Welcome back to the Security+ Bootcamp

Your instructors:

Michael J Shannon

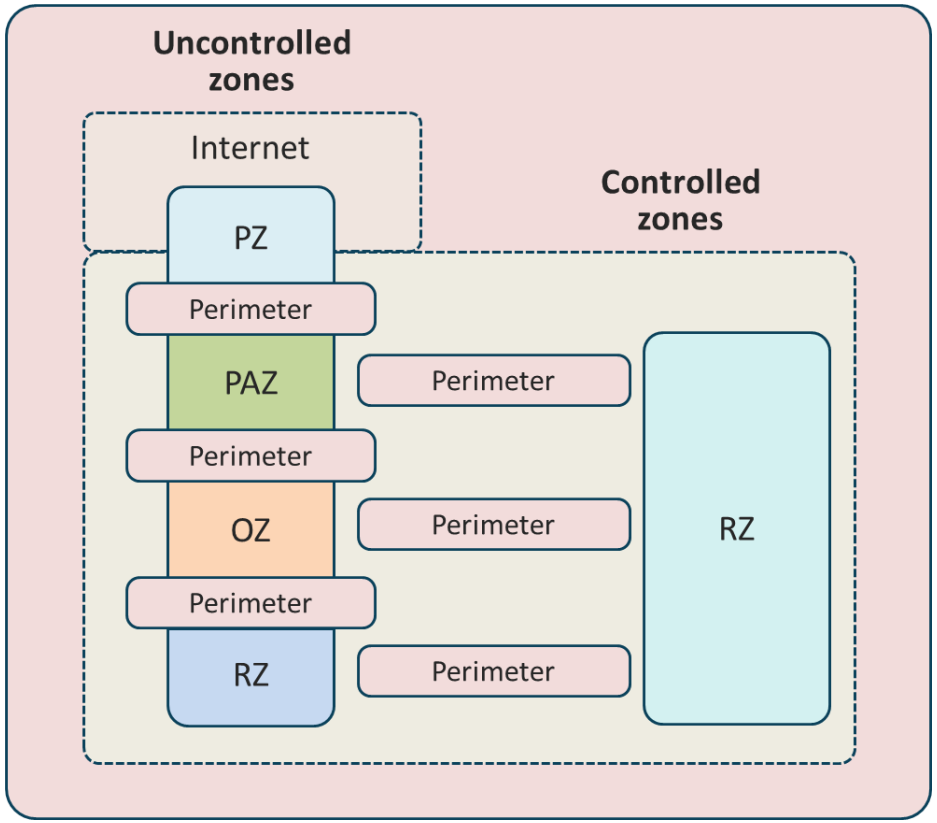
and

Carl Mullin

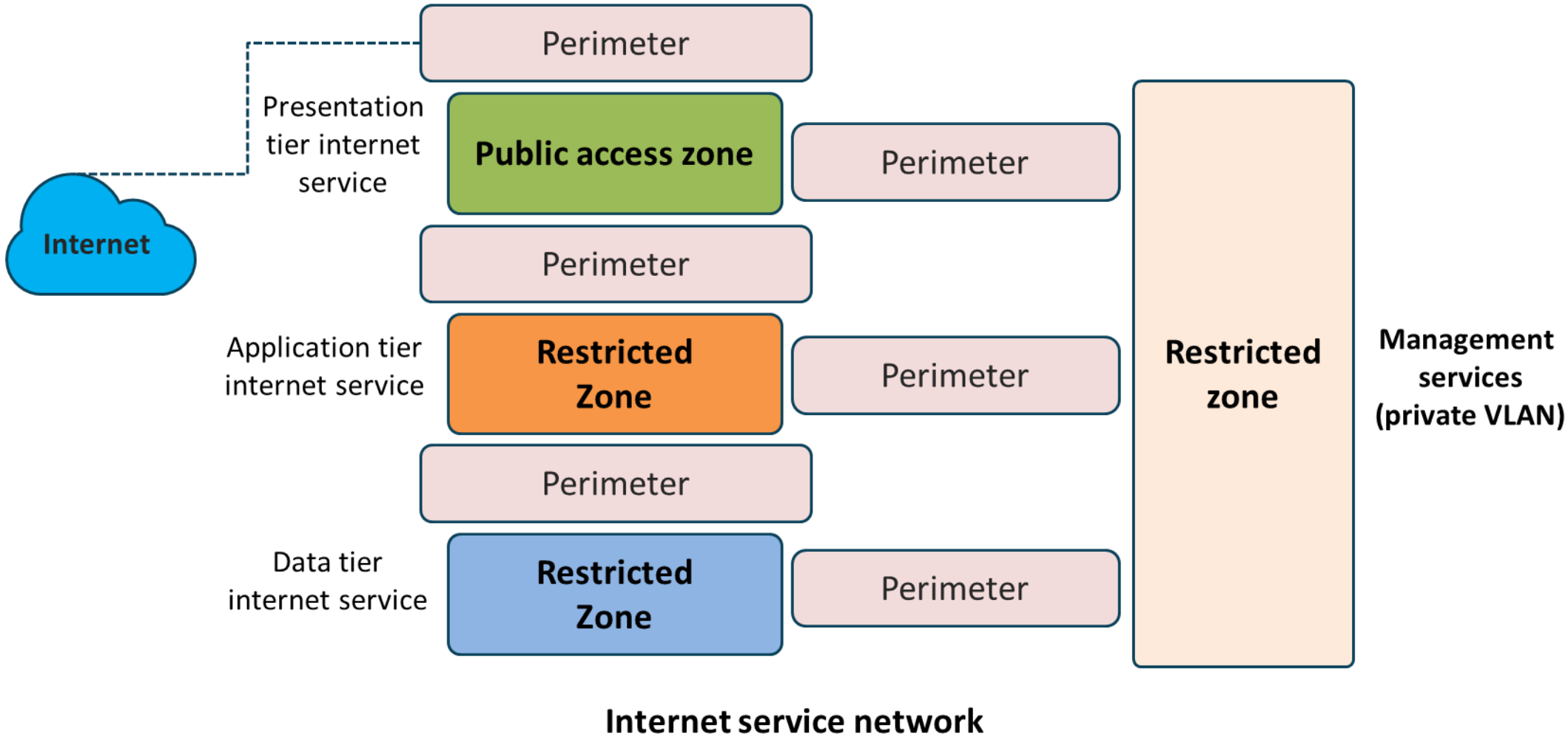
Class will begin at 10:00 A.M. Central Standard Time (CST)

Segmentation and Zoning

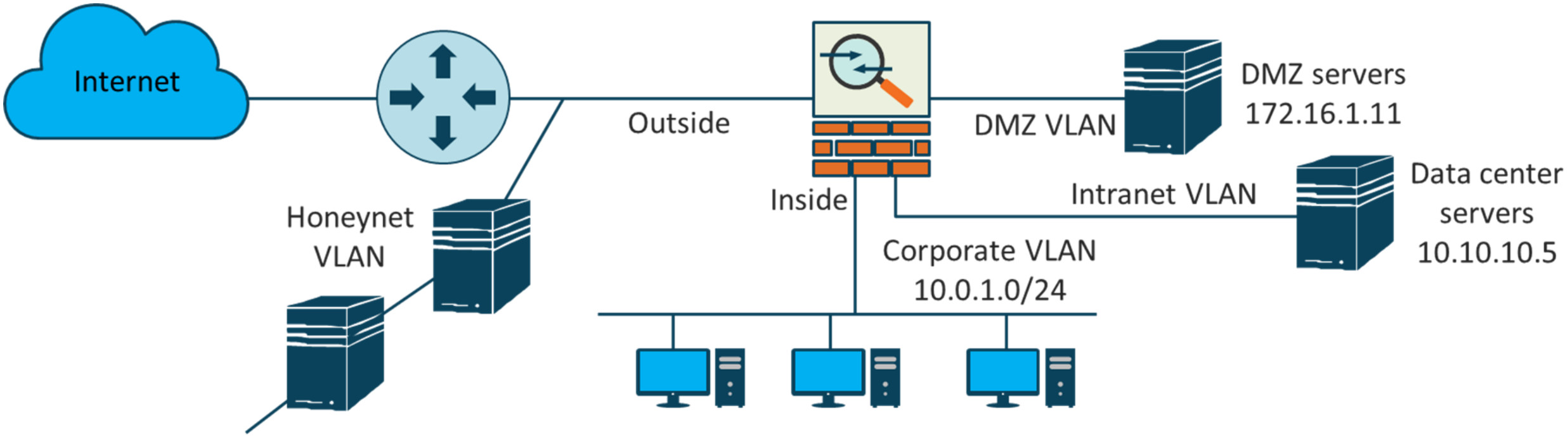
- Zoning is used to mitigate the risk of an open network by segmenting infrastructure services
- Zoning is a logical design approach used to control and restrict access
- Each zone has fundamental characteristics, defined by the security
  - Every zone contains one or more separate, routable networks
  - Every separate, routable network is contained within a single zone
  - Every zone connects to another zone via a perimeter that contains zone interface points (ZIPs)
  - The only zone that may connect to the public zone is the PAZ (DMZ)



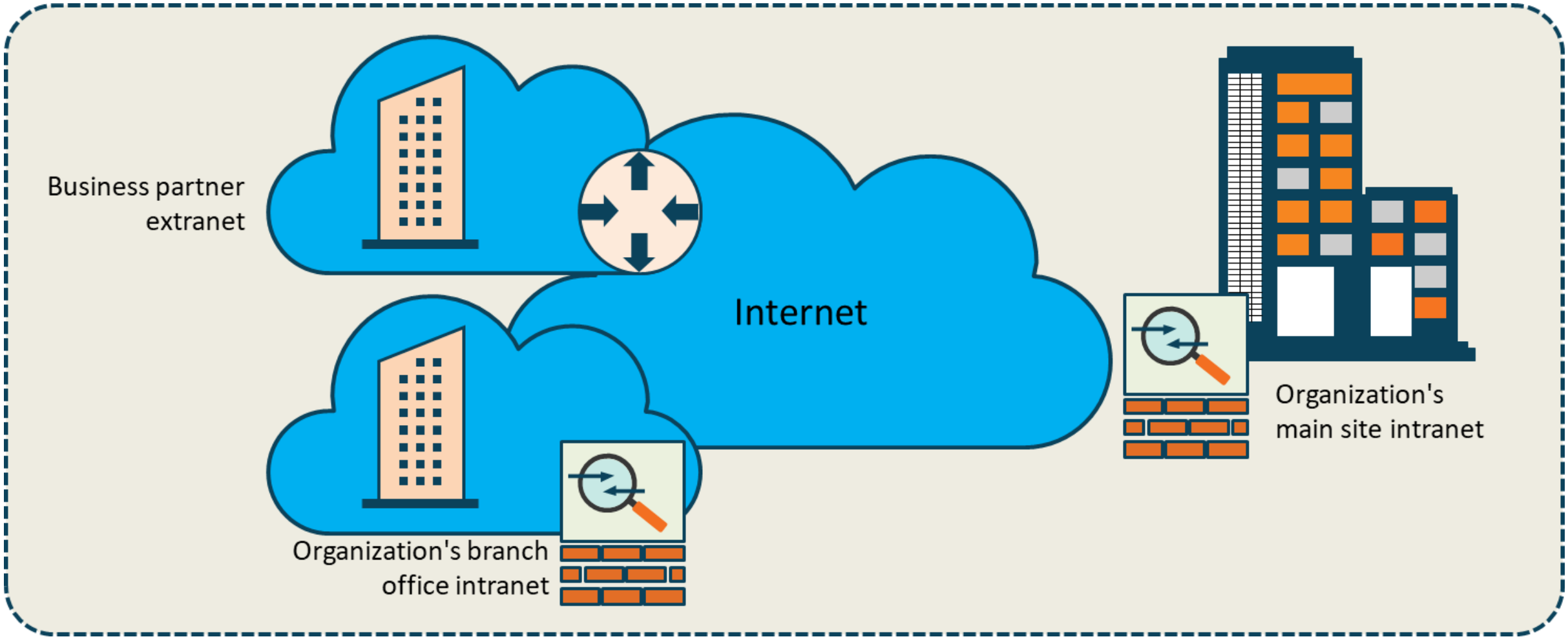
Segmentation and Zoning



Zones and VLANs

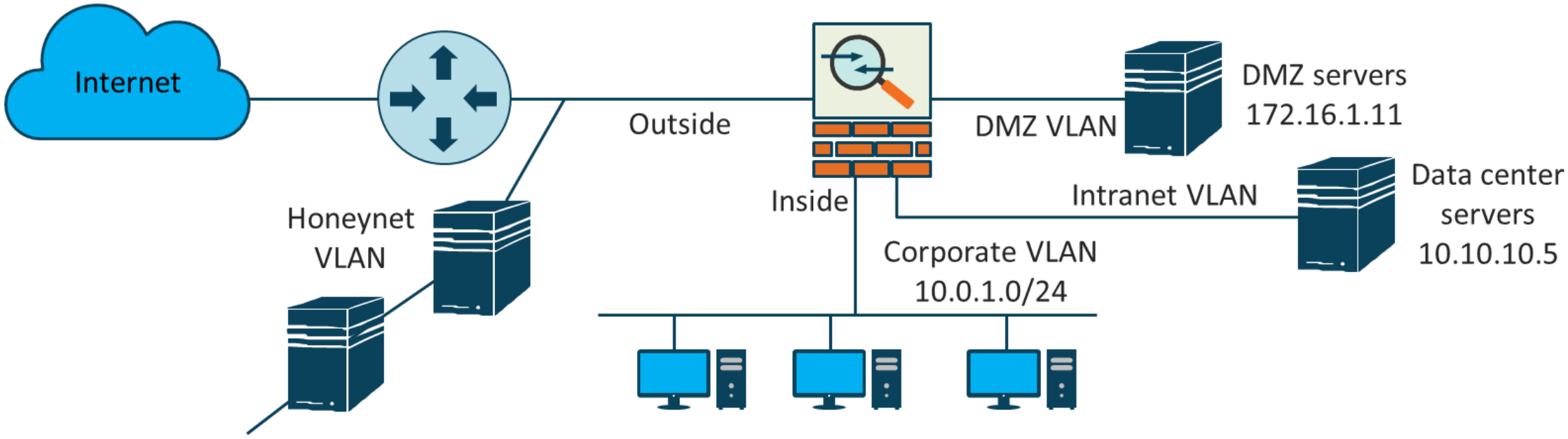


Extranets


Business partner
extranet
Internet
Organization's
main site intranet
Organization's branch
office intranet

Honeypots and Honeynets

- Honeypots and honeynets are isolated systems, sites and services with data that appear to be valuable to an attacker
  - Entice malicious users to connect
  - Track and log all traffic to and from the honeypot
  - Run IDS services and other next-generation cloud-based analysis

