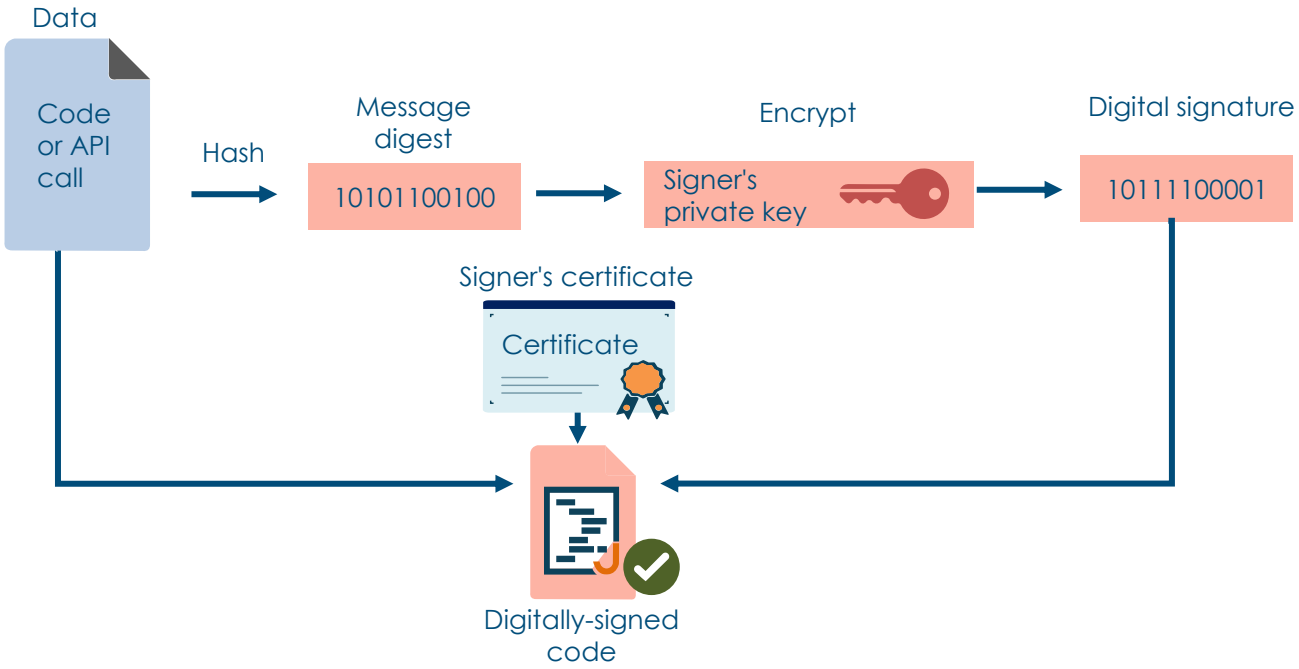
Anti-X

- Need to stay current with all updates and upgrades to security suites based on patch management initiatives
- Install two different vendor products on all systems if possible
- Newer security solutions should combine a variety of services including personal firewalls, cloud correlation, and ransomware protection, to name a few
- Managed security service providers can provide active agents to install on all endpoints, including mobile devices

Using Digitally Signed Code

- A digital signature is a cryptographic technique to achieve origin authentication, integrity, and non-repudiation
- All source code should be signed if feasible
- Other objects to digitally sign are executables, device drivers, OS images, service packs, updates, utilities, and API requests to programmatic cloud services

Using Digitally Signed Code



Advanced Persistent Threats (APTs)

- This is one of the most common descriptions of modern vectors used by threat agents today
- Threat actors will often conduct extensive planning and use critical success factors (CSFs) to determine the optimal targets for malware campaigns
- Describes many ransomware, extorsion, data theft, and cryptojacking exploits
- Advanced persistent threats (APTs) often attempt an escalation of access privileges soon after the initial compromise phase
  - The goal is to become a root or administrative user, level 15 user on a switch or router, exec user, Domain Admin group member, etc.

Advanced Persistent Threats (APTs)

- Often a long-term and well-planned malware campaign
- Pre-planned with cost-benefit analysis and CSF
- Persistent regarding both ongoing activities **and** system state existence
- Very often from nation state actors and cybercrime syndicates
- Sophisticated multi-phased polymorphic attacks

Insider Threats

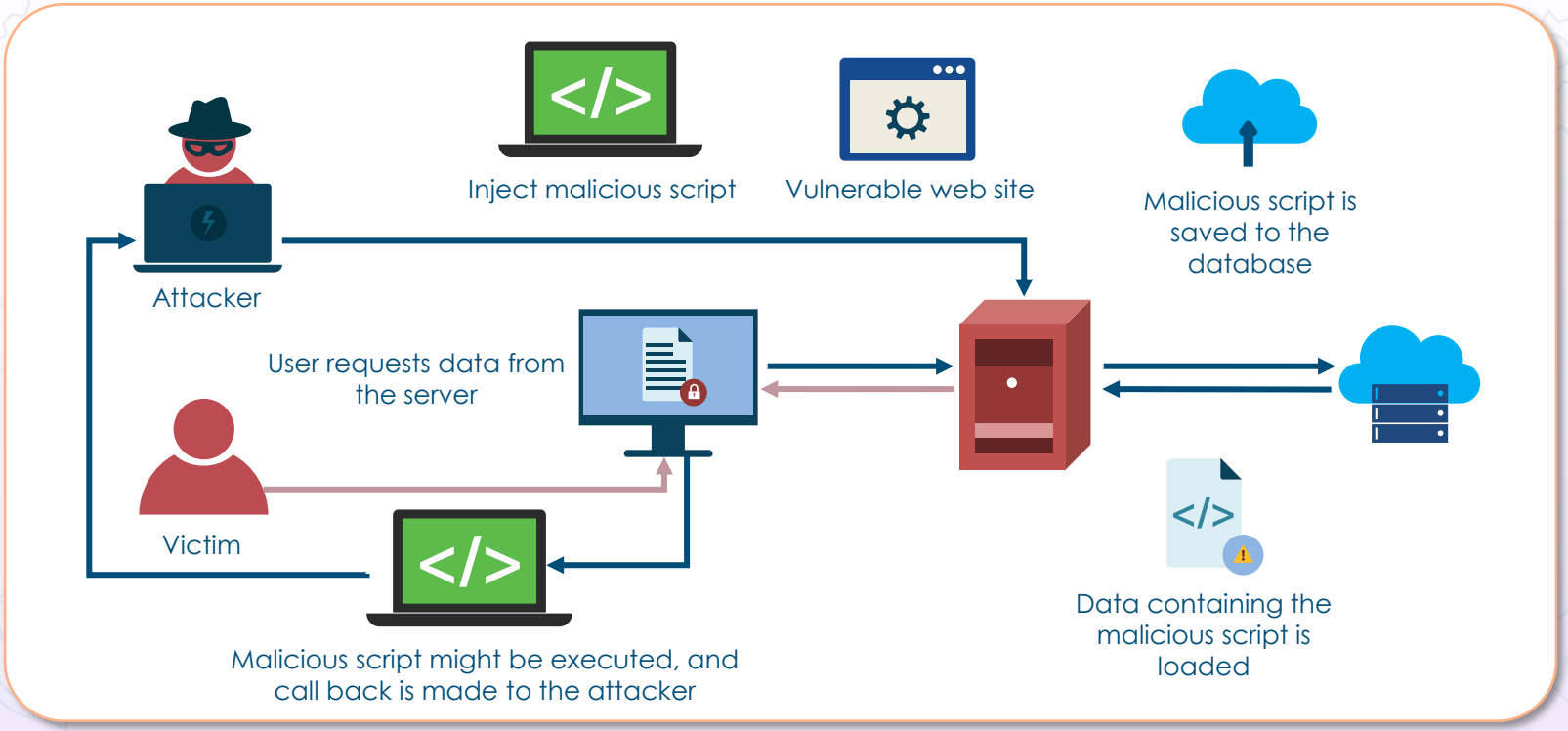
Often disgruntled employees or ex-employees

- Look for disgruntled or desperate employees with elevated privileges
- Have a zero-trust mentality regardless of the seniority of employees
- All are potentially susceptible to extortion or intimidation
- Always add ex-employees to the risk register/ledger soon after departure
- APTs can involve employees with fake identities or backgrounds infiltrating the enterprise
- Background checks and ongoing audits are critical as mitigation techniques

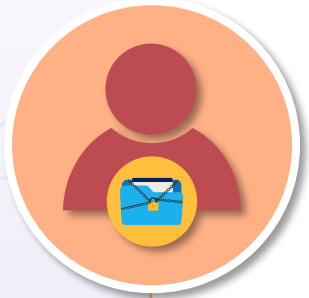
Cross-site Scripting (XSS)

- Flaws in pages rendered by web servers and not the web server code itself (i.e., Apache, IIS) where malicious scripts or code are injected into trusted or innocent web site pages
- Malicious scripts can steal cookies, session tokens, or other sensitive data stored by the browser and used with the site
- Attacker typically sends browser-side scripts to end user
- Can occur any time a web program uses user input within the output it generates without validating or encoding
- Variants are DOM-based (Local or Type 0), Reflected (Nonpersistent or Type 1), and Stored (Persistent or Type 2)

Cross-site Scripting (XSS)

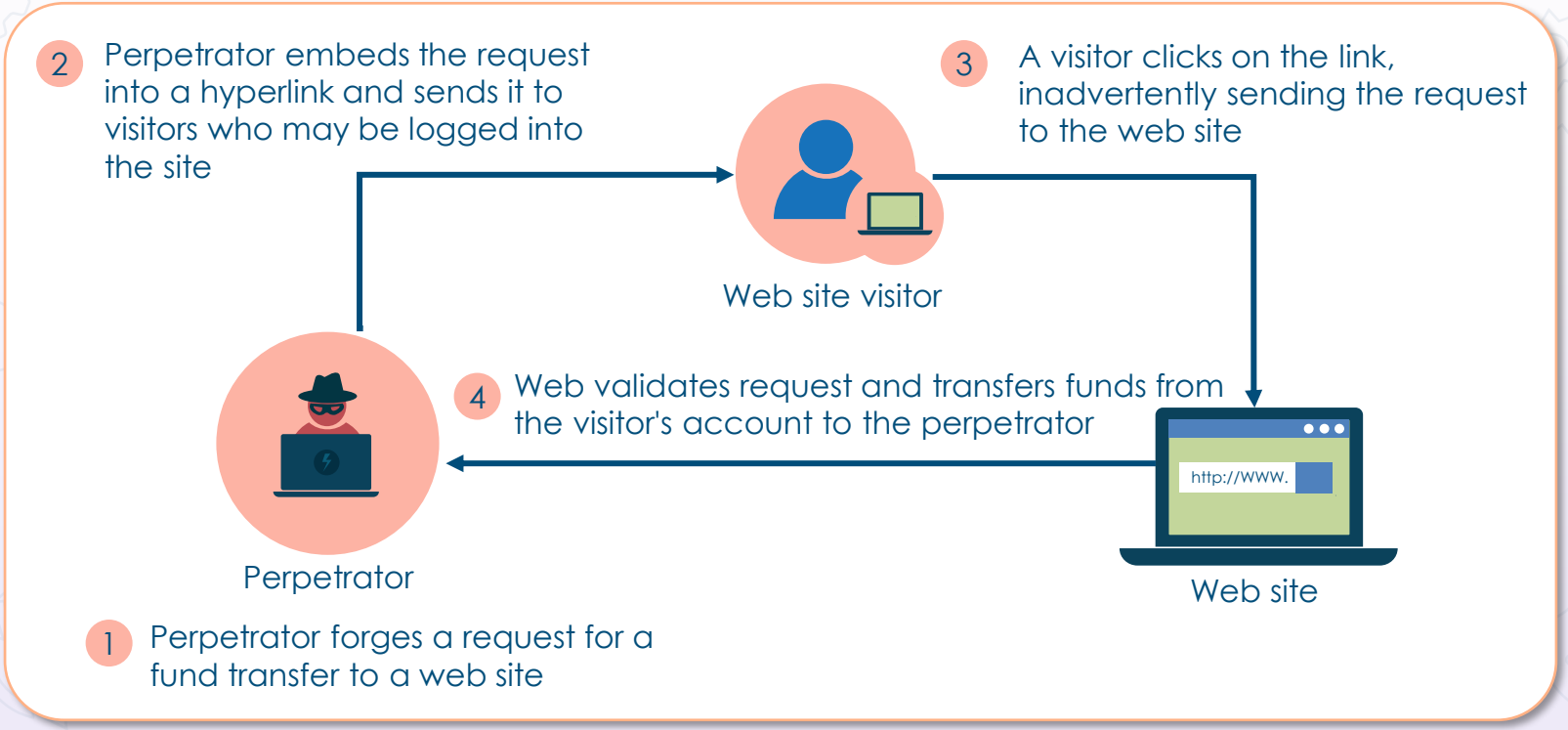


Request Forgery (CSRF/XSRF)



- Attack forces an end user to perform undesirable actions in a web application in which they are authenticated
- An effective Cross-site Request Forgery (CSRF/XSRF) attack can force users to perform state-changing requests such as
  - transferring funds
  - changing their e-mail address, and
  - changing their password
- If the victim is an administrative account, the CSRF attack can compromise the entire web application

Request Forgery (CSRF/XSRF)



SQL Injection

- One of the most common forms of injection attacks against web services
- Involves inserting a SQL query through input data from client to server application and can allow for several exploits
- A driving factor for migrating to NoSQL database systems

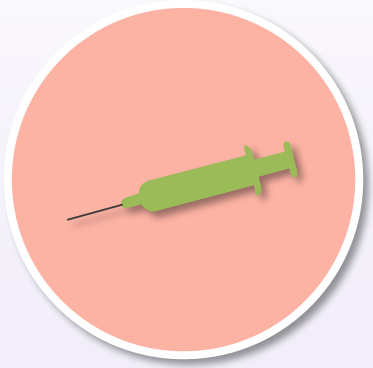
SQL Injection

- Read sensitive database data (SELECT FROM)
- Change database data (INSERT, UPDATE, DELETE)
- Execute administrative functions (e.g., shutdown DBMS)
- Get contents of files on database management system (DBMS)
- Run commands on operating system

LDAP Injection

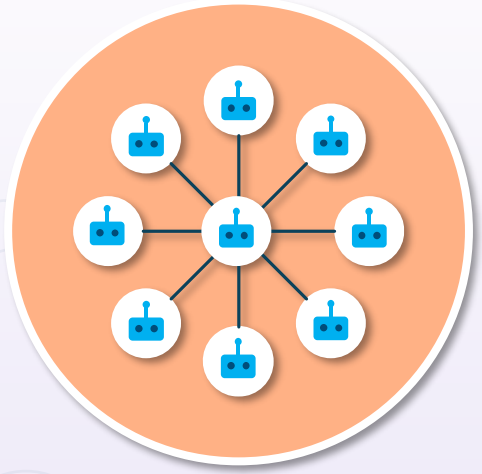
- The Lightweight Directory Access Protocol (LDAP) is a directory service protocol based on X.500 that runs on a layer above the TCP/IP stack
- LDAP is often used in web applications over the Internet or a corporate intranet
- The web applications take the input from the client in order to process it further, so the attacker exploits the data not being properly sanitized or going directly to a back-end database
- The attacks can render sensitive user information or change information in the LDAP directory

XML Injection



- Also known as "SOAP Injection"
- User input is inserted unsafely
- XML metacharacters can be used to modify web application
- Can interfere with application logic
- Performs unauthorized tasks or data access

Denial of Service (DoS) Attacks



Some of the oldest exploits that leverage inherent weaknesses in the TCP/IP stack

- DoS attacks try to consume a system's (or network's) critical resources, such as disk space, CPU cycles, memory (switch CAM tables), bandwidth, input queues, DHCP leases, etc.
- DoS attacks are still common and a major risk, because they can effectively interrupt business operations
- They are relatively simple to conduct with script kiddie tools

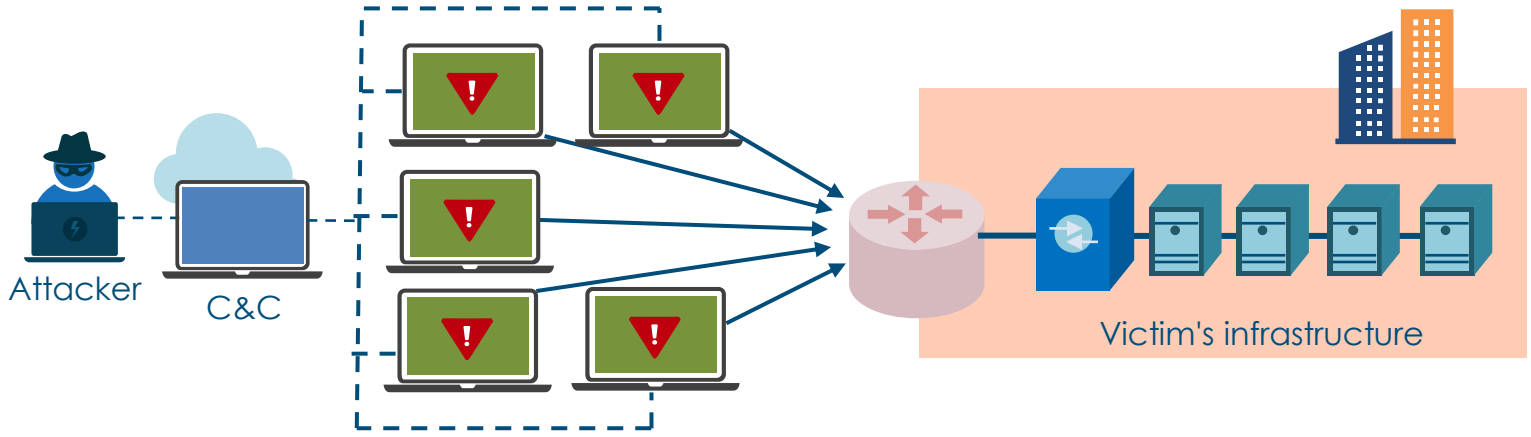
Botnets

- A botnet consists of a group of systems loaded with computer robot code (or bots)
- A C&C server control mechanism directs the zombie computers remotely, often by using Internet Relay Chat (IRC), peer-to-peer, or even Twitter

DDoS Botnets

- This is a Distributed DoS (DDoS) attack, which is often sourced from networks of compromised systems called botnets
- Malicious "zombiefied" hosts can also combine to flood a victim with many attack packets simultaneously from potentially thousands of sources

Botnets



Zero-day Vulnerabilities

All malware and exploits were a zero-day at one time or another

- "Zero-day" is a term describing a recently discovered exploit or malware for a vulnerability that attackers launch against systems
- Exploits can go unnoticed for years and are often sold on the black market for large sums of money