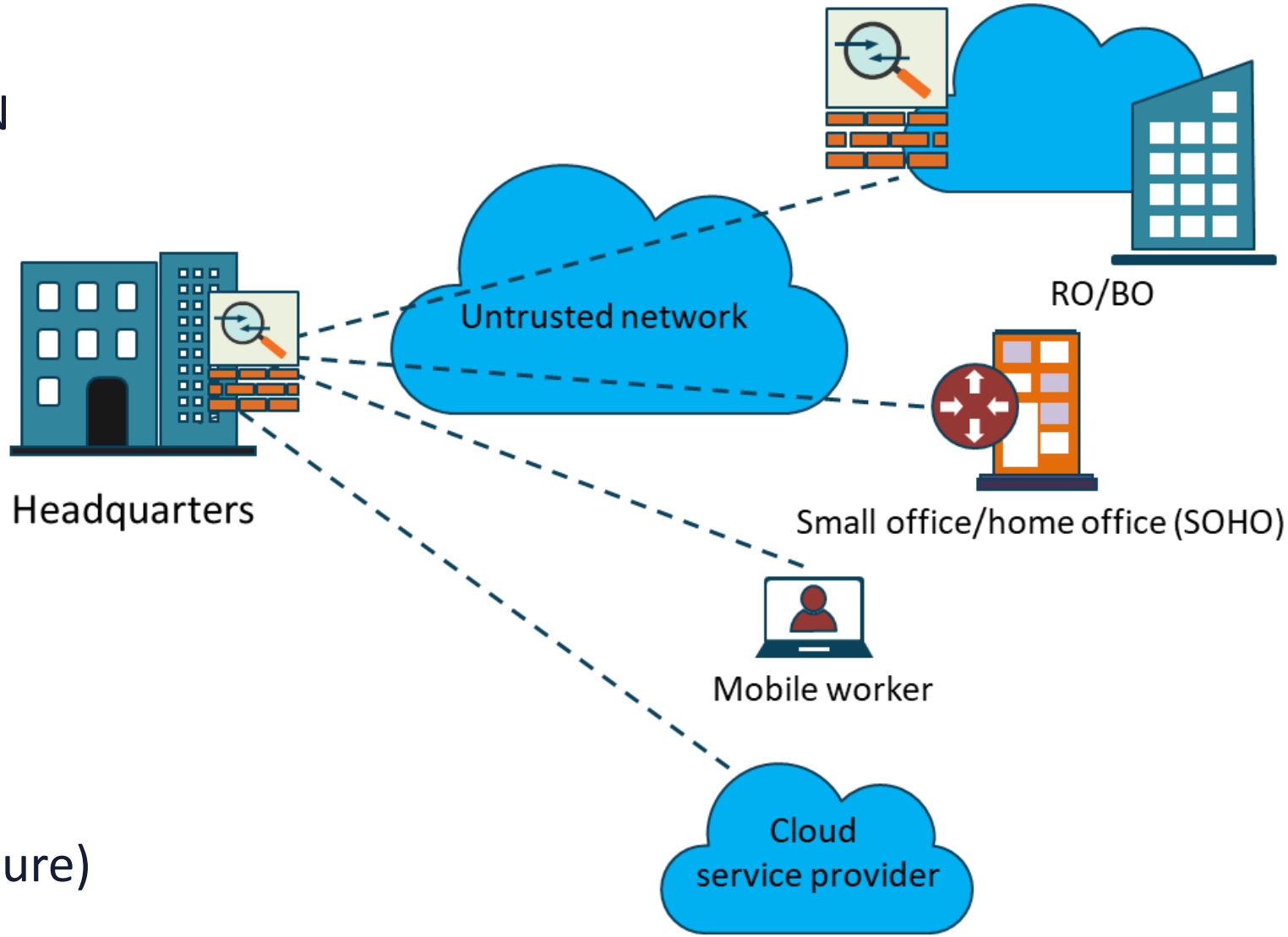


Virtual Private Networks (VPNs)

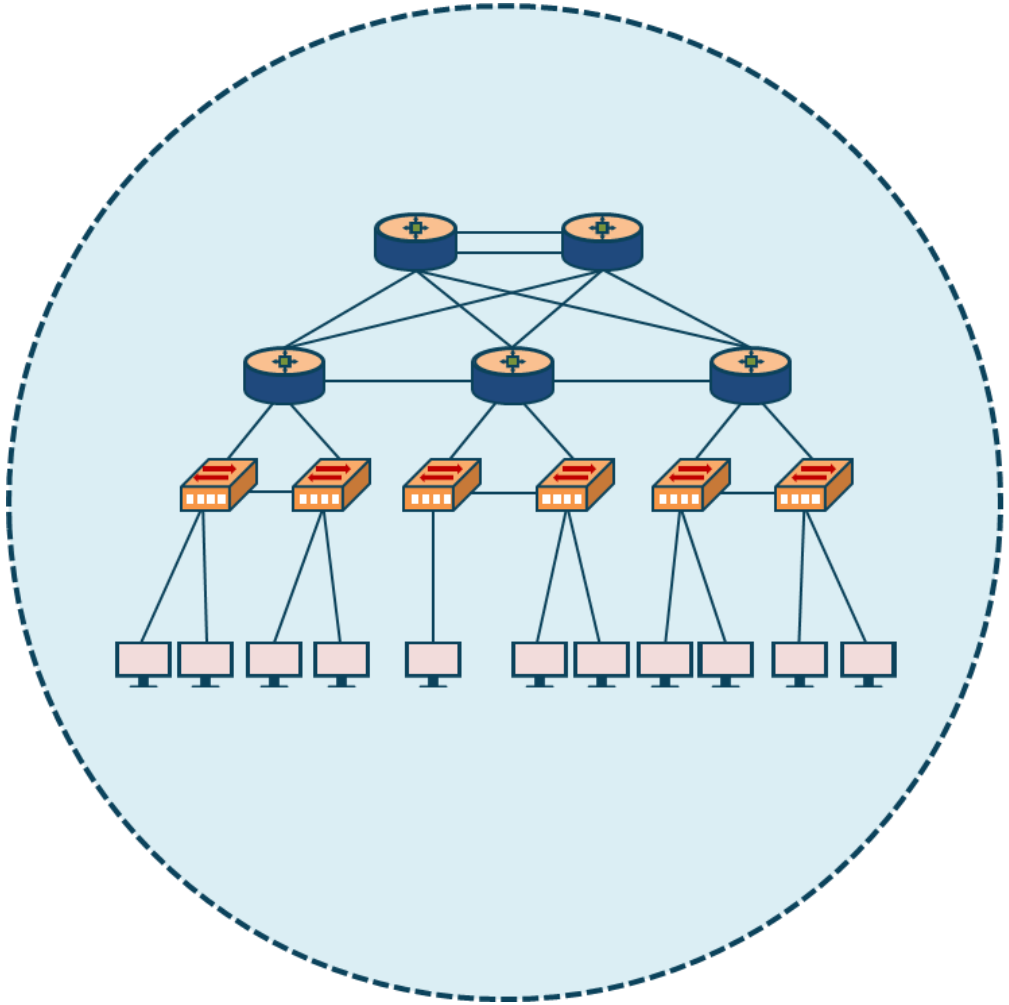
- VPN gateways are dedicated termination points (concentrators) for site-to-site and remote-access VPNs
- They can support IPsec IKE v1, IKE v2, and SSL/TLS protocol suites
- VPNs can be server or appliance-based and physical or virtual
- Routers and firewalls are common VPN gateways

VPN Connections

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



Switch Port Security



- Switches function at layers 2-4 with extensive capabilities and flexibility
- Access switches and aggregate (multi-layer) switches are common
- Can be physical or virtual (SDN)
- Switch port security should be a base configuration for MAC filtering

Switch Security Features

- Loop prevention, flood guard with BPDU, and root guard configurations
- DHCP 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
- 802.1X PNAC offers EAP-TLS, PEAP, and EAP-FAST
- MACsec offers AES-GCM-128/256 with GMAC

Switch Port Security

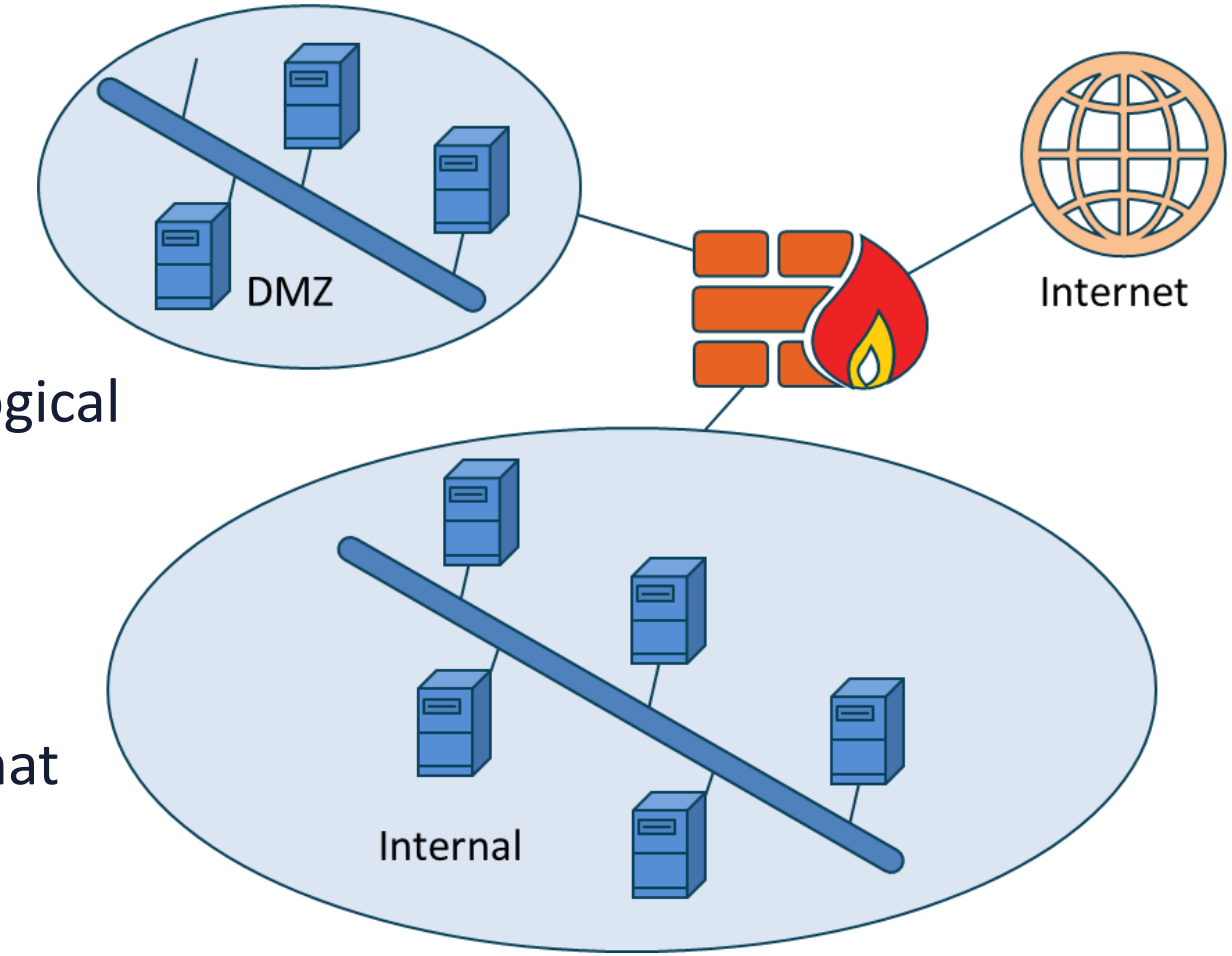
```
Switch (config-if)#switch
Switch (config-if)#switchport access vlan 500
Switch (config-if)#switchport po
Switch (config-if)#switchport port-security?
           aging       Port-security aging commands
           mac-address Secure mac addresses
           maximum     Max secure addresses
           violation   Security violation mode
           <cr>

Switch (config-if)#switchport port-security violation?
      protect  Security violation protect mode
      restrict Security violation restrict mode
      shutdown Security violation shutdown mode

Switch (config-if)#switchport pro
Switch (config-if)#switchport port protected
```

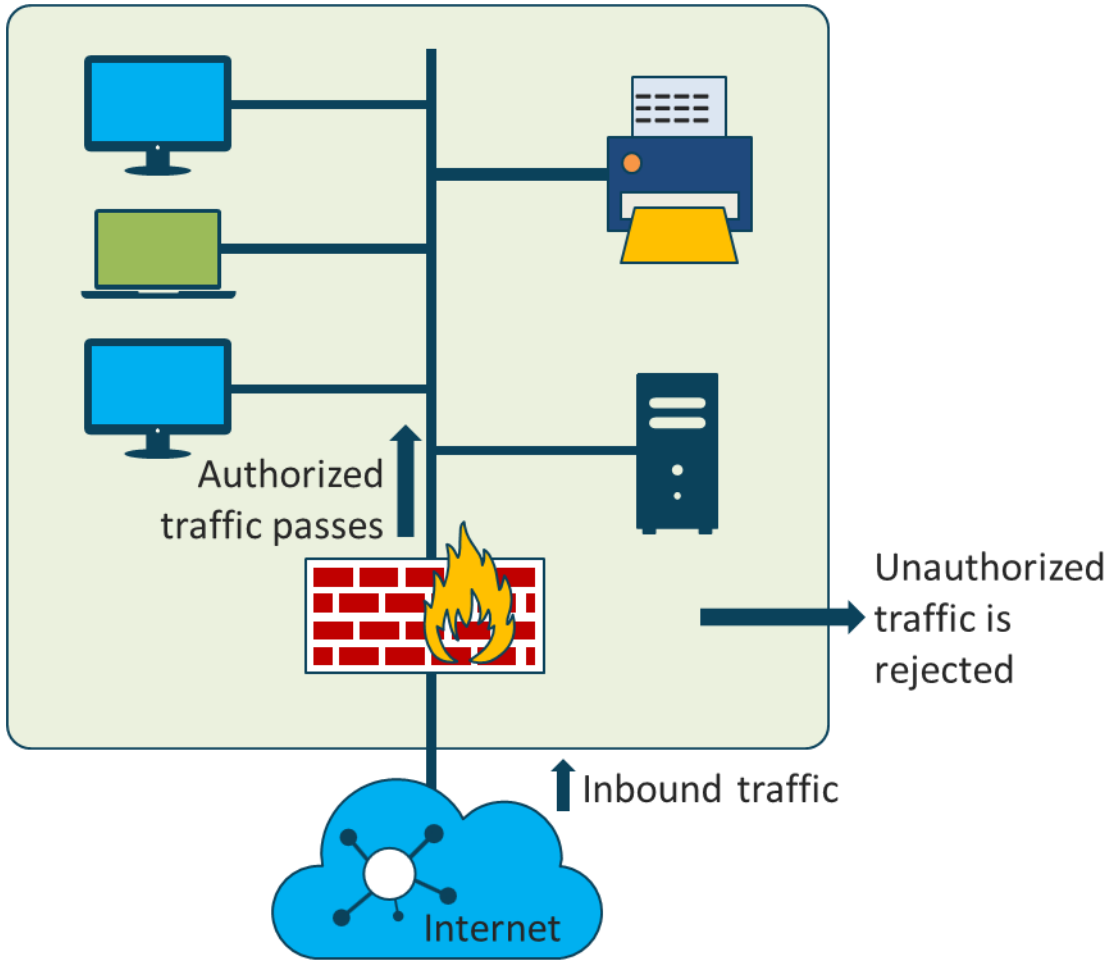
Firewalls

- Firewalls are integrated systems of threat defense, functioning at layers 2-7
- They should be placed between all zones, domains, and partitions either physical or logical
  - Network or application firewalls
  - Restrictive vs. permissive firewalls
  - Stateless vs. stateful firewalls
- Classic FWs use ACLs and inspection rules that are interface-based
- Can also be VPN and NAT Gateways