Zero-day Vulnerabilities

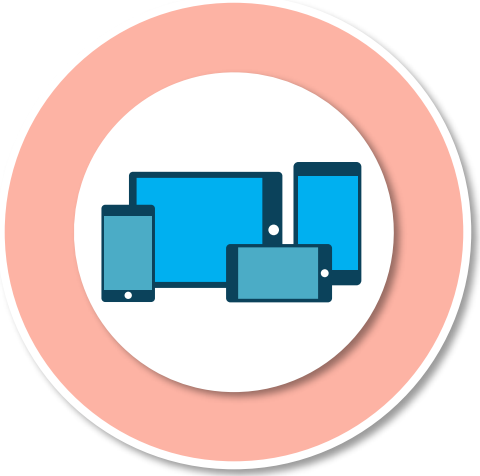
- These exploits are considered "zero-day" before and on the day that the vendor is made aware of the exploit's existence
- "Zero" refers to the number of days since the anti-malware vendor or organization discovered the threat
- Although there are millions of lines of zero-day code waiting to be logic bombed, the CVE is a valuable list of recently discovered security vulnerabilities
- Threat management and modeling tools like AWS GuardDuty are cutting-edge countermeasures

Malicious Activity Countermeasures

- Solid next-generation defense-in-depth mechanisms
- Advanced endpoint protection and enterprise mobility management
- User security awareness and training
- System hardening and patch management
- Change and configuration management
- Isolation and compartmentalization
- Data loss prevention (DLP) solutions and engines

Modern Enterprise Mobility Management

MobileIron, AirWatch, and XenMobile

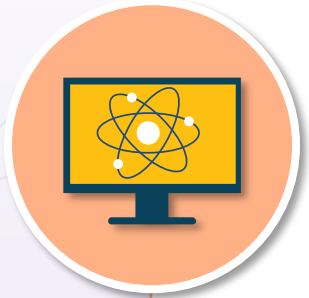


- Offer Bring Your Own Device (BYOD) and Mobile Application Management (MAM) security capabilities
- Provide flexible bundles for different use cases
- Unified endpoint management
- End-to-end security and identity management (IdM)
- Enterprise integration
- Productivity applications
  - Create mobile business apps without writing code
- Introduce User Behavioral Analytics (UBA)

Next-generation Endpoint Protection

- Partner with a Managed Security Services Provider (MSSP) or Cloud Access Security Broker (CASB)
- Advanced anti-virus with ML and AI
- Managed threat hunting (honey tokens)
- Cloud-based threat intelligence and UBA
- IT hygiene

Post-quantum Computing

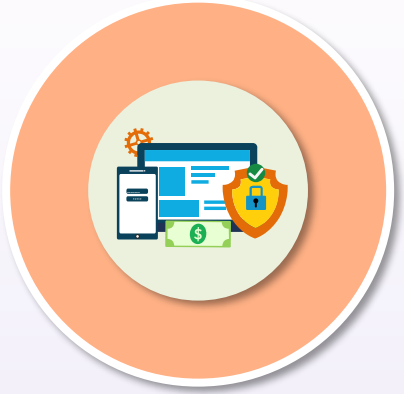


- Post-quantum cryptography involves developing new cryptosystems that can be implemented using today's existing computers but that will be resistant to attacks from tomorrow's quantum computers
  - Increase the size of digital keys
  - Develop more complex trapdoor functions
  - Lattice-based cryptography
  - Supersingular isogeny key exchange

Homomorphic Encryption

- Helps to protect data-in-use
- Data remains encrypted while being processed
- Cloud service providers can apply functions on encrypted data
- Commonly uses public/private keypair
- Uses algebraic operations on ciphertext

Systems Security Certified Practitioner (SSCP)



Endpoint protection and mobile device management

Host-based Intrusion Detection Systems (HIDS)

- Host-based IDS (HIDS) are designed to collect information about activity on a particular single system, or host
- These host-based agents (aka sensors) are often installed on a system that is deemed to be susceptible to possible attacks
- The host-based IDS (HIDS) market was dominated by Cisco and a few anti-virus companies for years
- HIDS eventually evolved into host-based IPS (intrusion prevention systems), security suites, and endpoint detection and response (EDR), although HIDS and HIPS solutions still exist on the market

Comparing HIDS Pros and Cons

Pros

- Can be a cost-effective way to add defense-in-depth to critical endpoints
- Can provide more granular visibility into local system activities of attacks and user behavior
- Are more customizable than network-based solutions

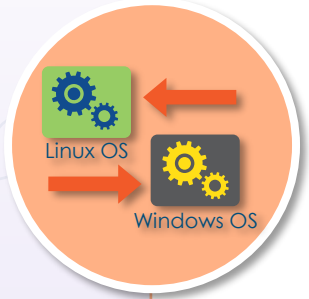
Cons

- Depend heavily on audit trails
- Agents can be difficult to uninstall
- Vendors are often way behind the OS manufacturers and quickly become outdated
- Earlier HIDS had no ability to do cloud updates

Host-based IPS (HIPS)

- Modern host-based IPS solutions utilize vendor-specific and proprietary techniques that increase the chance of halting attacks
- Most work in concert with cloud computing to stay up-to-date
- Most security suite packages are a form of HIPS, EDR, or next-generation endpoint protection

Personal Firewalls



- ZoneAlarm was one of the first third-party personal firewalls, introduced more than 20 years ago
- Operating system vendors like Microsoft soon offered integrated personal firewalls to
  - open and close unnecessary TCP and UDP ports
  - stop unused system services
  - offer program control and child-control filters, and
  - integrate antivirus and antimalware features
- These solutions can still be used together with third-party products, but most are replaced by full security suites from well-known vendors
- Secure browsers have also made huge inroads on client systems

Application Whitelisting

Whitelisting vs. blacklisting

Whitelisting

Application whitelisting usually involves a stateful firewall that permits traffic based on IP addresses, services, and port numbers while implicitly denying all other traffic

Personal firewalls and security suites can apply whitelisting on all types of endpoints

Blacklisting

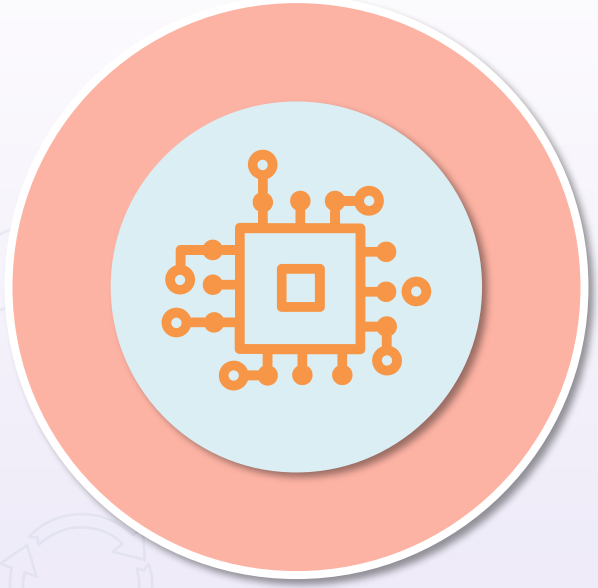
Blacklisting is a restrictive approach that typically uses stateless access control lists and firewall rules to deny specific traffic based on layer 3 and metadata in IPv4 and IPv6 headers

It is often used to protect endpoints that are under attack from specific attackers

Self-encrypting Drives (SED)

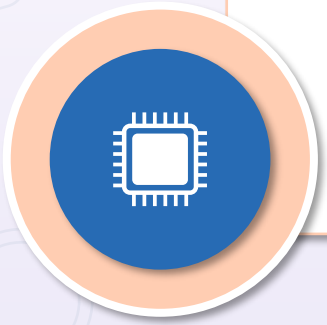
- Implements hardware-based full disk encryption (FDE)
  - All contents on the drive are encrypted, including keys
  - Encrypts data as written and decrypts data as read
  - Invisible and transparent to the end user and can't be turned off
  - Less susceptible to threats when compared with software-based encryption such as Microsoft BitLocker
  - Protects against stolen keys, repurposed drives, theft of device, and end-of-life challenges
  - Provides preboot authentication, endpoint security, and device authentication
  - Also offers key management, network access control, and policy compliance

Hardware Root of Trust



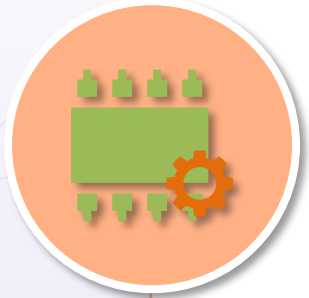
- Hardware root of trust anchors the trustworthiness of a system to hardware, not software, which is more secure than software solutions
- Less susceptible to attacks, since security solutions are on-chip
  - SED – self-encrypting drives
  - TPM – module embedded in a system
  - HSM – dedicated crypto processors

Boot Integrity



- UEFI – Unified Extensible Firmware Interface
  - Replaces legacy BIOS (basic input/output system)
  - Low-level software for booting the device
  - Tests hardware components – POST (power-on self-test)
  - Gets the OS up and running
  - Offers the ability to protect the device at a lower level with passwords

Boot Integrity



- Computer chip (microcontroller) installed on the device or built into PCs, tablets, and phones
  - Tamper-resistant security chip
  - Stores passwords, certificates, and encryption keys needed to authenticate the platform
- Provides the following for the platform:
  - integrity (ensures system has not been altered at a low level)
  - authentication (ensures system is in fact the correct system), and
  - privacy (ensures system is protected from prying eyes)

SEAndroid

Specialized Android operating system that uses Security-Enhanced Linux (SELinux) to enforce mandatory access control (MAC) over all processes

With SELinux, Android can protect and compartmentalize system services

SEAndroid controls access to application data and system logs

Together these reduce the effects of malicious software and protect users from probable flaws in code on mobile devices

Secure Browsing

- Secure browsers will use several security features:
  - browsing privacy features and anti-tracking
  - automatic updates with vendor cloud
  - sandboxing of potentially unwanted programs (PUPs)
  - VPN integration
  - anti-phishing and ransomware protection
  - automatic HTTPS encryption (using HSTS)
  - secure "Bank Mode" that creates a virtual desktop to isolate sensitive transactions against hacks
  - Webcam cracking protections

Endpoint Detection and Response (EDR)