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 Firewalls (WAF)

- An appliance, server plugin, or CSP service that applies a set of rules to an HTTP/S connection
- WebACLs filter for common attacks, such as:
  - Cross-site scripting (XSS)
  - SQL injection
  - Cross-site request forgery (CSRF)
  - Buffer overflows
  - DDoS and botnets
  - Custom WebACL rules

Network Appliances

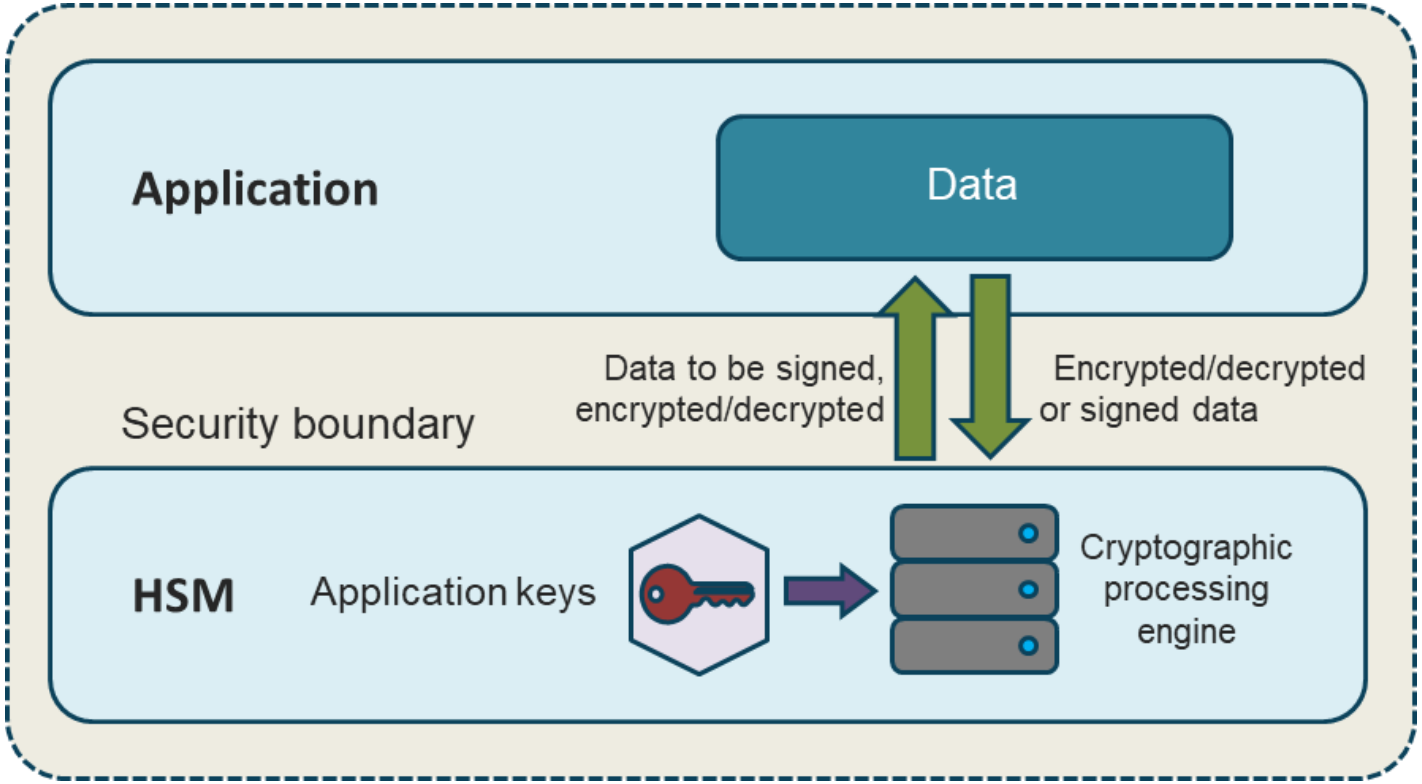
- Network Admission Control (NAC)
- Bastion or jump hosts
- Proxy servers
- Network IPS sensors
- Port mirroring/spanning taps
- Advanced malware control
- VPN gateways
- Threat modeling with machine learning
- SIEM appliances
- NetFlow collectors

Database Activity Monitoring (DAM)

- A suite of tools used to identify and report on fraudulent, illegal, or other undesirable behavior concerning data
- A DAM system should have minimal or no impact on user operations and productivity
- Modern solutions deploy a comprehensive toolkit for visibility, discovery and classification, vulnerability protection, application-level analysis, intrusion prevention, support for unstructured data security, identity and access management integration, and risk management support

Hardware Security Modules (HSM)

- Use tamper-proof, hardened devices
- Provide crypto processing
- Protect cryptographic functions
- Secure cryptographic keys
- Separate administration and security domains
- Apply key use policies
- Can be used in place of software crypto libraries



Wi-Fi Protected Access (WPA)

The transitory replacement for WEP

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

Wi-Fi Protected Access 2 (WPA2)

The replacement for WPA (2004)

- Devices require testing and certification from Wi-Fi Alliance (2006)
- Uses CCMP for encryption
- Supports PSK and enterprise authentication

Counter Mode With Cipher Block Chaining (CCMP)

Part of 802.11i wireless standard

Designed for WiMAX technology

Algorithm based on Advanced Encryption Standard (AES)

Uses 128-bit keys and a 48-bit IV for replay attacks

Includes a MAC for data integrity and origin authentication

802.11 EAP Variants

802.1x EAP types feature / benefit	MD5 --- Message digest 5	TLS --- transport level-security	TTLS --- Tunneled transport-level security	PEAP --- Protected transport-level security	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	Easy	Difficult (due to client certificate deployment)	Moderate	Moderate	Moderate
Wi-Fi security	Poor	Very high	High	High	High

WPA3

The replacement for WPA2

- 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

The replacement for WPA2

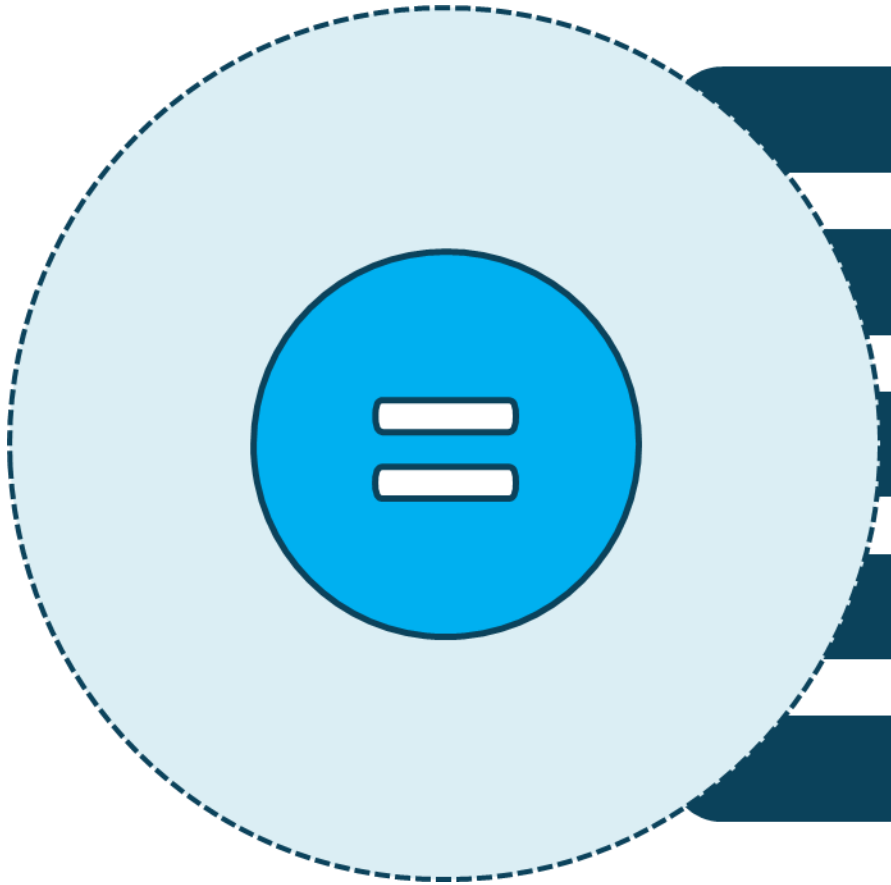
- Authenticated encryption - GCMP-256
- Key derivation and confirmation - 384-bit HMAC with Secure Hash Algorithm (HMAC-SHA384)
- Key establishment and authentication – ECDH exchange and ECDSA using a 384-bit elliptic curve
- Robust management frame protection - 256-bit Broadcast/Multicast Integrity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

WPA3 Personal

The replacement for WPA2 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

Wi-Fi Protected Access (WPA2) Modes

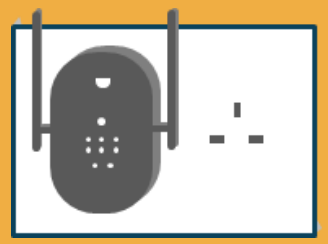
WPA-PSK (Personal)

- 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 variants
- AES used for encryption

Wi-Fi Protected Setup (WPS)

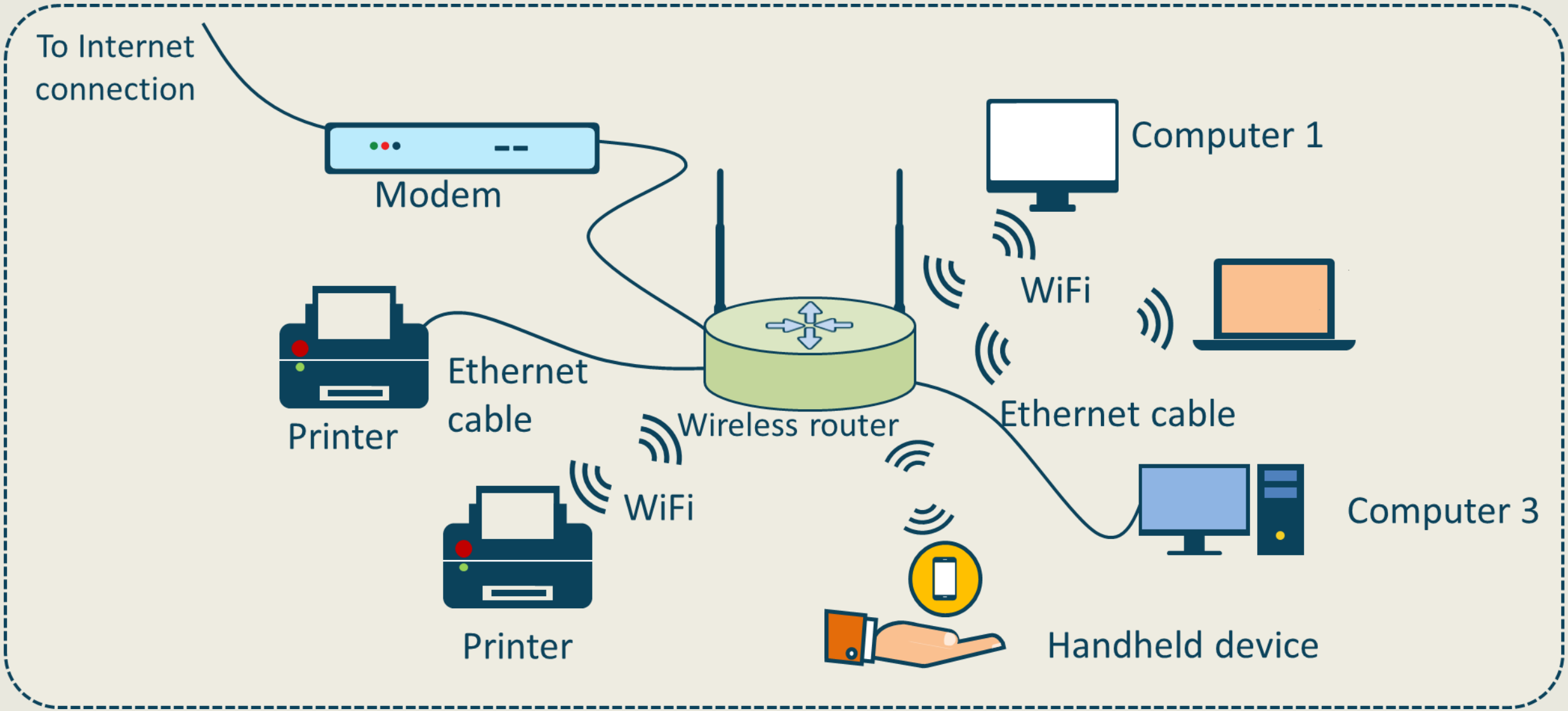


- Wi-Fi Alliance standardized method for simplifying station setup and initial configuration previously called Wi-Fi Simple Config
- Newer wireless routers are less vulnerable
- This program is not part of WPA2, and this feature should be avoided and turned off due to many known weaknesses and attacks against it
- Should never be used in the enterprise

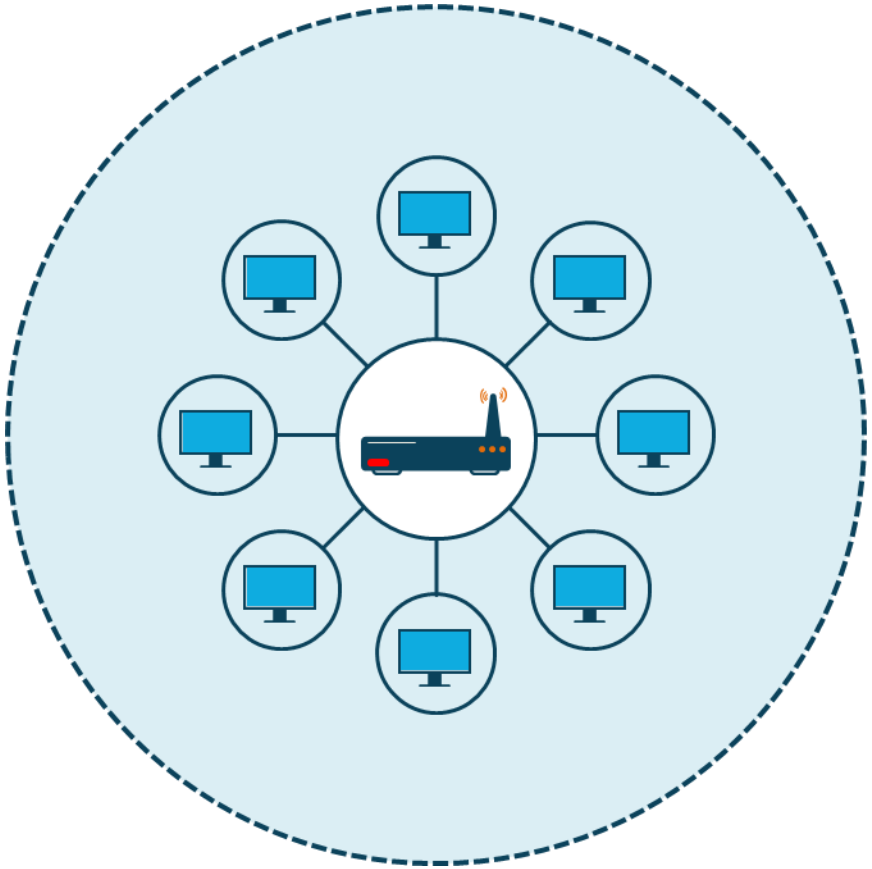
Wireless Captive Portals

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

Wireless LANS



Wireless Installation Considerations



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

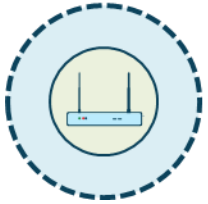
Wireless Installation Considerations

Conducting site surveys with scanners and analyzers

Presenting visual heat maps and topologies

Analyzing power outputs and interference

Designing the channel overlays and DHCP roaming



Strategically placing WAPs and internal/external antennas

Cellular Technologies

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

5G

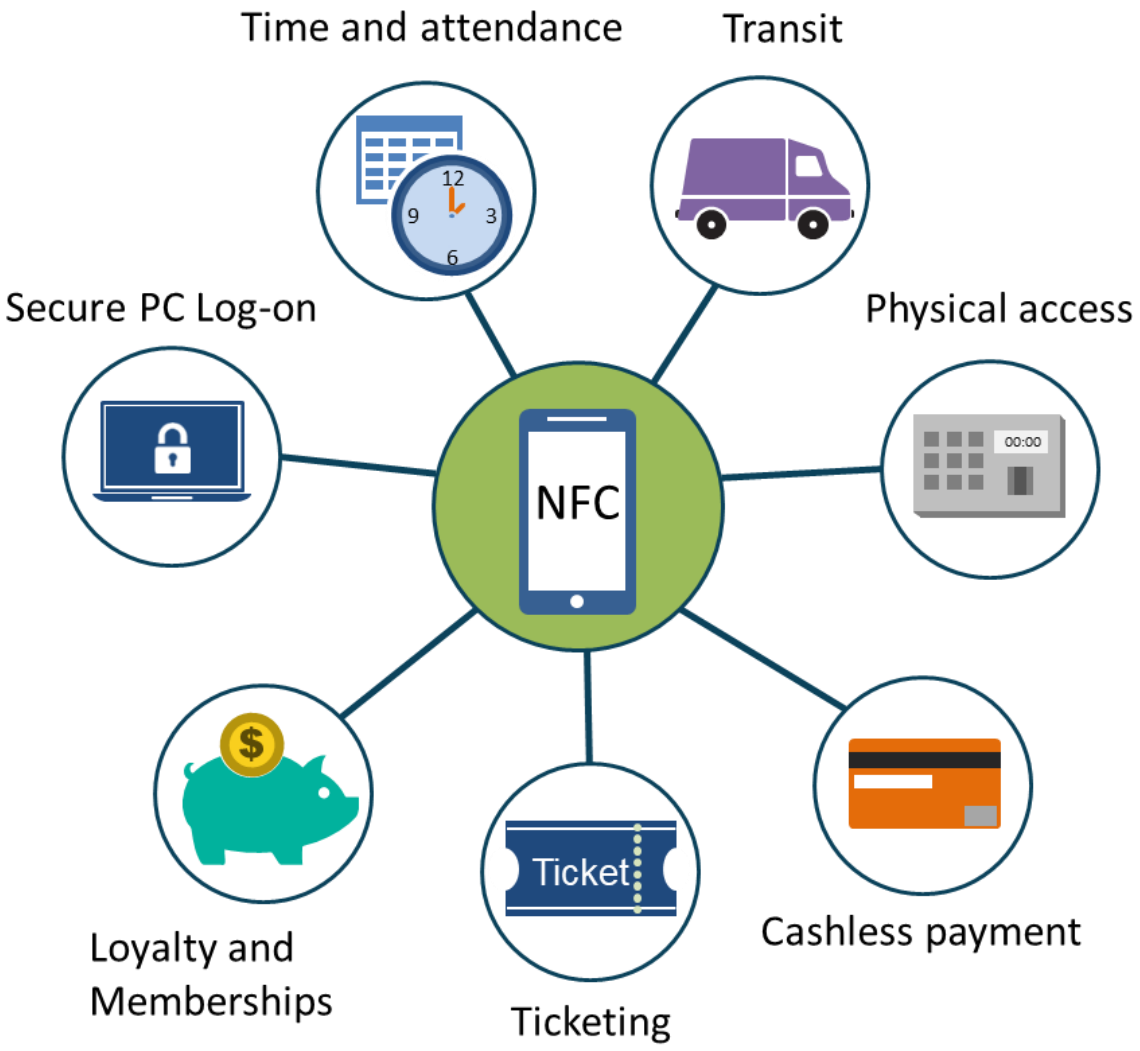
- The fifth generation of wireless cellular mobile networking
- All 5G devices in a cell are linked to the Internet and telephone network by radio waves through a local antenna in the cell
- The goal is to deliver bandwidths up to 10 Gbps by using higher-frequency radio waves than current cellular networks

Bluetooth

- Method of creating personal area networks (PAN) with many applications
- Telephones, speakers, tablets, media players, robotics systems, handheld, 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

RFID and NFC

- The benefits of rapid and contactless payments and entry/exit without long waiting times are very tempting
- RFID technology digitally encodes data in RFID tags or smart labels that are captured by a reader through radio waves
- 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

Infrared

- One of the most common uses of infrared radiation is in heat-sensitive thermal imaging cameras and night-vision systems
- Used in wireless communications, monitoring, and control applications
- Common uses are home-entertainment remote-control boxes, WLANs, links between laptops and PCs, cordless modems, intrusion and motion detectors, fire sensors, medical diagnostic equipment, missile guidance systems, and geological monitoring devices

Infrared Communication

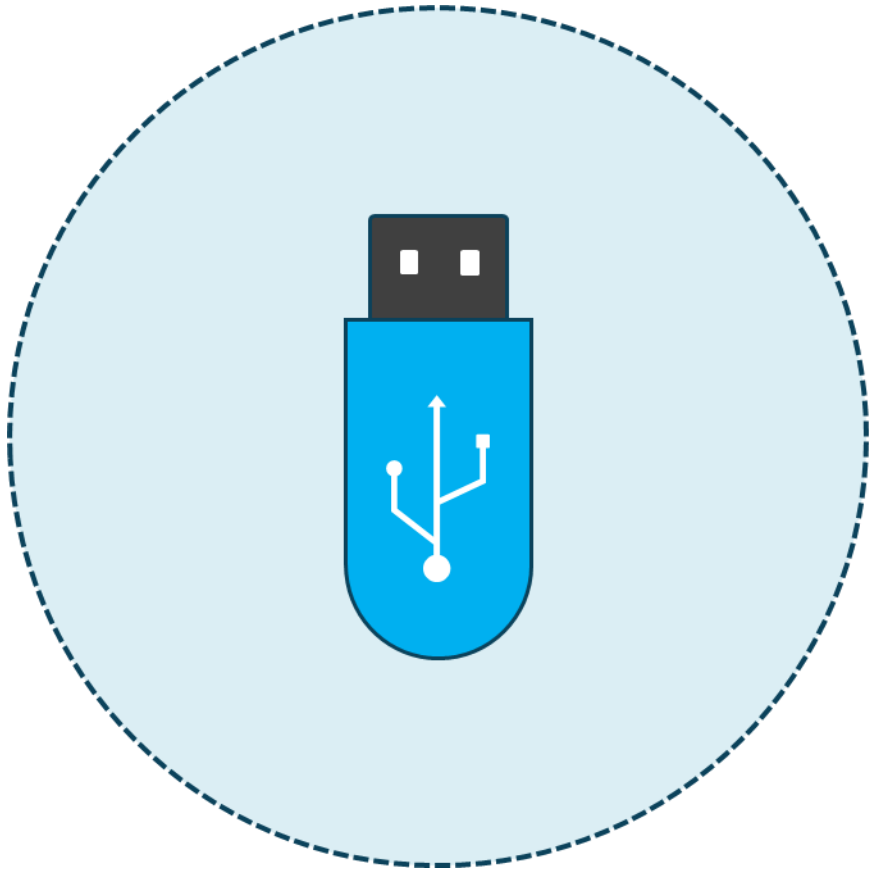
Point-to-point

- P2P needs a line of sight between the transmitter and receiver, as in remote control communication
- Transmitting IR data between devices is also called beaming

Diffuse

- Diffuse does not require line of sight
- The link between the transmitter and receiver is preserved by reflection off surface's wireless LAN communication system

Wireless USB



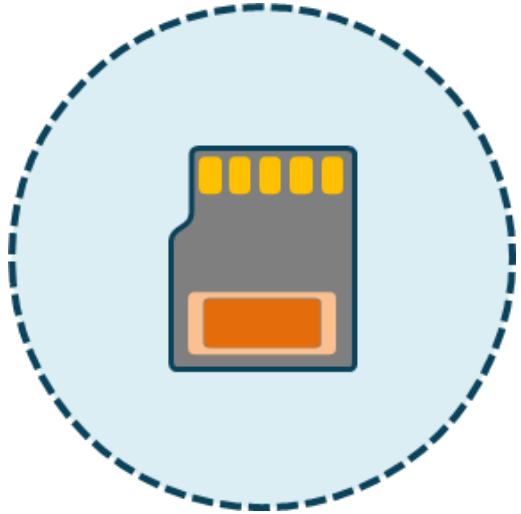
- A high-bandwidth wireless radio communication PAN protocol
- IPv6 is integrated into this technology
- Maintained by the WiMedia Alliance
- Sometimes abbreviated as "WUSB"

Global Positioning System (GPS)

- Each GPS satellite transmits data on two frequencies, L1 (1575.42 MHz) and L2 (1227.60 MHz)
- Satellites carry unwavering atomic clocks that are synchronized with each other and ground clocks
- Many applications use one or more of GPS's three basic components: absolute location, relative movement, and time transfer
- Geofencing and geotagging are exam-relevant uses

MicroSD HSM

- A lightweight HSM in a MicroSD card commonly used with Android devices
- Used to remotely generate, backup, restore, and utilize RSA and ECC cryptographic keys
- These are becoming more popular as people store and use cryptocurrencies with secure mobile wallets



SEAndroid

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

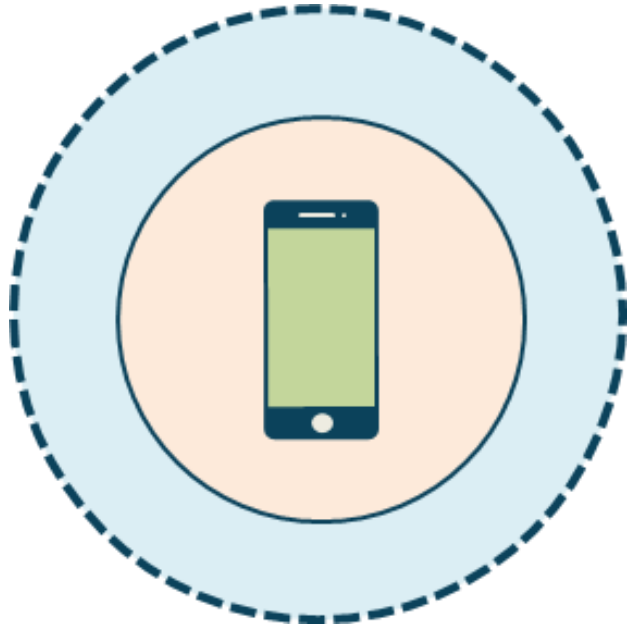
With SELinux, Android can protect and compartmentalize system services, and control access to application data and system logs

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

Bring Your Own Device

BYOD

- 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
  - Access while preventing local storage of data



Choose Your Own Device

CYOD

- CYOD is like BYOD in that it lets employees work from anywhere using a mobile device
- CYOD devices must be approved by the organization, as opposed to 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

Corporate-owned Personally-enabled

COPE

- With COPE, the company gives employees mobile devices
- Users can handle as if they were their own
- This policy prevents the need for two smartphones
- COPE programs should use containerization tools to maintain a separation between personal and work data and applications.