- Evolved from early HIDS solutions
- A "lighter" software agent installed on the host system often provides the basis for event monitoring and reporting
- EDR tools monitor endpoint and network events and send information to a SEIM system or centralized database so further analysis, investigation, and reporting can take place

Endpoint Detection and Response (EDR)

- EDR tools primarily focus on detecting and investigating suspicious activities and are indicators of compromise (IoCs) on hosts/endpoints such as
  - insider threats
  - data theft and exfiltration
  - distributed denial of service (DDoS)/botnets
  - zero-day exploits
  - web-based attacks, and
  - advanced persistent threats (APTs)

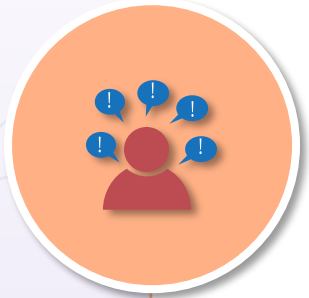
Key EDR Features

- **Filtering** – reduces alert fatigue and lowers the possibility for real threats to slip through unnoticed
- **Advanced threat blocking** – prevents threats the moment they are detected and throughout the lifecycle of the attack
- **Incident response capabilities** - threat hunting and incident response can help prevent full-blown data breaches (DLP, i.e., data loss prevention)
- **Multiple threat protection** – cloud-based visibility into many finding categories

Next-generation Endpoint Protection

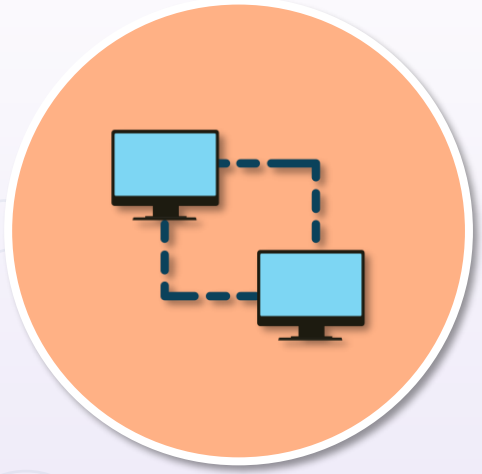
- Partner with an MSSP or CASB
- Advanced anti-virus with ML and AI
- Managed threat hunting (honey tokens)
- Cloud-based threat intelligence and User Behavioral Analytics (UBA)
- IT hygiene

Heuristics and Behavioral Analytics



- Most NGIPS and anti-virus systems use heuristic and ML mechanisms to achieve better results than traditional signature-based and anomaly-based solutions
- Heuristic engine used by an anti-malware/IPS program might include proactive rules and behavioral analytics to look for
  - a program that tries to copy itself into other programs (in other words, a classic computer virus), or
  - a program that tries to remain resident in memory after it has finished executing

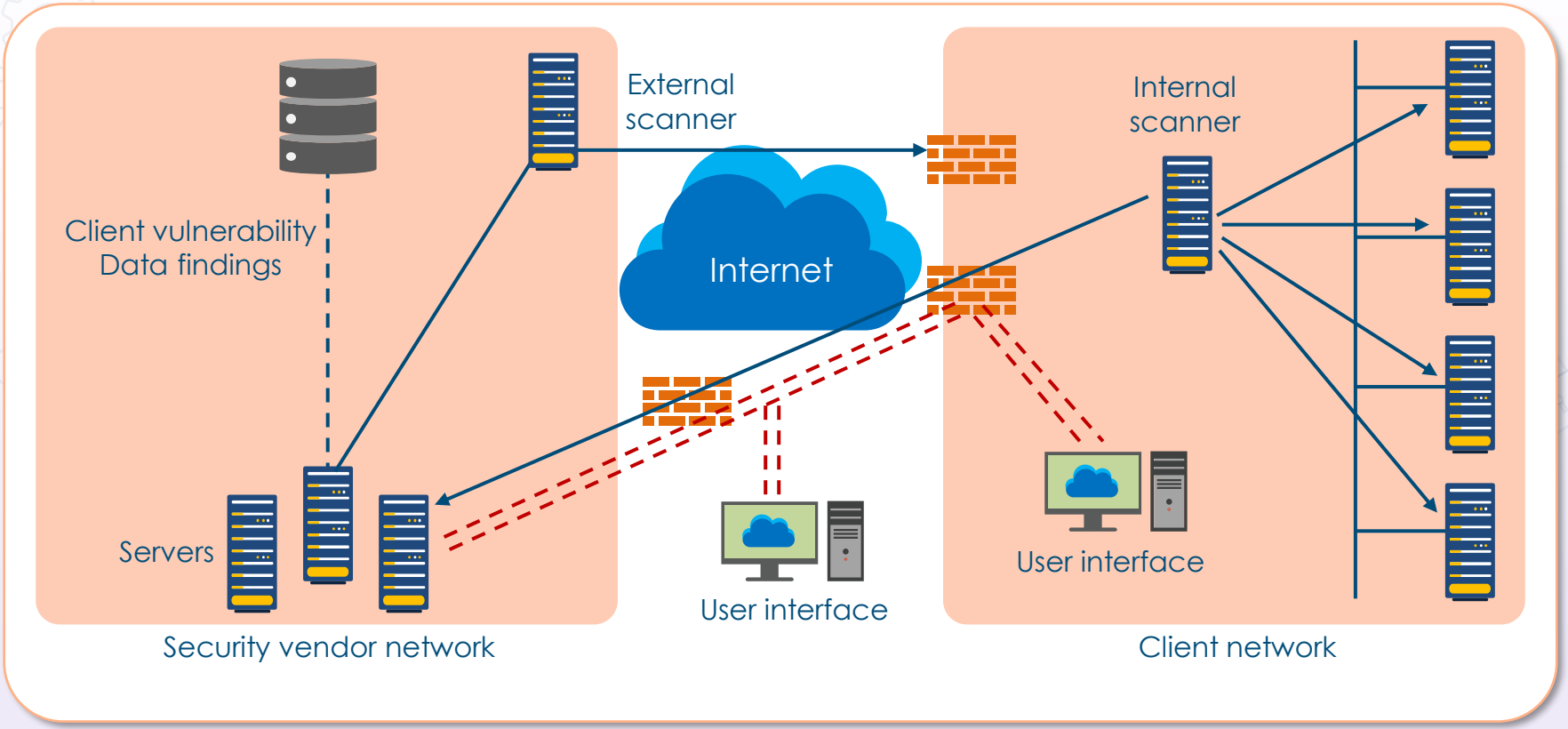
NAC and Endpoint Protection



Network Admission Control (NAC) was an industry initiative sponsored by Cisco

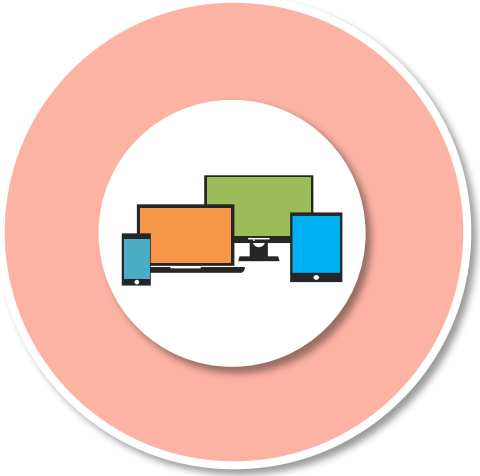
- Cisco NAC and similar technologies are officially on the exam but have been replaced by newer solutions, such as TrustSec and Zero Trust Security
- It was part of the Cisco Self-Defending Network initiative and is the foundation for enabling NAC on Layer 2 and Layer 3 networks
- Do not trust anything inside or outside the perimeter without stringent authentication and verification
- Helps secure access from users and their devices, API calls, IoT, microservices, containers (Dockers, Kubernetes,) and more

Cloud-based EDR



Mobile Deployment Models

BYOD



- **Bring Your Own Device**
- Employees are permitted to use their personal mobile devices to access enterprise data and systems
- There are four basic options:
  - unlimited access for personal devices
  - access only to non-sensitive systems and data
  - access with IT control over personal devices, apps, and stored data, or
  - access while preventing local storage of data

Mobile Deployment Models

CYOD

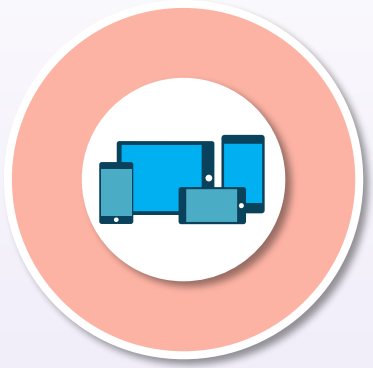
- **Choose Your Own Device**
- Much like BYOD in that it lets employees work from anywhere using a mobile device
- CYOD devices must be approved by the organization, unlike BYOD
- Users often select from a list of approved devices, which are usually smartphones
- These networks offer more stability, security, and simplified IT for most businesses

Mobile Deployment Models

COPE

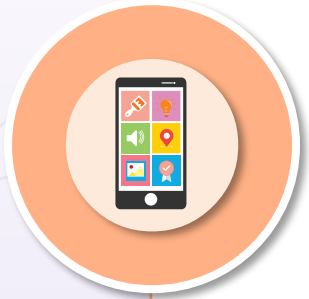
- **Corporate-owned Personally-enabled (COPE)**
- Company gives employees mobile devices
- Users can handle as if they were their own
- Prevents the need for two smartphones
- Programs should use containerization tools

Virtual Desktop Infrastructure (VDI) for Mobility Devices



- Utilizes virtual desktop interface technology
- Reduces cost/complexity and improves security and uptime
- Increased agility, as not just for smartphones (COPE)
- VDI separates the app and the data
- Tablets using a separate Bluetooth-enabled keyboard

Enterprise Mobility Management (EMM)



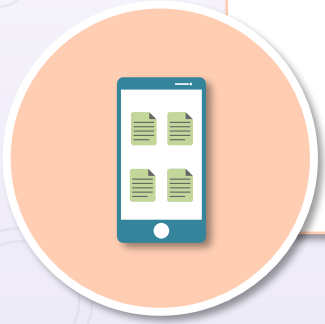
- Organizations must securely configure and implement each layer of the technology stack, including mobile hardware, firmware, O/S, management agent, and the apps used for business
- Solution should reduce risk, so employees are able to access the necessary data from nearly any location, over any network, using a wide variety of mobile devices
- Enterprise mobility management is the combination of mobile device management (MDM) and mobile application management (MAM)

Mobile Device Management (MDM)

- Organizations must securely configure and implement each layer of the mobile technology stack, including hardware, firmware, O/S, management agent, provider agreements, and apps used for business
- The solutions should reduce risk while enabling employees to access applications and necessary data from nearly any location, over any network, using a wide variety of mobile devices in some cases
- Enterprise mobility management (EMM) = mobile device management (MDM) + mobile application management (MAM)

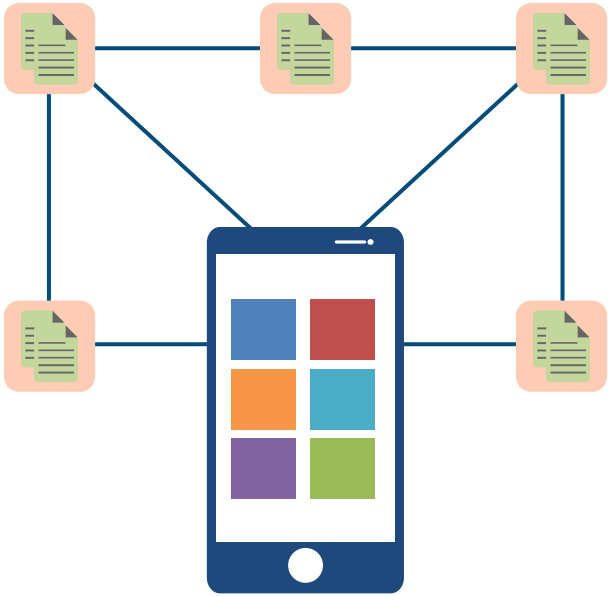
Enterprise Mobility Management (EMM)

- There are three basic core competencies that all organizations need from an EMM solution:
  - **Visibility**: understanding what's running on mobile devices is the key to discovering potential risks and adhering to compliance policies
  - **Secure access**: providing the ability for mobile users to securely authenticate and authorize access to apps and data
  - **Data protection**: offering dynamic anti-malware and data loss prevention capabilities to help limit the risk of attacks and data breaches



Mobile Device Management (MDM)

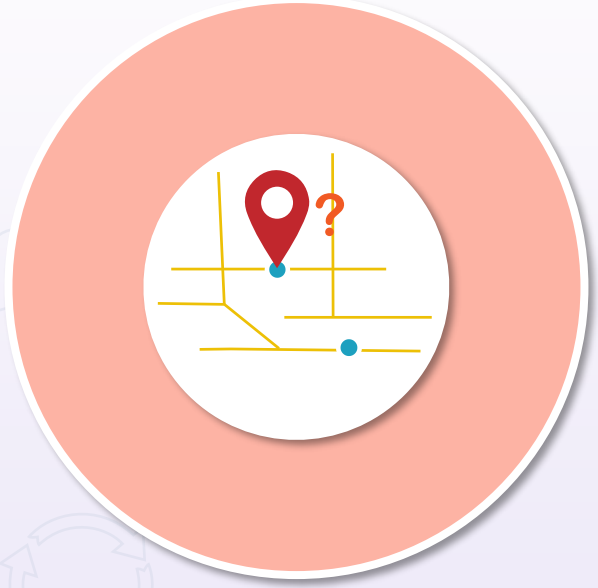
- Technology to enable the management and control of mobile devices used to access business resources
  - Enrolling devices for management
  - Provisioning settings, like digital certificates and profiles
  - Monitoring, measuring, and reporting device compliance
  - Removing corporate data from devices (data leak prevention)
- Some activities are network access control, preadmission control, remote lock and wipe
- Other features that can sometimes be attributed to MDM platforms are remote virtual private network (VPN) capabilities



Common MDM Activities

- Onboarding, offboarding, and installing certificates
- Implementing touch ID authentication and screen locking
- Configuring PINs and push notifications for user devices
- Deploying and managing full device encryption
- Finding lost devices and remote wiping

Geofencing and Geolocation

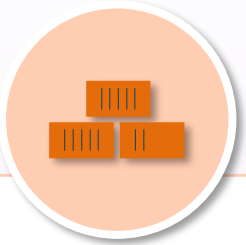


- Geofencing and geolocation services allow IT to physically track mobile devices
- Geolocation is a point on a map whereas geofencing is a square area on the map also known as GPS tagging
- Administrators can use geolocation to find a lost or stolen device and geofencing to determine when a device moves in and out of a certain (secure) area

Mobile Biometrics

- Toshiba introduced fingerprint scanning in 2007
- Apple brought Touch IDs for 5S in 2013
- Fingerprint recognition is the most popular
- Voice recognition and iris scanning are emerging
- Electroencephalogram reading and pattern swipe are future technologies

Advanced MDM

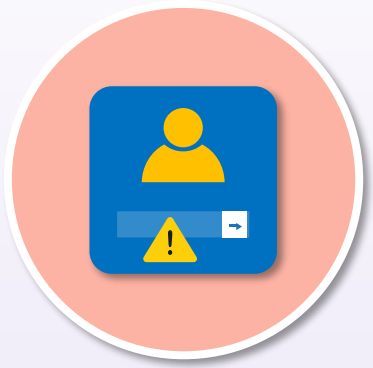


Containerization is orchestrating the packaging, isolation, and encapsulation of apps and work data in a separate segmented user space within the device

Storage segmentation involves partitioning various types of data on devices to protect IP, PII, and PHI and support DLP initiatives

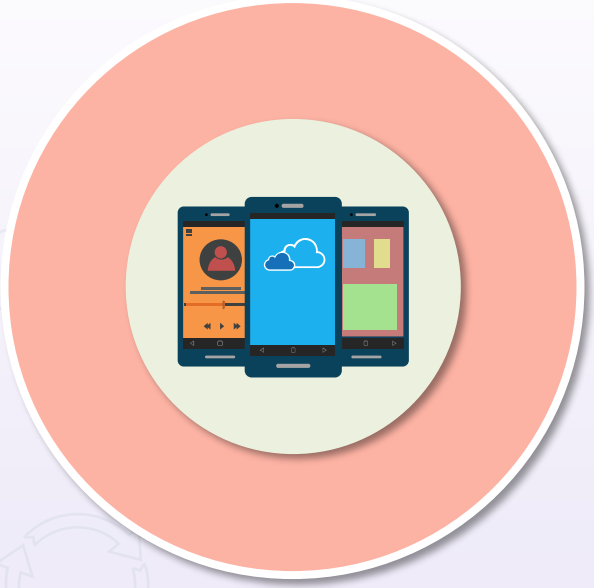
Full Device Encryption (FDE) is strong encryption at the hardware level on a smartphone or other device beyond the control of the user

EMM Challenges



- Managing X509v3 certificates
- Tethering and tokenization (used as MFA factor)
- Mobile payments and cybercurrency wallets (also NFC-enabled)
- OEM and carrier fragmentation
- Unauthorized remote locking and wiping

Mobile Application Management (MAM)



- Involves publishing mobile apps to users
- Continual monitoring, configuration, and updating of apps
- Mobile managers will report on app inventory and usage
- Securing and removing corporate data within mobile apps
- Also involves mobile content management

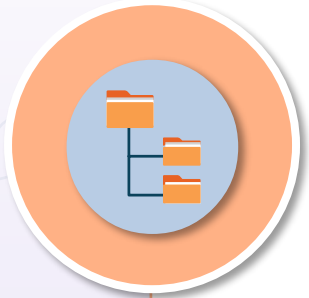
MAM Data Privacy Concerns

- Data storage and remnants
- Non-removable storage
- Removable storage
- Transfer/back up data to uncontrolled cloud storage
- Intellectual property and corporate data leakage

Jailbreaking

- Jailbreaking and rooting are very different, even though they both involve privilege escalation
- Jailbreaking an iPhone basically allows the installation of third-party apps not approved by Apple's strict controls
- You cannot modify the OS or system files like an administrator, and you're still bound by the iOS framework
- A jailbroken iPhone can be reverted back to a standard 'jailed' device by restoring the device in Recovery Mode
- Apple has responded with patching exploits and upgrading hardware to iOS

Rooting



- Rooting grants full access to a device on a level much higher than jailbreaking, giving access to the Android system and beyond
- Every line of code in the Linux-based device becomes editable, with options only restricted by coding skills
- Since Android is open source, you can go into recovery mode and download a modified or even entirely new version of the OS if you want
- You can alter any and all hardware, software, or aesthetic settings on the device

Sideloading

- Sideloading basically refers to the moving of media files to a mobile device using USB, Bluetooth, or Wi-Fi
- It can also involve writing to a memory card to insert into a mobile device
- With Android apps, sideloading usually installs an app package in APK format onto a device, with packages typically downloaded from sites other than Google Play
- Sideloading of apps is only likely if the user has allowed "Unknown Sources" in their security settings