Virtual Desktop Infrastructure for Mobility Devices

Utilizes virtual desktop interface technology

Reduces cost/complexity and improves security and uptime

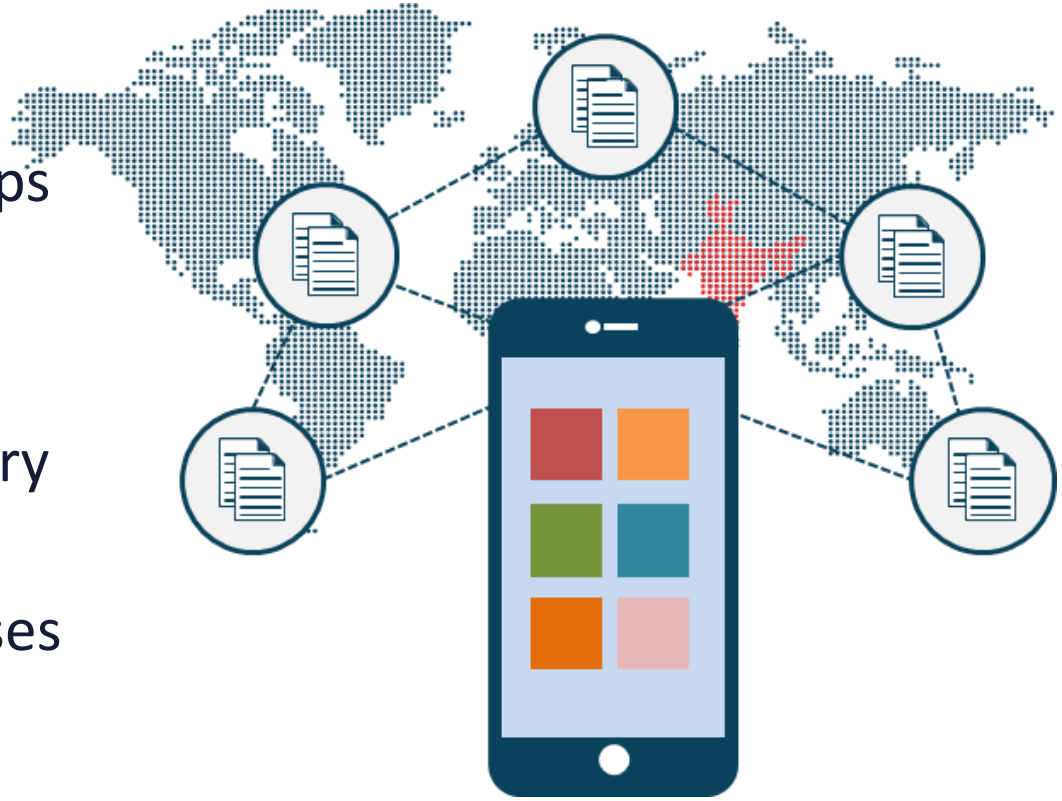
Increased agility, as not just for smartphones (COPE)

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 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 the 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)



MDM vs. MAM

Mobile device management (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)

Mobile app management (MAM)

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

Common MDM Activities

Finding lost devices and remote wiping

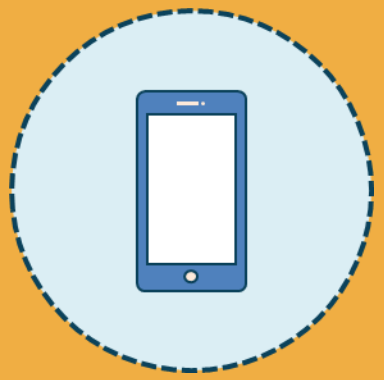
Implementing touch ID authentication and screen locking

Configuring PINs and push notifications for user devices

Deploying and managing full device encryption

Onboarding, offboarding, and installing certificates

Mobile Content Management



- Also called mobile information management (MIM)
- Falls under the umbrella of EMM
- In a large enterprise can be separate from MDM, MAM, and mobile security management (MSM)
- Well-designed mobile content initiatives allow users to access mission-critical data securely
- Users can collaborate with other employees on any network or device without work-critical data access restriction

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 device management (MDM) systems have added these features for the enterprise

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

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

Mobile Sandboxing

- Containerization and sandboxing provide protection, isolation, and integrity functionality for better levels of overall data isolation
- Containerization is usually a MAM technique that limits the environments in which certain code can run
- Users can continue to chat, text, and tweet without affecting business functions, since sensitive apps and data remain protected within sandboxed containers with separate controls and higher security levels

Secure Enclave Processor (SEP)

- A security circuit designed to perform secure services for the rest of the SoC
- Runs its own operating system (SEPOS) that has its own kernel, drivers, services, and applications
- Prevents main processor from gaining direct access to sensitive data and supports services such as Touch ID
- Contains its own set of peripherals accessible by memory-mapped dedicated I/O lines
- Uses inline AES to encrypt external RAM

Sideloading and Third-party Apps

- Sideloading involves installing applications that aren't from the official Android Market
- In COPE and CYOD environments this is a highly-enforced part of the mobile device policy
- Managers often remove the Unknown Sources field in the device settings to block downloading of third-party apps and deal with piracy, DRM, and licensing issues

Jailbreaking

- Jailbreaking an iPhone allows the installation of third-party apps not approved by Apple's strict controls
- Some of these out-of-market apps offer free features or added tweaks that represent what a root user can often do
- Key Raider malware (2015) and a semi-untethered Phoenix tool were released (2017) to jailbreak iOS 9.3.5 on 32-bit devices
- Apple has responded with patching exploits and upgrading hardware to iOS

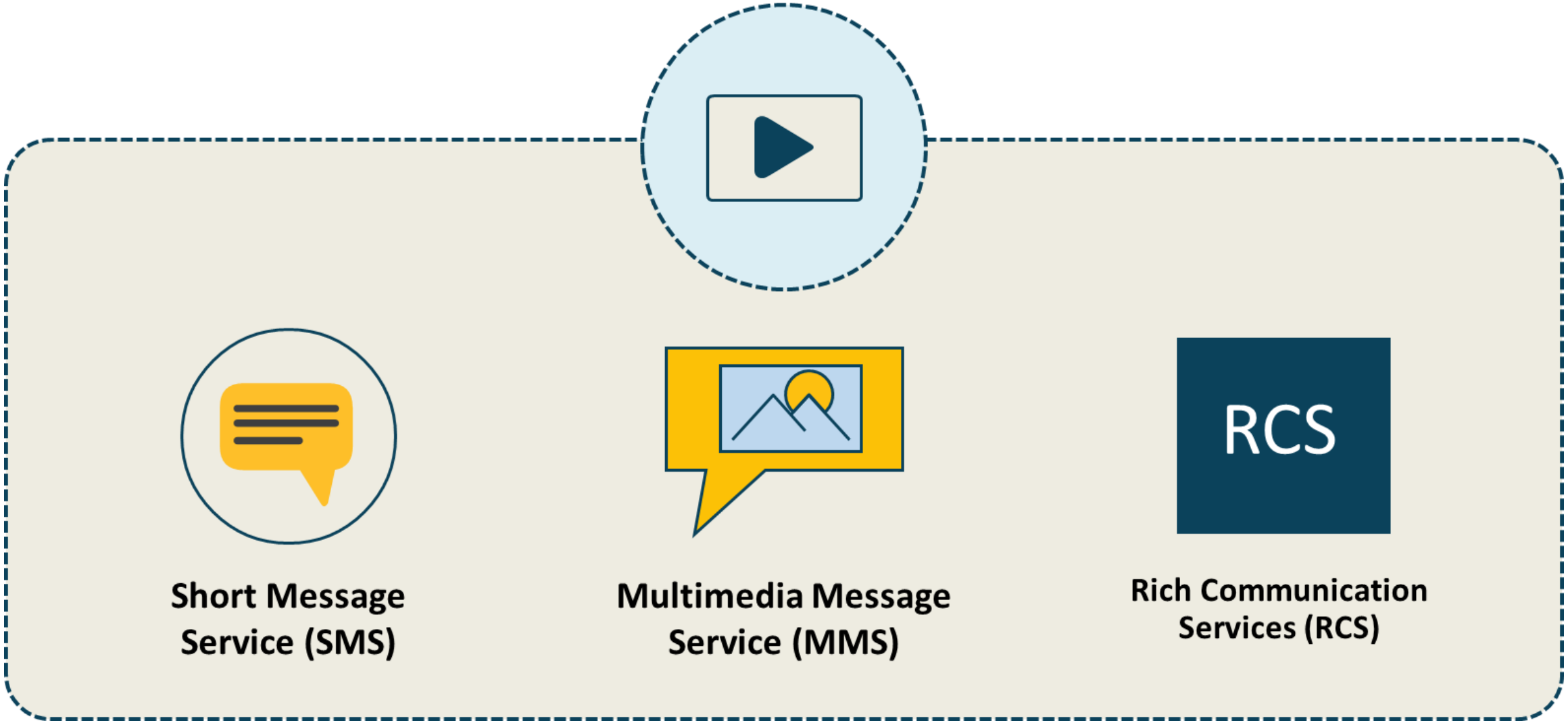
Rooting

- 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
- Because Android is open source, you can go into recovery mode and download a modified or entirely new version of the OS
- You can alter any hardware, software, or aesthetic settings on the device

Mobile Enforcement and Monitoring

- Customize device controls
- Conduct OS and firmware OTA
- Prevent custom firmware
- Perform carrier unlocking

Managing Mobile Communication Services



USB On-The-Go (USB OTG)

- Allows mobile devices to directly connect to one another
- By enabling a device to act as a USB host, additional unauthorized peripherals like storage, keyboards, or musical instruments can be used with the handset
- USB OTG defines two roles: An OTG A-device power supplier and the OTG B-device power consumer

Tethering

- Tethering involves making your device available to other devices as a wireless access point
- Regular patches and updates on wireless devices needed to prevent bridging and tethering from others
- May need to enforce these AUP restrictions with MDM:
  - Wi-Fi direct/ad hoc networks
  - Hotspots
  - Unauthorized domain bridging

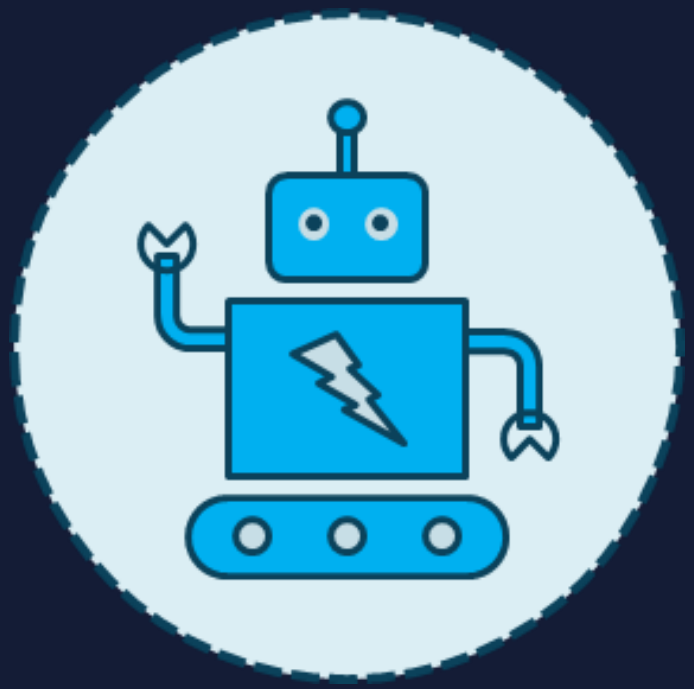
Mobile Devices for Payments

- Tokenization for payments and MFA
- Near-field communication (NFC)
- Mobile wallets for cybercurrency
- Peripheral-enabled payments (NFC)
- Vendor-specific payments (Apple)

Embedded System Security and Constraints

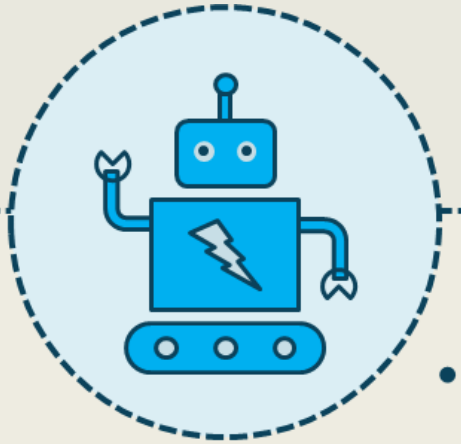
- Complete embedded source code is often not available
- Many of the device drivers and other components are simply binary sites with no source code at all
- Even if a patch is available, it is rarely applied in a consistent manner
- Hundreds of millions of devices are sitting on the Internet, unpatched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

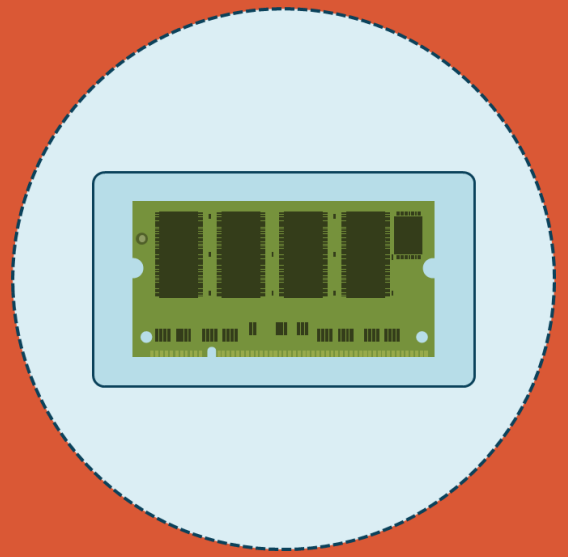
Securing Raspberry Pi



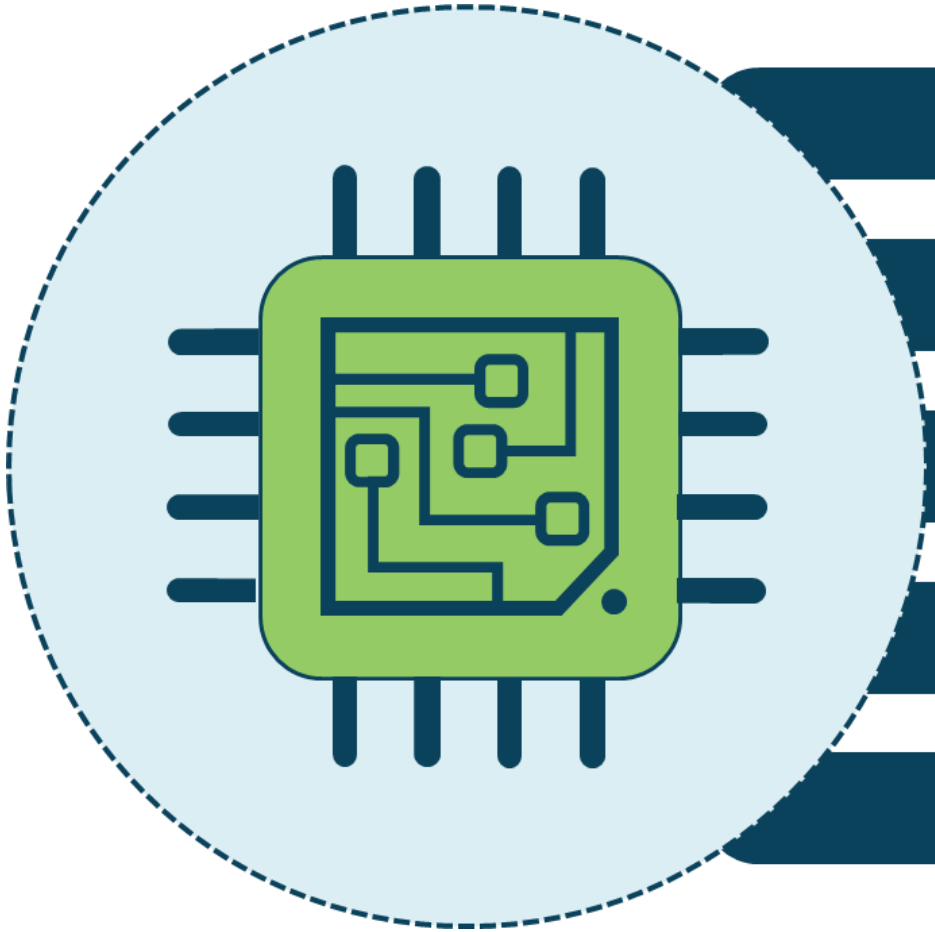
- Keep your system updated
- Don't use auto-login or empty passwords
- Change the default password
- Disable the pi user
- Stop unnecessary services
- Make sudo require a password
- SSH: prevent root login
- SSH: change the default port (SSH default port is 22)
- SSH: use SSH keys instead of passwords
- Install Fail2ban