MDM vs. MAM in a Nutshell

MDM

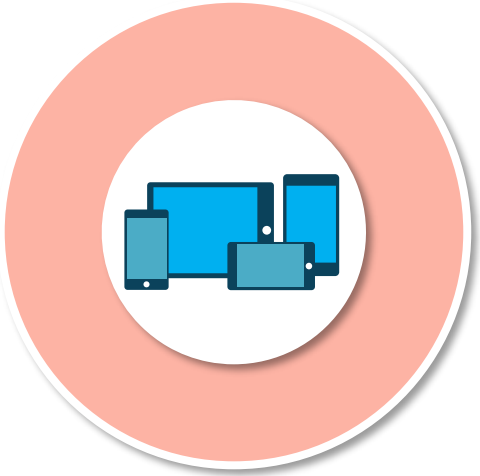
- Enrolling devices for management
- Provisioning settings, like digital certificates and profiles
- Monitoring, measuring, and reporting device compliance
- Removing corporate data from devices (data leak prevention)

MAM

- Publishing mobile apps to users
- Configuring and updating apps
- Reporting app inventory and usage
- Securing and removing corporate data within mobile apps

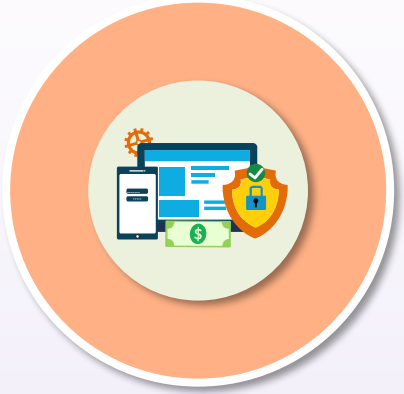
Modern EMM Attributes

MobileIron, AirWatch, and XenMobile



- Offer BYOD and MAM security capabilities
- Provide flexible bundles for different use cases
- Unified endpoint management
- End-to-end security and identity management (IdM)
- Enterprise integration
- Productivity applications that enable the creation of mobile business apps without writing code
- Introduce User Behavioral Analytics (UBA)

Systems Security Certified Practitioner (SSCP)



Endpoint protection and mobile device management

Host-based Intrusion Detection Systems (HIDS)

- Host-based IDS (HIDS) are designed to collect information about activity on a particular single system, or host
- These host-based agents (aka sensors) are often installed on a system that is deemed to be susceptible to possible attacks
- The host-based IDS (HIDS) market was dominated by Cisco and a few anti-virus companies for years
- HIDS eventually evolved into host-based IPS (intrusion prevention systems), security suites, and endpoint detection and response (EDR), although HIDS and HIPS solutions still exist on the market

Comparing HIDS Pros and Cons

Pros

- Can be a cost-effective way to add defense-in-depth to critical endpoints
- Can provide more granular visibility into local system activities of attacks and user behavior
- Are more customizable than network-based solutions

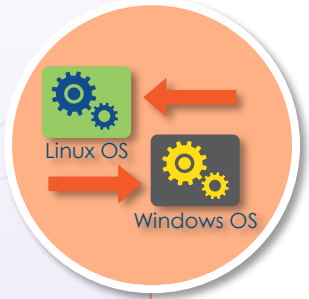
Cons

- Depend heavily on audit trails
- Agents can be difficult to uninstall
- Vendors are often way behind the OS manufacturers and quickly become outdated
- Earlier HIDS had no ability to do cloud updates

Host-based IPS (HIPS)

- Modern host-based IPS solutions utilize vendor-specific and proprietary techniques that increase the chance of halting attacks
- Most work in concert with cloud computing to stay up-to-date
- Most security suite packages are a form of HIPS, EDR, or next-generation endpoint protection

Personal Firewalls



- ZoneAlarm was one of the first third-party personal firewalls, introduced more than 20 years ago
- Operating system vendors like Microsoft soon offered integrated personal firewalls to
  - open and close unnecessary TCP and UDP ports
  - stop unused system services
  - offer program control and child-control filters, and
  - integrate antivirus and antimalware features
- These solutions can still be used together with third-party products, but most are replaced by full security suites from well-known vendors
- Secure browsers have also made huge inroads on client systems

Application Whitelisting

Whitelisting vs. blacklisting

Whitelisting

Application whitelisting usually involves a stateful firewall that permits traffic based on IP addresses, services, and port numbers while implicitly denying all other traffic

Personal firewalls and security suites can apply whitelisting on all types of endpoints

Blacklisting

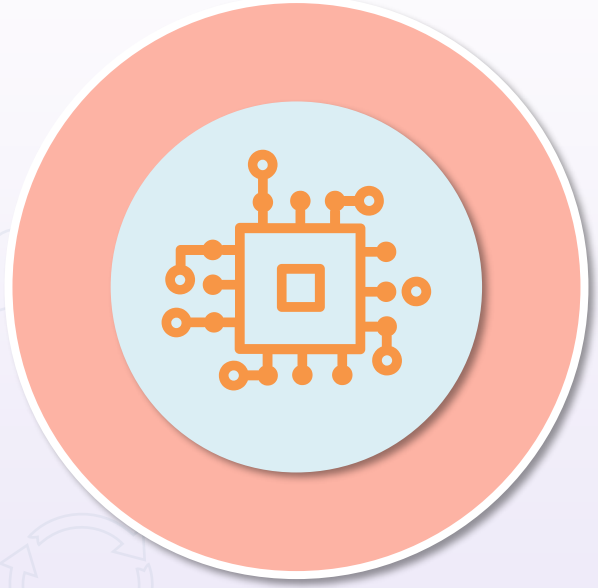
Blacklisting is a restrictive approach that typically uses stateless access control lists and firewall rules to deny specific traffic based on layer 3 and metadata in IPv4 and IPv6 headers

It is often used to protect endpoints that are under attack from specific attackers

Self-encrypting Drives (SED)

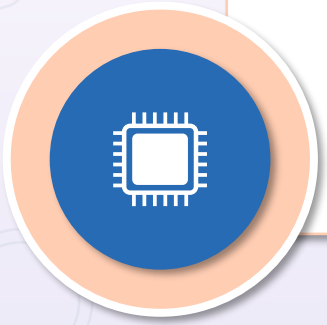
- Implements hardware-based full disk encryption (FDE)
  - All contents on the drive are encrypted, including keys
  - Encrypts data as written and decrypts data as read
  - Invisible and transparent to the end user and can't be turned off
  - Less susceptible to threats when compared with software-based encryption such as Microsoft BitLocker
  - Protects against stolen keys, repurposed drives, theft of device, and end-of-life challenges
  - Provides preboot authentication, endpoint security, and device authentication
  - Also offers key management, network access control, and policy compliance

Hardware Root of Trust



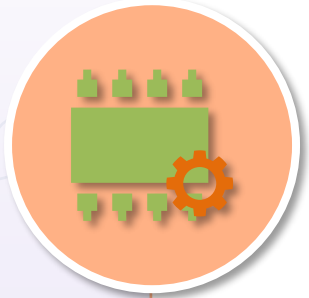
- Hardware root of trust anchors the trustworthiness of a system to hardware, not software, which is more secure than software solutions
- Less susceptible to attacks, since security solutions are on-chip
  - SED – self-encrypting drives
  - TPM – module embedded in a system
  - HSM – dedicated crypto processors

Boot Integrity



- UEFI – Unified Extensible Firmware Interface
  - Replaces legacy BIOS (basic input/output system)
  - Low-level software for booting the device
  - Tests hardware components – POST (power-on self-test)
  - Gets the OS up and running
  - Offers the ability to protect the device at a lower level with passwords

Boot Integrity



- Computer chip (microcontroller) installed on the device or built into PCs, tablets, and phones
  - Tamper-resistant security chip
  - Stores passwords, certificates, and encryption keys needed to authenticate the platform
- Provides the following for the platform:
  - integrity (ensures system has not been altered at a low level)
  - authentication (ensures system is in fact the correct system), and
  - privacy (ensures system is protected from prying eyes)

SEAndroid

Specialized Android operating system that uses Security-Enhanced Linux (SELinux) to enforce mandatory access control (MAC) over all processes

With SELinux, Android can protect and compartmentalize system services

SEAndroid controls access to application data and system logs

Together these reduce the effects of malicious software and protect users from probable flaws in code on mobile devices

Secure Browsing

- Secure browsers will use several security features:
  - browsing privacy features and anti-tracking
  - automatic updates with vendor cloud
  - sandboxing of potentially unwanted programs (PUPs)
  - VPN integration
  - anti-phishing and ransomware protection
  - automatic HTTPS encryption (using HSTS)
  - secure "Bank Mode" that creates a virtual desktop to isolate sensitive transactions against hacks
  - Webcam cracking protections

Endpoint Detection and Response (EDR)

- Evolved from early HIDS solutions
- A "lighter" software agent installed on the host system often provides the basis for event monitoring and reporting
- EDR tools monitor endpoint and network events and send information to a SEIM system or centralized database so further analysis, investigation, and reporting can take place

Endpoint Detection and Response (EDR)

- EDR tools primarily focus on detecting and investigating suspicious activities and are indicators of compromise (IoCs) on hosts/endpoints such as
  - insider threats
  - data theft and exfiltration
  - distributed denial of service (DDoS)/botnets
  - zero-day exploits
  - web-based attacks, and
  - advanced persistent threats (APTs)

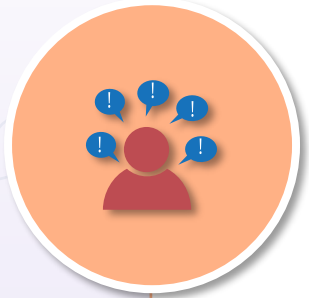
Key EDR Features

- **Filtering** – reduces alert fatigue and lowers the possibility for real threats to slip through unnoticed
- **Advanced threat blocking** – prevents threats the moment they are detected and throughout the lifecycle of the attack
- **Incident response capabilities** - threat hunting and incident response can help prevent full-blown data breaches (DLP, i.e., data loss prevention)
- **Multiple threat protection** – cloud-based visibility into many finding categories

Next-generation Endpoint Protection

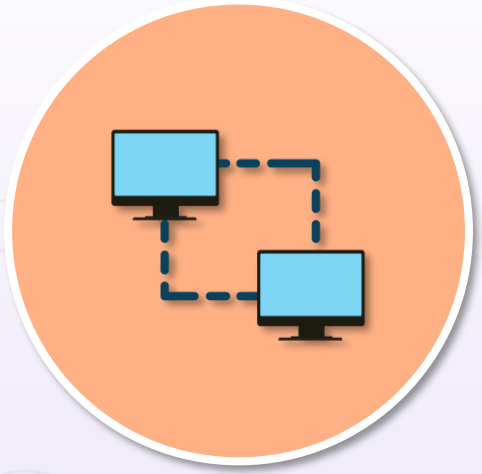
- Partner with an MSSP or CASB
- Advanced anti-virus with ML and AI
- Managed threat hunting (honey tokens)
- Cloud-based threat intelligence and User Behavioral Analytics (UBA)
- IT hygiene

Heuristics and Behavioral Analytics



- Most NGIPS and anti-virus systems use heuristic and ML mechanisms to achieve better results than traditional signature-based and anomaly-based solutions
- Heuristic engine used by an anti-malware/IPS program might include proactive rules and behavioral analytics to look for
  - a program that tries to copy itself into other programs (in other words, a classic computer virus), or
  - a program that tries to remain resident in memory after it has finished executing

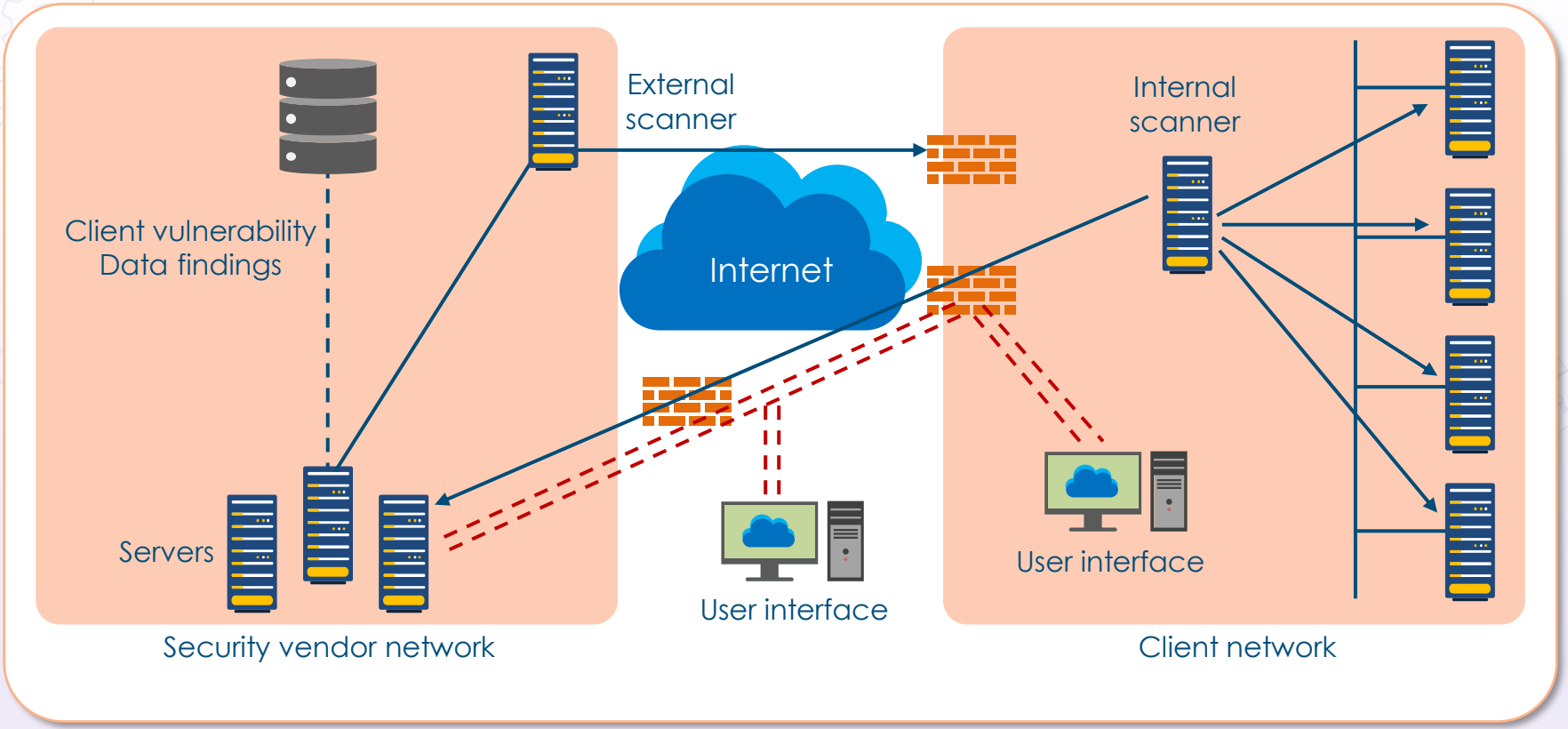
NAC and Endpoint Protection



Network Admission Control (NAC) was an industry initiative sponsored by Cisco

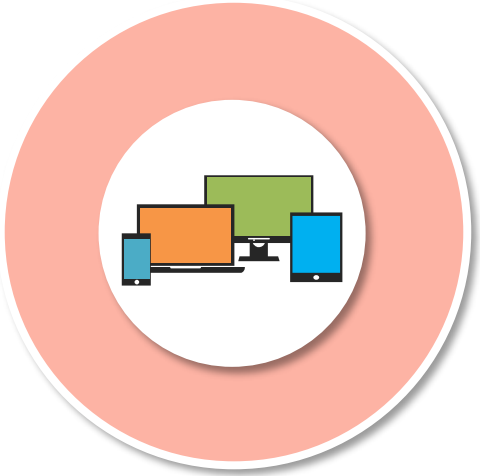
- Cisco NAC and similar technologies are officially on the exam but have been replaced by newer solutions, such as TrustSec and Zero Trust Security
- It was part of the Cisco Self-Defending Network initiative and is the foundation for enabling NAC on Layer 2 and Layer 3 networks
- Do not trust anything inside or outside the perimeter without stringent authentication and verification
- Helps secure access from users and their devices, API calls, IoT, microservices, containers (Dockers, Kubernetes,) and more

Cloud-based EDR



Mobile Deployment Models

BYOD



- **Bring Your Own Device**
- Employees are permitted to use their personal mobile devices to access enterprise data and systems
- There are four basic options:
  - unlimited access for personal devices
  - access only to non-sensitive systems and data
  - access with IT control over personal devices, apps, and stored data, or
  - access while preventing local storage of data

Mobile Deployment Models

CYOD

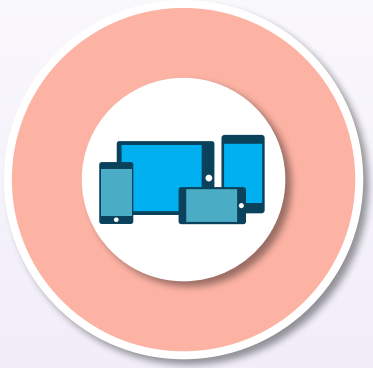
- **Choose Your Own Device**
- Much like BYOD in that it lets employees work from anywhere using a mobile device
- CYOD devices must be approved by the organization, unlike BYOD
- Users often select from a list of approved devices, which are usually smartphones
- These networks offer more stability, security, and simplified IT for most businesses

Mobile Deployment Models

COPE

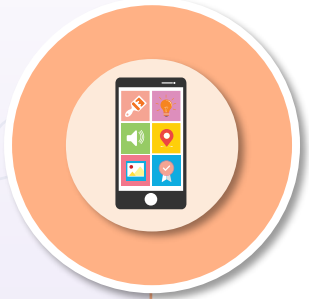
- **Corporate-owned Personally-enabled (COPE)**
- Company gives employees mobile devices
- Users can handle as if they were their own
- Prevents the need for two smartphones
- Programs should use containerization tools

Virtual Desktop Infrastructure (VDI) for Mobility Devices



- Utilizes virtual desktop interface technology
- Reduces cost/complexity and improves security and uptime
- Increased agility, as not just for smartphones (COPE)
- VDI separates the app and the data
- Tablets using a separate Bluetooth-enabled keyboard

Enterprise Mobility Management (EMM)



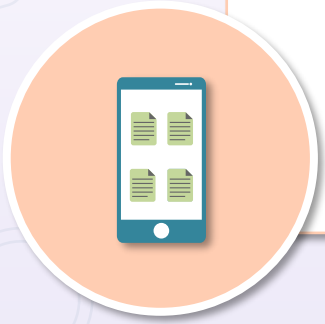
- Organizations must securely configure and implement each layer of the technology stack, including mobile hardware, firmware, O/S, management agent, and the apps used for business
- Solution should reduce risk, so employees are able to access the necessary data from nearly any location, over any network, using a wide variety of mobile devices
- Enterprise mobility management is the combination of mobile device management (MDM) and mobile application management (MAM)

Mobile Device Management (MDM)

- Organizations must securely configure and implement each layer of the mobile technology stack, including hardware, firmware, O/S, management agent, provider agreements, and apps used for business
- The solutions should reduce risk while enabling employees to access applications and necessary data from nearly any location, over any network, using a wide variety of mobile devices in some cases
- Enterprise mobility management (EMM) = mobile device management (MDM) + mobile application management (MAM)