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



Field Programmable Gate Arrays (FPGA)



- Field programmable integrated
- Fuse-based and battery-backed root
- Encrypted design bitstream
- Data erasure protection
- Glitch resistant features

Securing Embedded Devices

- Test in cloud before deployment
- Change and configuration management
- Patch management
- Digitally signed code
- Trusted OS and firmware
- Hire skilled systems/security practitioners

Supervisory Control and Data Acquisition (SCADA)

- SCADA represents the software used to collect and send data to other facility systems
- Programmable Logic Controllers (PLC) are the hardware component
- Systems that are not air-gapped introduce various threats

Supervisory Control and Data Acquisition (SCADA)

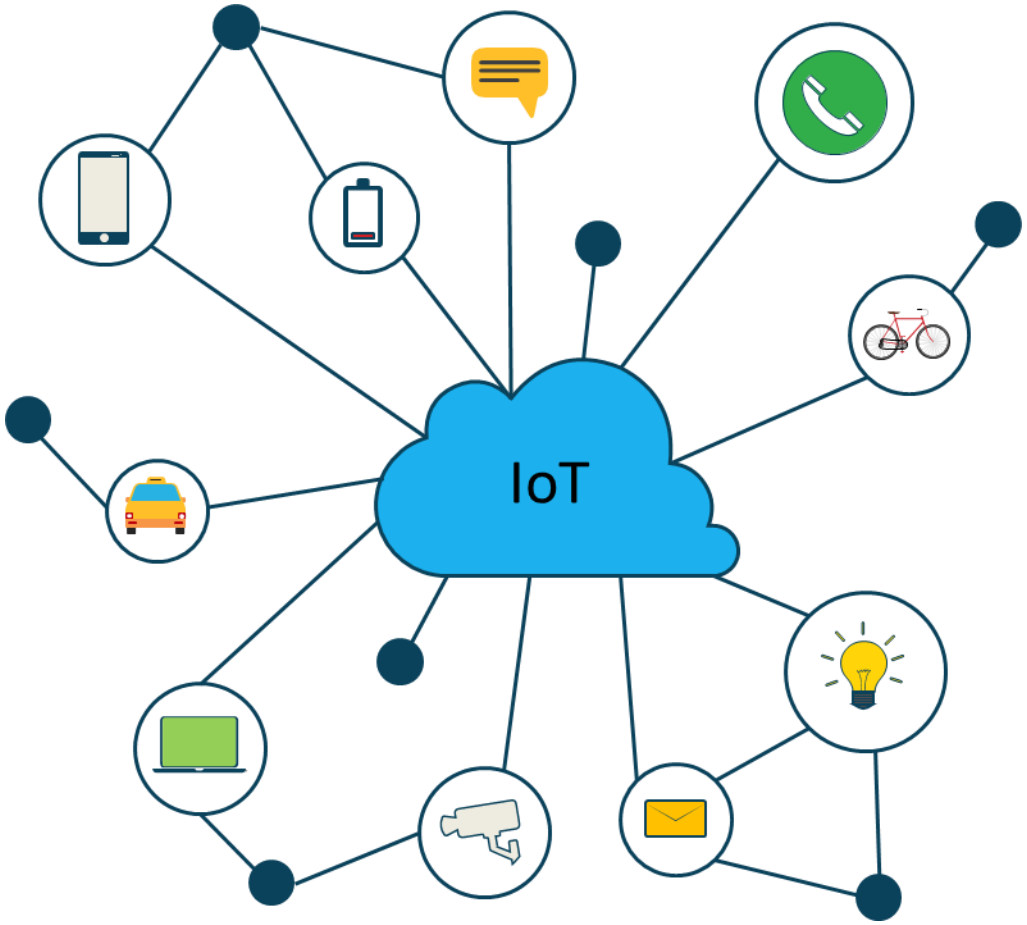
- SCADA represents the software used to collect and send data to other facility systems
- Programmable Logic Controllers (PLC) are the hardware component
- Systems that are not air-gapped introduce various threats

Supervisory Control and Data Acquisition (SCADA)

- Facility and manufacturing control and management systems
- Water management systems
- Electric and nuclear power grid
- Solar and wind farms
- Traffic signals and mass transit systems
- Environmental control systems
- Manufacturing systems

Internet of Things (IoT)

- Facility and manufacturing control and management systems
- Water management systems
- Electric and nuclear power grid
- Solar and wind farms
- Traffic signals and mass transit systems
- Environmental control systems
- Manufacturing systems



OWASP IoT Top Ten

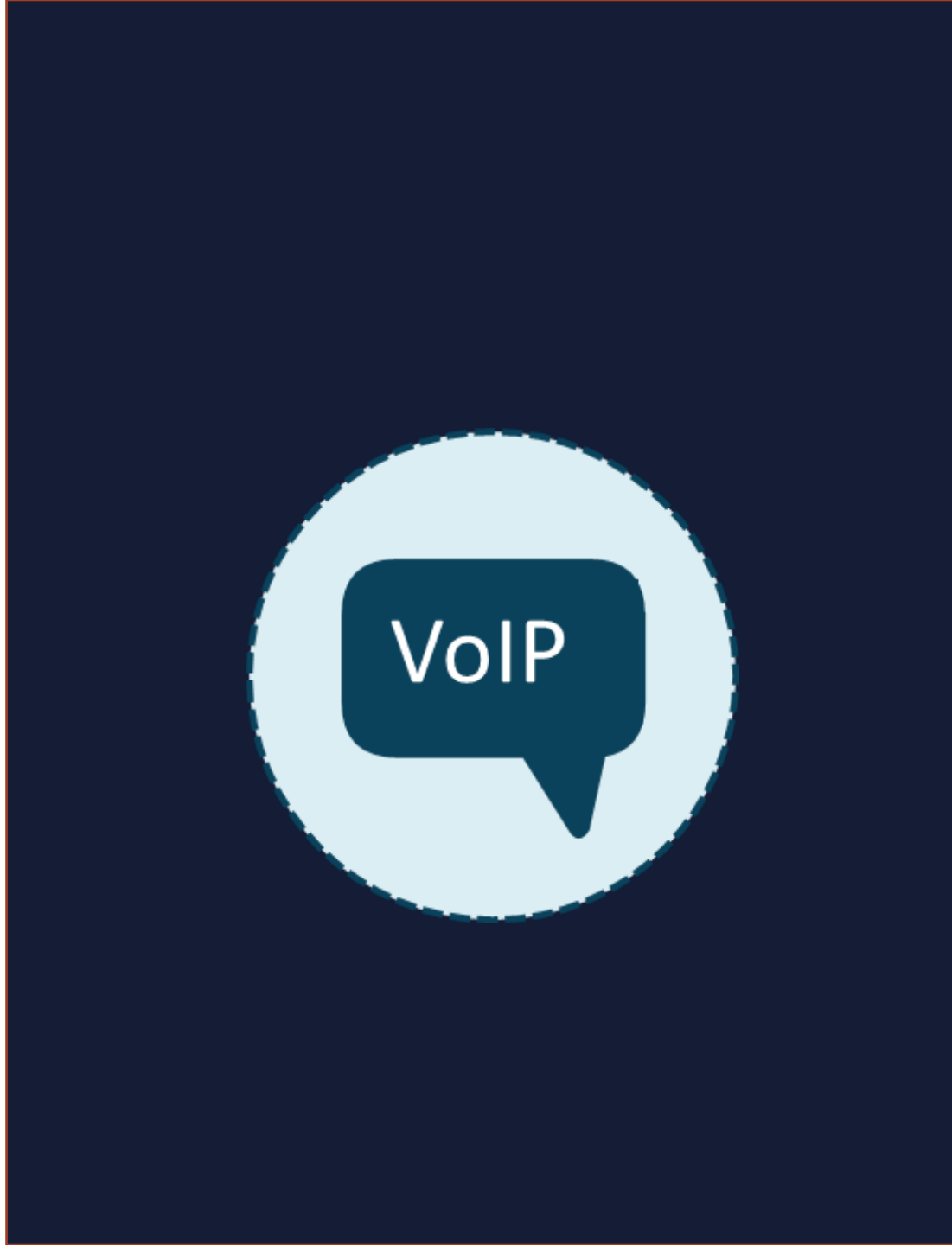
1. Weak, guessable, or hardcoded passwords
2. Insecure network services
3. Insecure ecosystem interfaces
4. Lack of secure update mechanism
5. Use of insecure or outdated components

OWASP IoT Top Ten

6. Insufficient privacy protection
7. Insecure data transfer and storage
8. Lack of device management
9. Insecure default settings
10. Lack of physical hardening

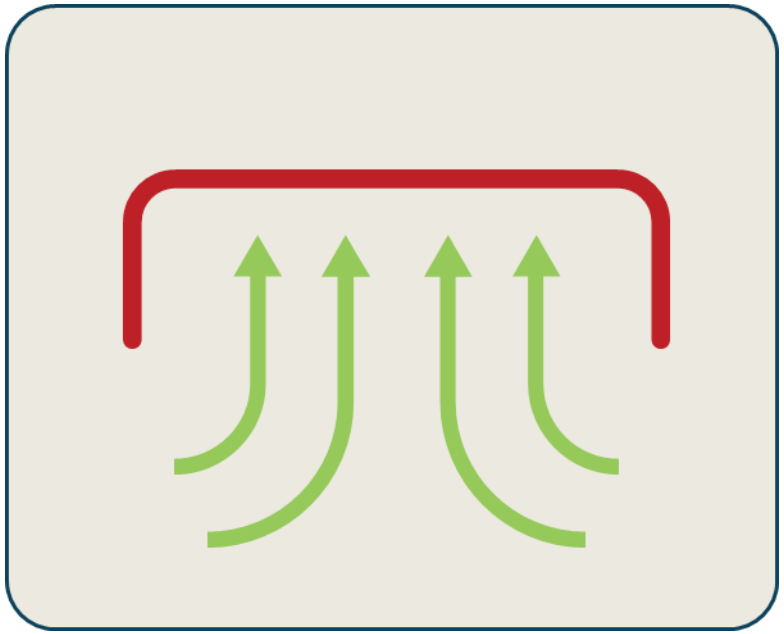
Securing Voice over IP (VoIP)

- Harden and patch the IP PBX
- Make sure there is security of data-in-transit and high-availability with RADIUS and backend databases
- On the VoIP firewalls:
  - Allow only call control information (such as SIP)
  - Allow lookup to the LDAPS server
  - Allow management protocols in both signaling and media access
  - Control the source addresses (remember that SIP uses ports 5060 and 5061, H.323 uses TCP port 1720) to set up a call connection

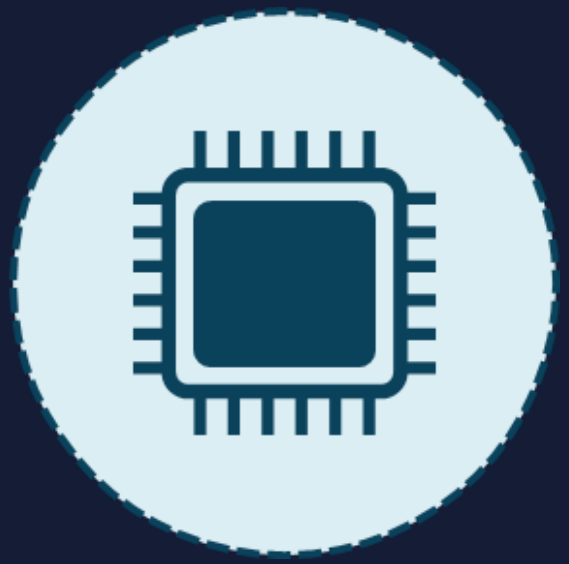


HVAC

- Provides heating, ventilation, and air-conditioning for a building
- Controlled via a network
  - Open
  - Closed
- If breached, hackers may shut down system
- Causes an increase or decrease in temperature and humidity
- If breached, hackers may have access to a multitude of information
- Includes confidential information in other parts of the network



System on a Chip (SoC)



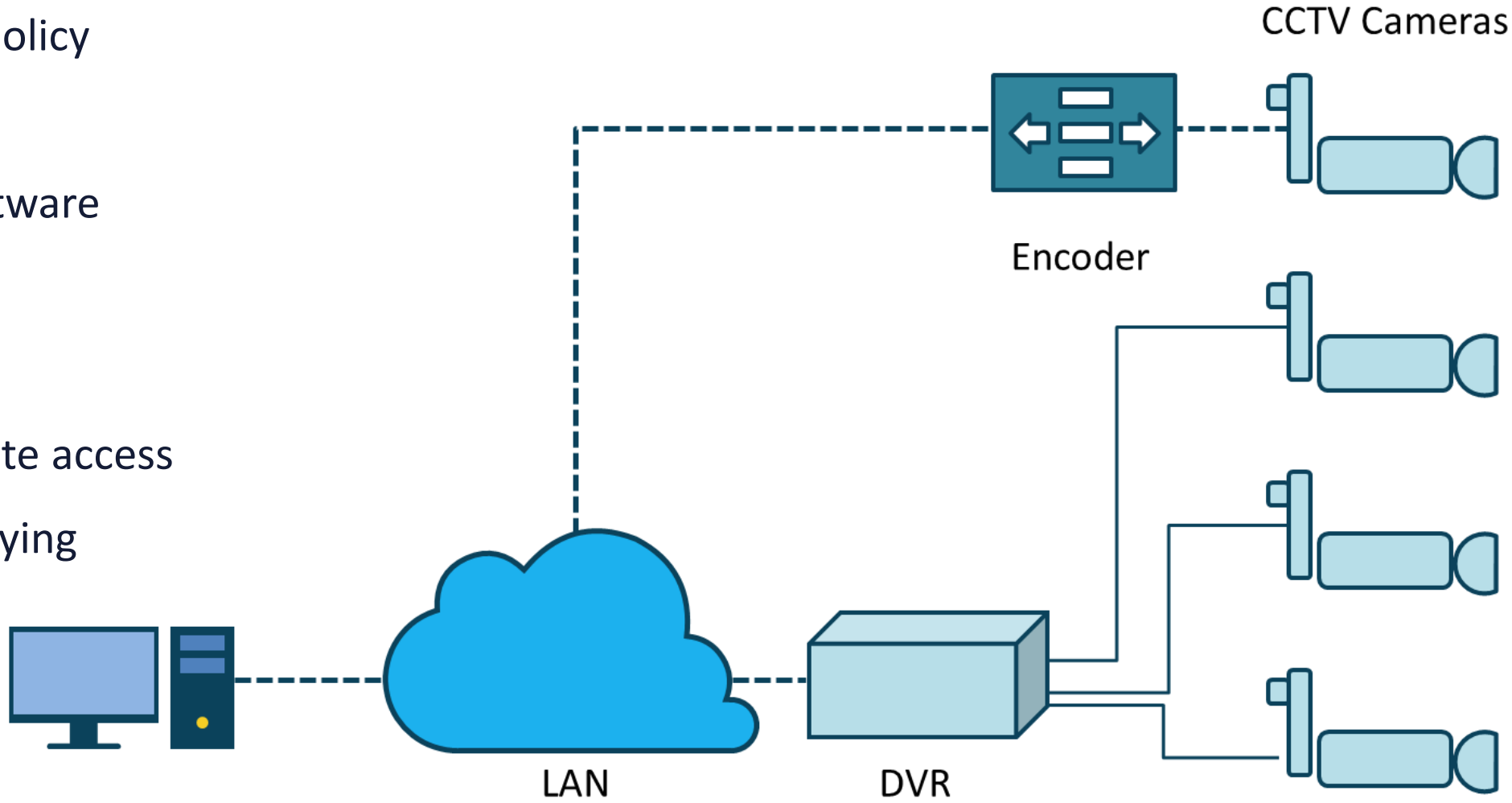
- Combining electrical circuits of various components and software onto a single chip
- Common in IoT devices, mobile products, wearables, and RFID systems
- Security concerns:
  - Lack of security controls
  - Lack of and speed of updates
  - Privacy
  - Malware
  - Root access