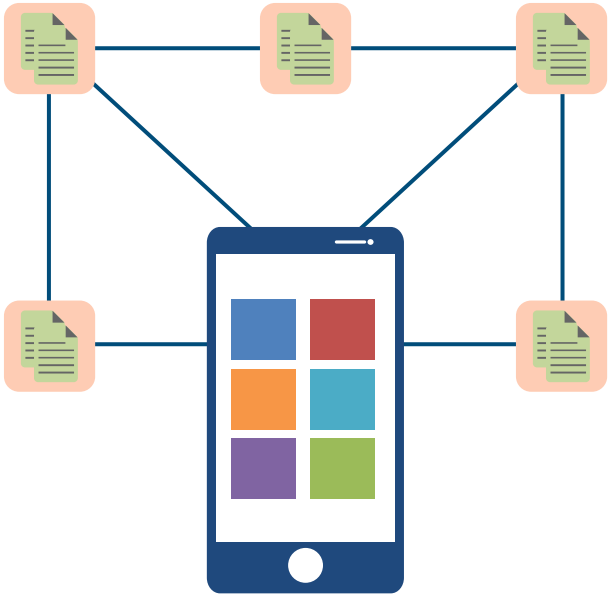
Enterprise Mobility Management (EMM)

- There are three basic core competencies that all organizations need from an EMM solution:
  - **Visibility**: understanding what's running on mobile devices is the key to discovering potential risks and adhering to compliance policies
  - **Secure access**: providing the ability for mobile users to securely authenticate and authorize access to apps and data
  - **Data protection**: offering dynamic anti-malware and data loss prevention capabilities to help limit the risk of attacks and data breaches



Mobile Device Management (MDM)

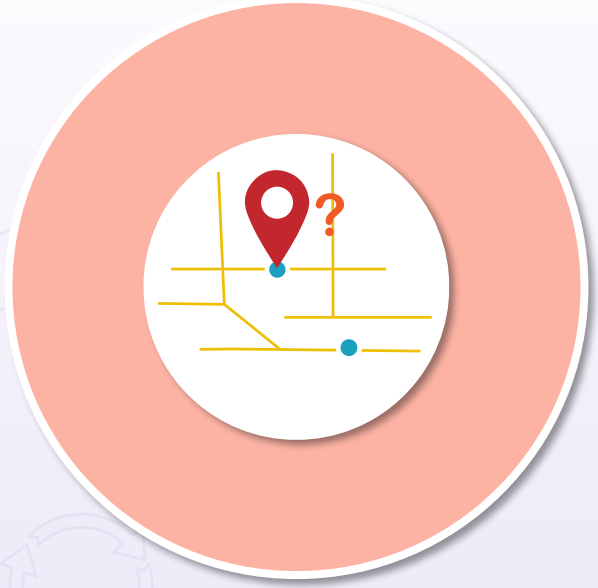
- Technology to enable the management and control of mobile devices used to access business resources
  - Enrolling devices for management
  - Provisioning settings, like digital certificates and profiles
  - Monitoring, measuring, and reporting device compliance
  - Removing corporate data from devices (data leak prevention)
- Some activities are network access control, preadmission control, remote lock and wipe
- Other features that can sometimes be attributed to MDM platforms are remote virtual private network (VPN) capabilities



Common MDM Activities

- Onboarding, offboarding, and installing certificates
- Implementing touch ID authentication and screen locking
- Configuring PINs and push notifications for user devices
- Deploying and managing full device encryption
- Finding lost devices and remote wiping

Geofencing and Geolocation

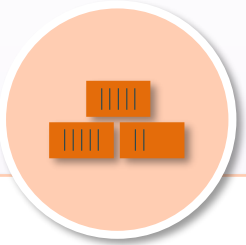


- Geofencing and geolocation services allow IT to physically track mobile devices
- Geolocation is a point on a map whereas geofencing is a square area on the map also known as GPS tagging
- Administrators can use geolocation to find a lost or stolen device and geofencing to determine when a device moves in and out of a certain (secure) area

Mobile Biometrics

- Toshiba introduced fingerprint scanning in 2007
- Apple brought Touch IDs for 5S in 2013
- Fingerprint recognition is the most popular
- Voice recognition and iris scanning are emerging
- Electroencephalogram reading and pattern swipe are future technologies

Advanced MDM

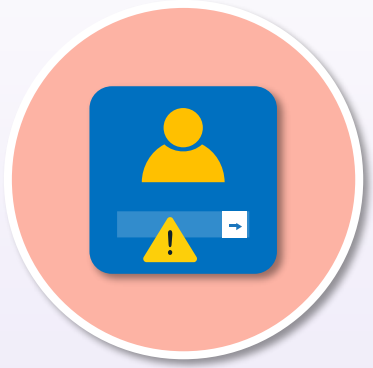


Containerization is orchestrating the packaging, isolation, and encapsulation of apps and work data in a separate segmented user space within the device

Storage segmentation involves partitioning various types of data on devices to protect IP, PII, and PHI and support DLP initiatives

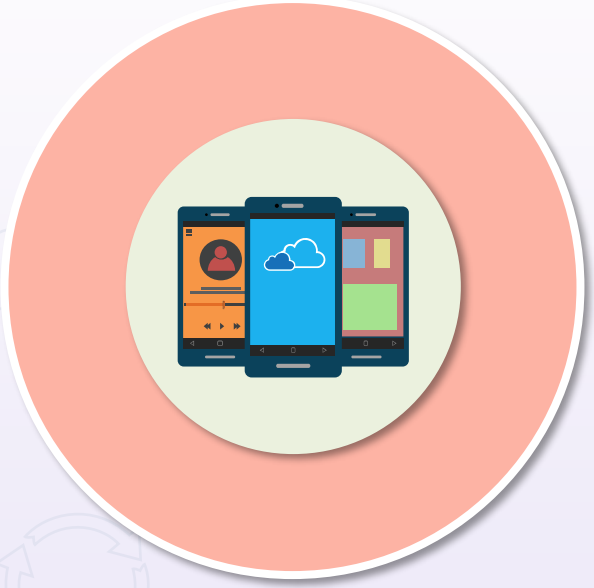
Full Device Encryption (FDE) is strong encryption at the hardware level on a smartphone or other device beyond the control of the user

EMM Challenges



- Managing X509v3 certificates
- Tethering and tokenization (used as MFA factor)
- Mobile payments and cybercurrency wallets (also NFC-enabled)
- OEM and carrier fragmentation
- Unauthorized remote locking and wiping

Mobile Application Management (MAM)



- Involves publishing mobile apps to users
- Continual monitoring, configuration, and updating of apps
- Mobile managers will report on app inventory and usage
- Securing and removing corporate data within mobile apps
- Also involves mobile content management

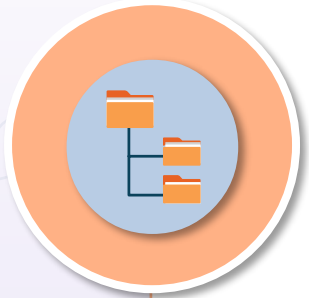
MAM Data Privacy Concerns

- Data storage and remnants
- Non-removable storage
- Removable storage
- Transfer/back up data to uncontrolled cloud storage
- Intellectual property and corporate data leakage

Jailbreaking

- Jailbreaking and rooting are very different, even though they both involve privilege escalation
- Jailbreaking an iPhone basically allows the installation of third-party apps not approved by Apple's strict controls
- You cannot modify the OS or system files like an administrator, and you're still bound by the iOS framework
- A jailbroken iPhone can be reverted back to a standard 'jailed' device by restoring the device in Recovery Mode
- Apple has responded with patching exploits and upgrading hardware to iOS

Rooting



- Rooting grants full access to a device on a level much higher than jailbreaking, giving access to the Android system and beyond
- Every line of code in the Linux-based device becomes editable, with options only restricted by coding skills
- Since Android is open source, you can go into recovery mode and download a modified or even entirely new version of the OS if you want
- You can alter any and all hardware, software, or aesthetic settings on the device

Sideloading

- Sideloading basically refers to the moving of media files to a mobile device using USB, Bluetooth, or Wi-Fi
- It can also involve writing to a memory card to insert into a mobile device
- With Android apps, sideloading usually installs an app package in APK format onto a device, with packages typically downloaded from sites other than Google Play
- Sideloading of apps is only likely if the user has allowed "Unknown Sources" in their security settings

MDM vs. MAM in a Nutshell

MDM

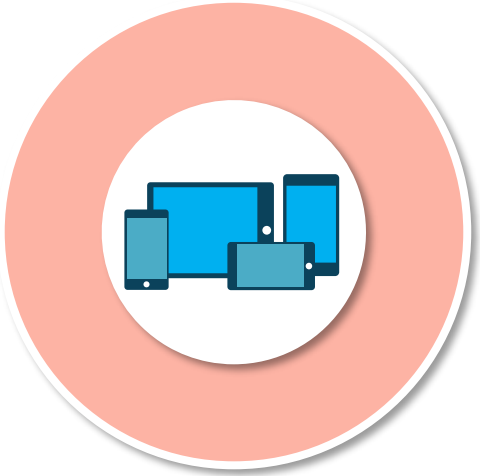
- Enrolling devices for management
- Provisioning settings, like digital certificates and profiles
- Monitoring, measuring, and reporting device compliance
- Removing corporate data from devices (data leak prevention)

MAM

- Publishing mobile apps to users
- Configuring and updating apps
- Reporting app inventory and usage
- Securing and removing corporate data within mobile apps

Modern EMM Attributes

MobileIron, AirWatch, and XenMobile



- Offer BYOD and MAM security capabilities
- Provide flexible bundles for different use cases
- Unified endpoint management
- End-to-end security and identity management (IdM)
- Enterprise integration
- Productivity applications that enable the creation of mobile business apps without writing code
- Introduce User Behavioral Analytics (UBA)