Real-time Operating System (RTOS)

- OS that serves real-time applications
  - Processes data immediately or in tenths of seconds
- Security concerns are:
  - Code injection
  - Privacy
  - Exploiting shared memory
  - Priorities
  - DoS attacks
  - Inter-process communications

Video Surveillance and Webcams

- Lack of security policy
- Weak passwords
- Poorly coded software
- Malware
- Privacy
- Mobile and remote access
- Recording and spying



Other Specialty Systems

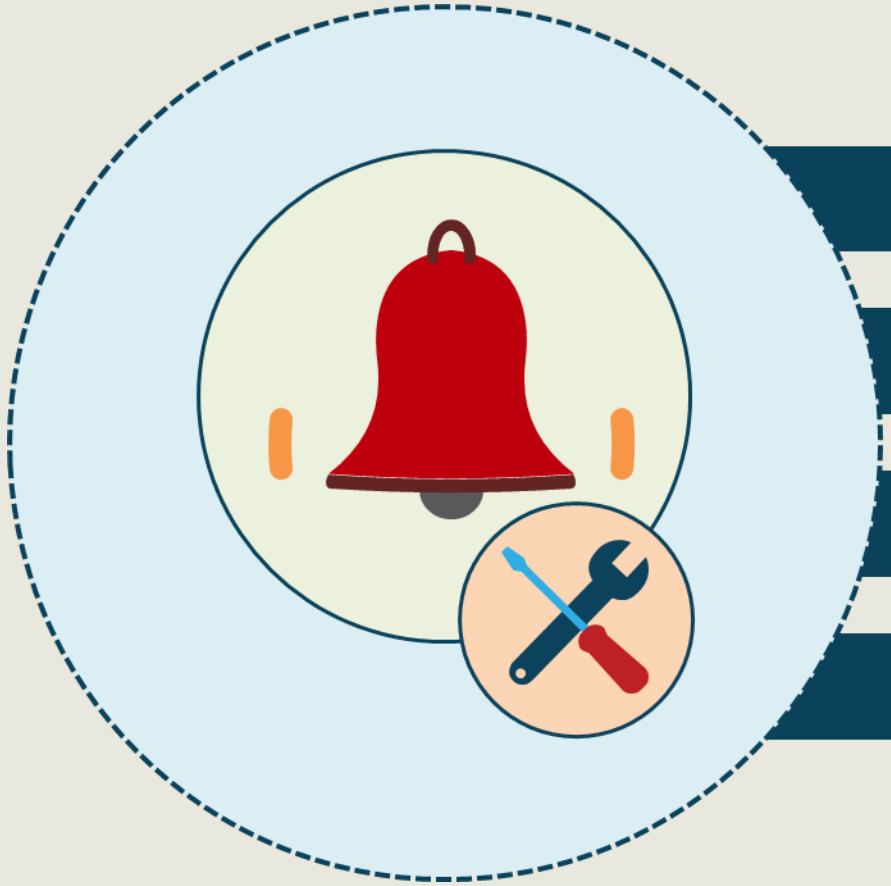
- Adaptive voltage scaling (AVS) - a closed-loop dynamic power minimization method that adjusts the voltage sent to a computer chip to match the chip's needs during operation
- Unmanned aerial vehicle (UAV) - an aircraft that carries no human pilot or passengers, often called “drones” and usually controlled remotely by a human pilot
- Multifunction printers (MFP) - a combination of email, fax, photocopier, printer, and scanner

Incident Response

Not all events are “incidents”

- Steps taken when a negative event disrupts normal operations
- Severity of incident will determine level of action
  - Is it an event or an incident?
  - How critical is the target?
  - What is the immediate impact on operations?

Goals of Incident Response

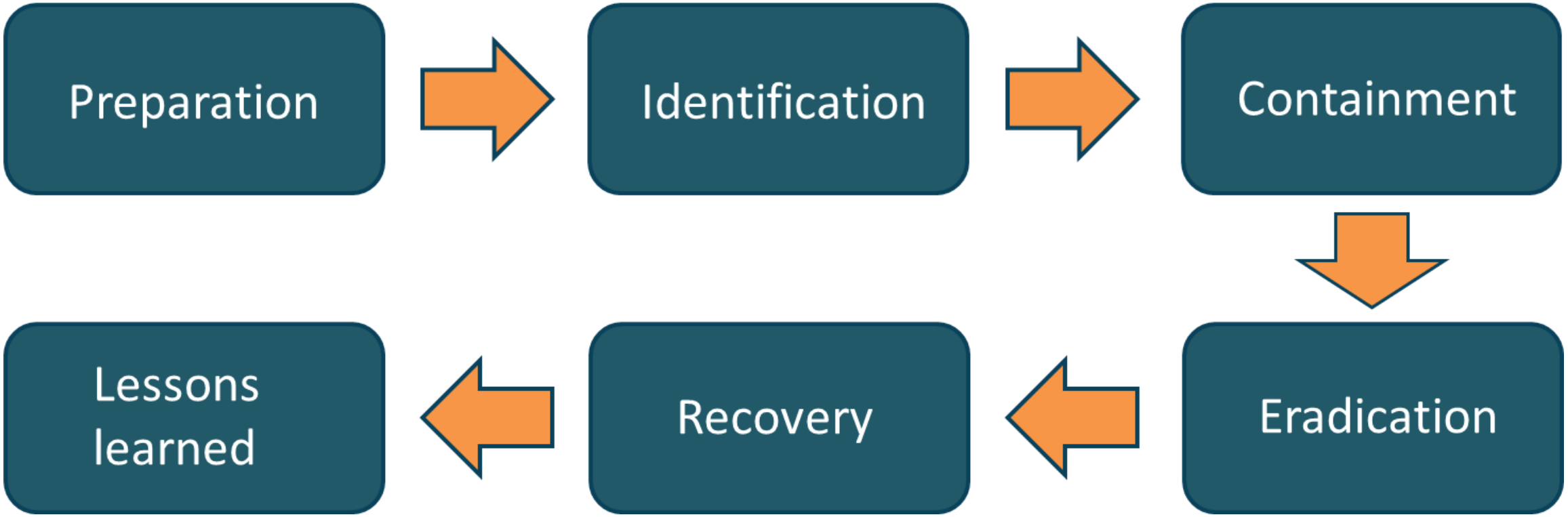


- Reduce the immediate impact
- Maintain and restore business operations
- Provide after-action reports and lessons learned
- Deter future attacks

Incident Response Processes

- To be prepared you need a plan
- Documented incident types/category definitions based on risk assessments and BIA
- Know roles and responsibilities of the first responders
- Reporting requirements/escalation
- Contact lists, public relations, and legal obligations
- Cyber-incident response teams (CSIRT)
- May be out-sourced or swarm team
- Best practice is to have pre-performed exercises, drills, and simulations

Incident Response Lifecycle



1. Preparation

- Involves all information gathering, missions, charters, and project initiation tasks
- Get buy-in and funding from executive management in order to know the scope of the incident response plan
- Determine the roles and responsibilities of internal employees on incident response teams
- Establish first responders and processes for communication to relevant stakeholders
- Conduct IR exercises and drills based on budget

2. Identification

- Separate an event from an incident or breach immediately using pre-defined metrics and experience
- Implement techniques for categorizing and prioritizing the incident based on an established risk register or risk ledger
  - When did it occur?
  - How were you alerted?
  - Who made the discovery?
  - What is the scope of impact?
  - Does it qualify for escalation or disaster recovery?
  - Can you quickly identify the root cause?

3. Containment

- Implement short-term processes, such as disconnecting devices from the network
- Use firewalls, NG-IPS, ML algorithms, and other forensic tools to maintain separation, containment, and segregation
- Evaluate backups and snapshots for future recovery

4. Eradication

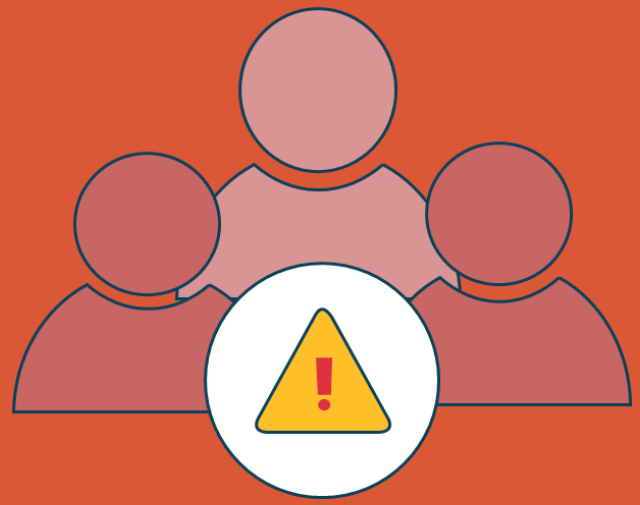
- This step is often integrated with the previous phase, Containment, as opposed to being a separate action
- Involves determining the root cause of the incident and applying immediate remedies if available
- Involves removing all indicators of compromise and any action, artifacts, remnants, or fingerprints associated with the attack

5. Recovery

- The process of restoring negatively affected data, applications, systems, and devices to an established baseline performance level or, if possible, the original state
- This often involves only remediation to a certain operational point and not total recovery
- During this process, it is vital to establish that you are not in danger of another incident or breach

6. Lessons Learned

- Knowledge gained from the process of conducting the program
- Sessions usually held at the response close-out
- To share and use knowledge derived from an experience
- Endorse the recurrence of positive outcomes
- Prevent the recurrence of negative outcomes



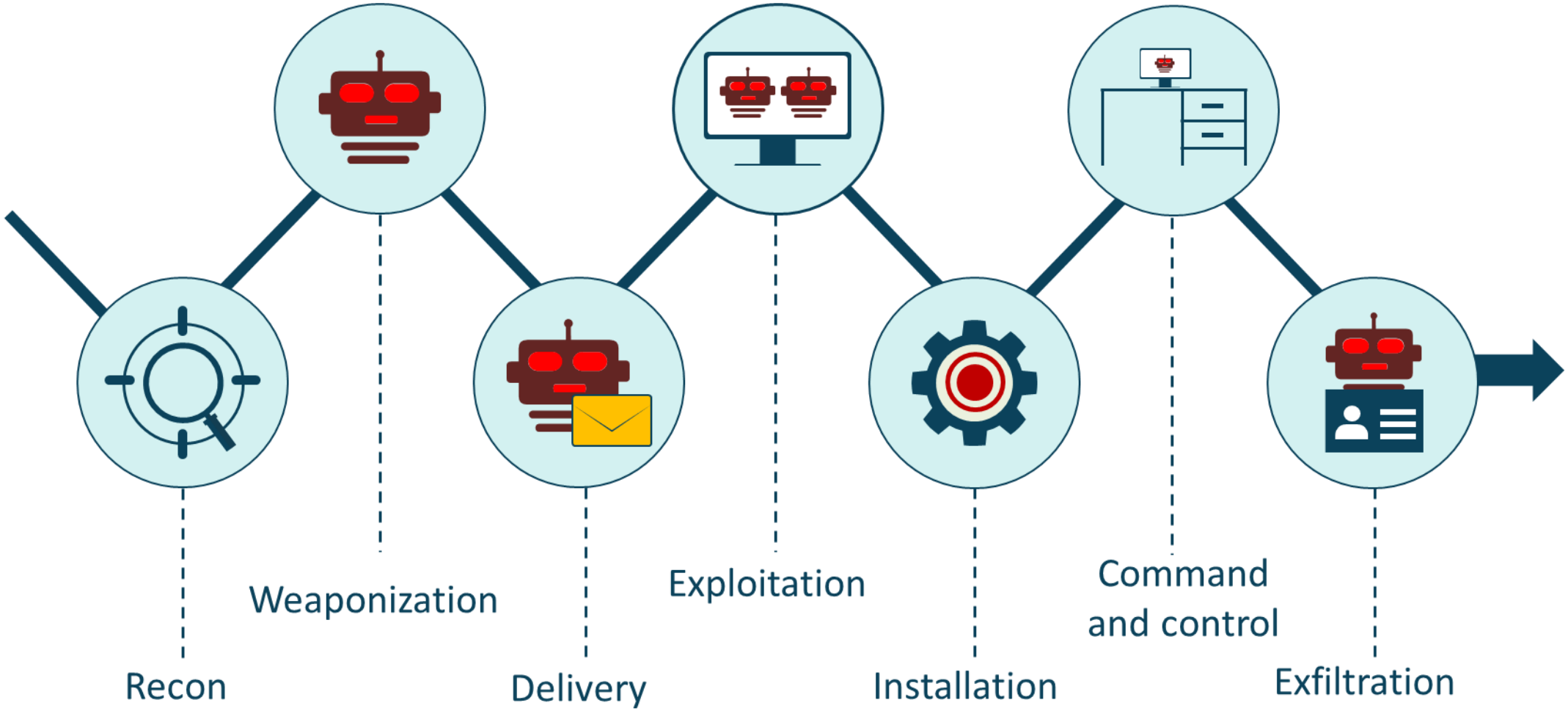
Incident Response Exercises

- Plan review (read-through)
  - Group discussion, plan auditing, and Delphi and brainstorming sessions with stakeholders
- Tabletop
  - Examine documented plans, diagrams, and logical and virtual walkthroughs to eliminate gaps/errors
- Walkthrough (exercise)
  - Planned rehearsals and drills
  - Performed in stages and by department/building only
  - Should find additional gaps to those found during plan review and tabletop exercises

Incident Response Exercises (cont.)

- Simulation
  - Focuses on specific scenarios and areas
  - Uses real BCP and DRP resources (recovery sites) and teams (swarm simulations)
  - Tests snapshot recovery and hot spares
  - May be the highest-level test that most organizations conduct
- Parallel
  - Real-world drill while still operating business
  - More resource-intensive than simulations
- Full Interruption
  - Real-world drill while ceasing business activities
  - Cost-prohibitive for most organizations

7-Phase Cyber Kill Chain



8-Phase Cyber Kill Chain

1. Reconnaissance
2. Intrusion
3. Exploitation
4. Privilege escalation
5. Lateral movement
6. Obfuscation/anti-forensics
7. Denial of service
8. Exfiltration

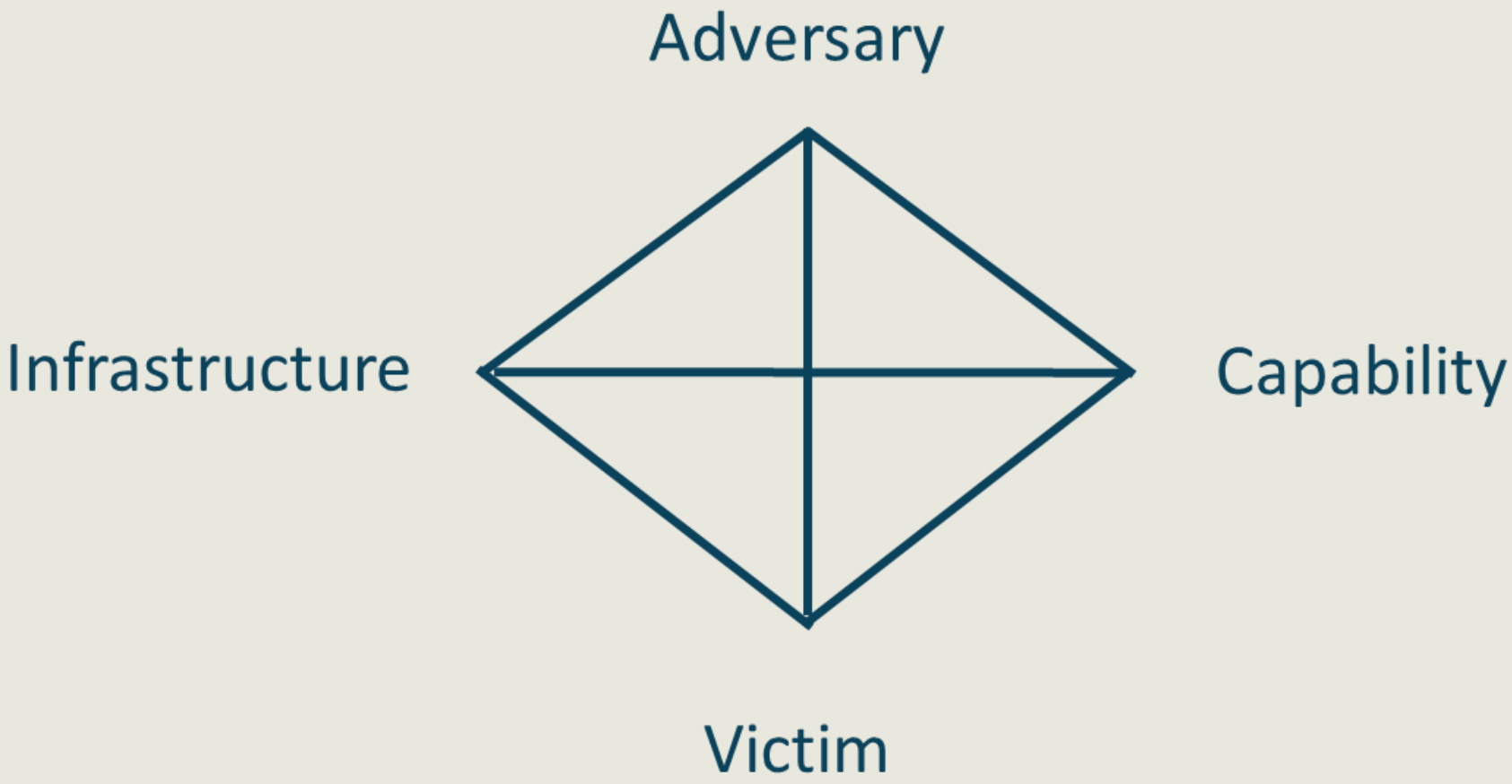
MITRE ATT&CK

- A knowledge base from mitre.org composed of aggressive attack methods and practices based on real-world interpretations
- Used for generating threat modeling and threat assessment tools in all sectors
- Organizations commonly use the enterprise matrix as a starting point

Diamond Model of Intrusion Analysis

- A breakthrough cybersecurity initiative that is renowned in the cyber security community as one of several key resources for analysts
- Emphasizes granular attacker activities and generates a model that helps cybersecurity analysts classify relationships between motivations, victims, and the technologies used to conduct the attack

Diamond Model of Intrusion Analysis



Incident Response Teams (IRT)

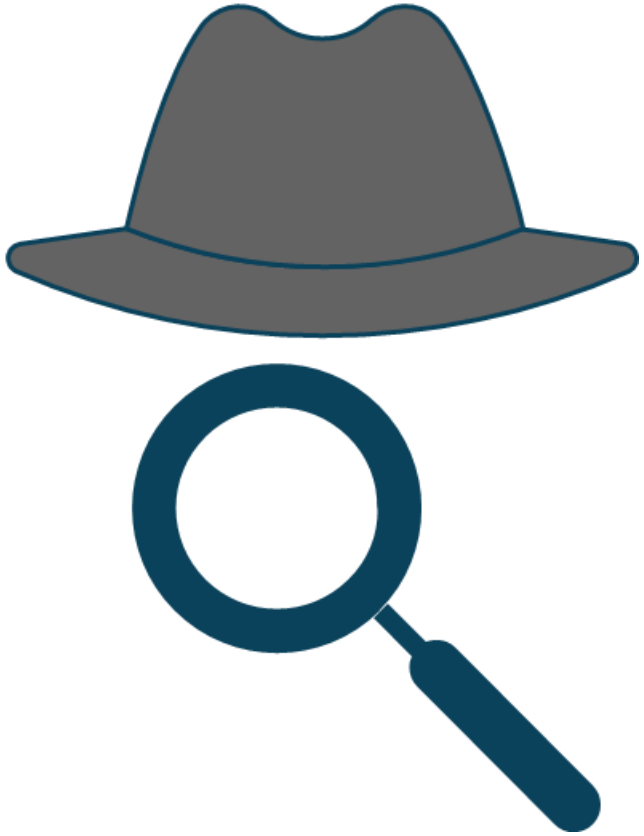
- Also called CSIRT (Computer Security IRT)
- Receives alerts and alarms of security breaches
- First responders determine severity and priority
- Implements rehearsed plans and procedures
- Conducts analysis of activities and documents action plan
- May perform forensic and investigative techniques

Incident Response Teams

- May be a pre-designed group or an ad hoc association
- May be internal or external
- Internal IRTs gather periodically for proactive tasks, such as DR testing, and vulnerability and penetration testing and assessment
- Members should come from various business units and have different skillsets

Cyber Forensic Investigations

- Involves the scientific investigation of a cyber incident
  - Data breach
  - Insider attack
  - Malware campaign
    - Ransomware
    - Cryptojacking
  - DDoS
  - Blackstortion
  - CP files
  - Pirated content
  - Any illegal activities



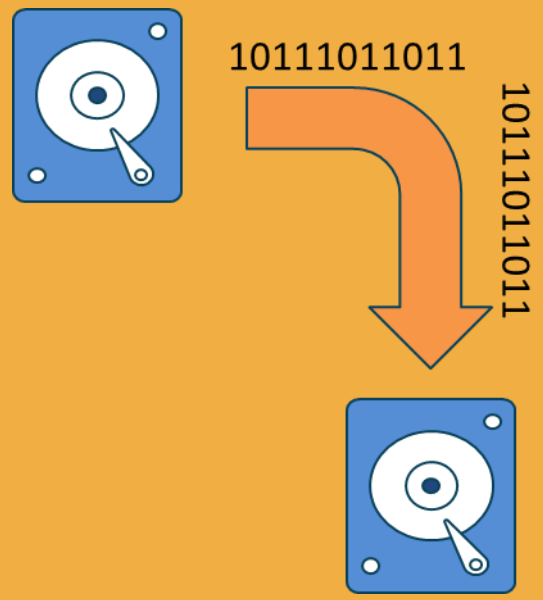
Cyber Forensics

- Investigations need to be carried out in a standardized manner
  - Identification of the crime
  - Collection of evidence
  - Examination of the evidence
  - Analysis of the evidence
  - Reporting on the findings of the analysis

Collection of Evidence

- Capture system images
  - Use write-blockers
  - Forensic kits
- Network traffic and logs
- Timeline of event sequence
- Capture video
- Record time offsets
- Take hashes
- Create screenshots
- Conduct witness interviews

Examination of Evidence

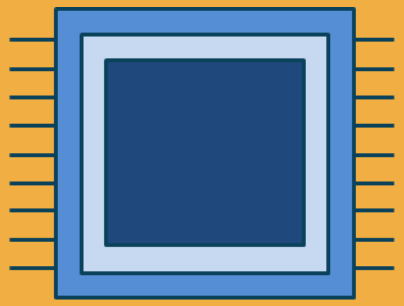


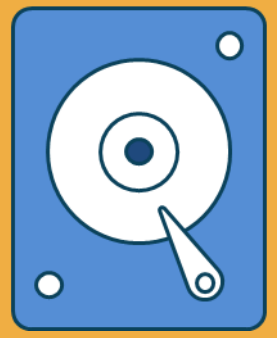
- Follows evidence through entire life cycle until possible court date
- Involves strict procedures for collecting, handling, and tagging evidence
- Provides a history and timeline of the handling of the evidence
  - Maintains evidence integrity
  - Provides accountability
  - Prohibits tampering
- Anticipates any admissibility issues, such as legal holds

Forensic Techniques

- Validation
  - Encrypted volume detection
- Filtering
  - Filtering SIDs on shared systems for privacy reasons
- Pattern matching
  - Regular expressions and metacharacters in forensic kits
- Hidden data discovery and extraction
- Searching slack space
- Tracing

Order of Volatility



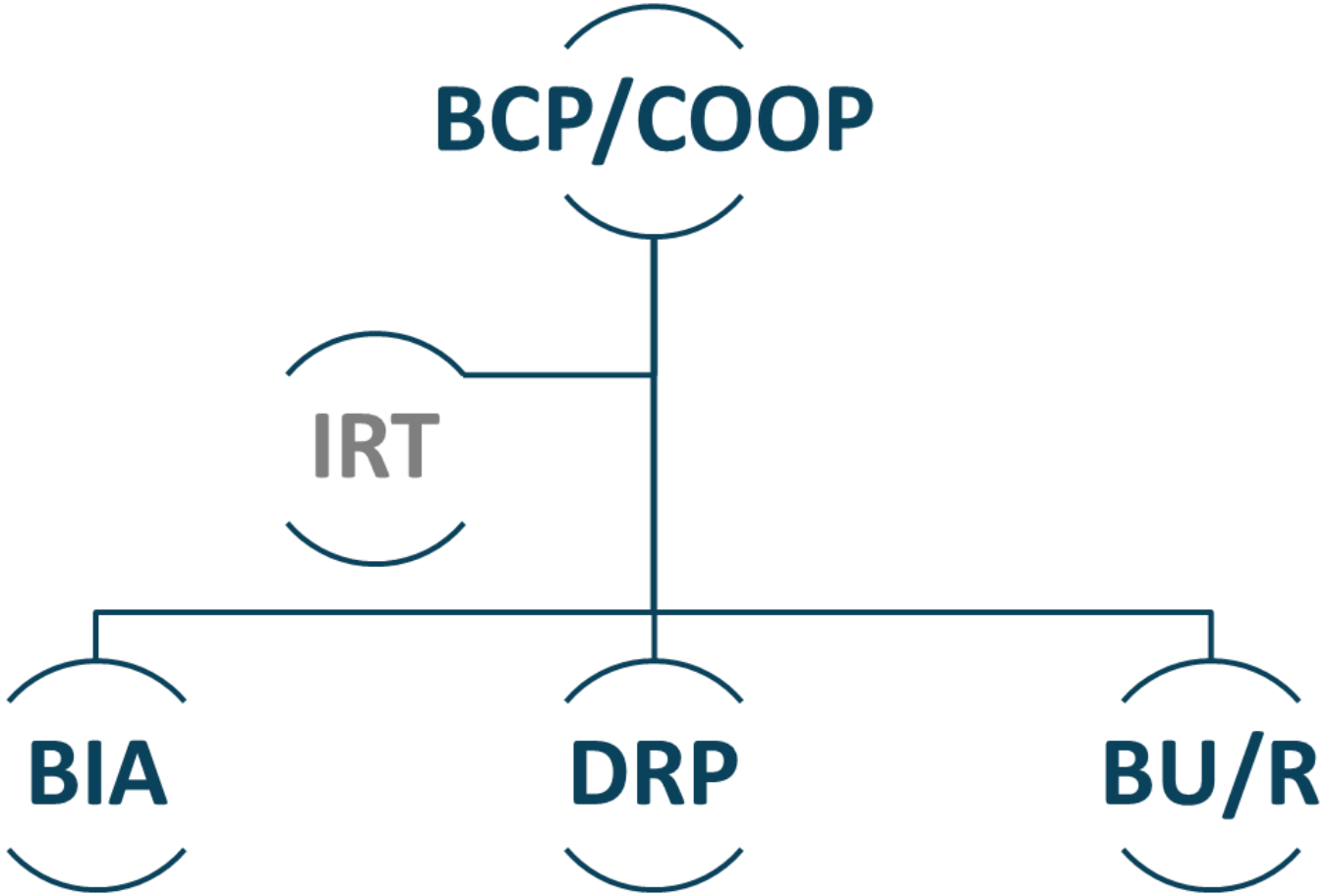


1. CPU and its cache
2. Kernel statistics, tables, and caches
3. Memory (RAM)
4. Temporary file systems, and swap/slack space
5. Disk drives and volumes
6. Attached removable drives
7. Logged data to a remote location
8. Copies of data to archived media/cloud

e-discovery

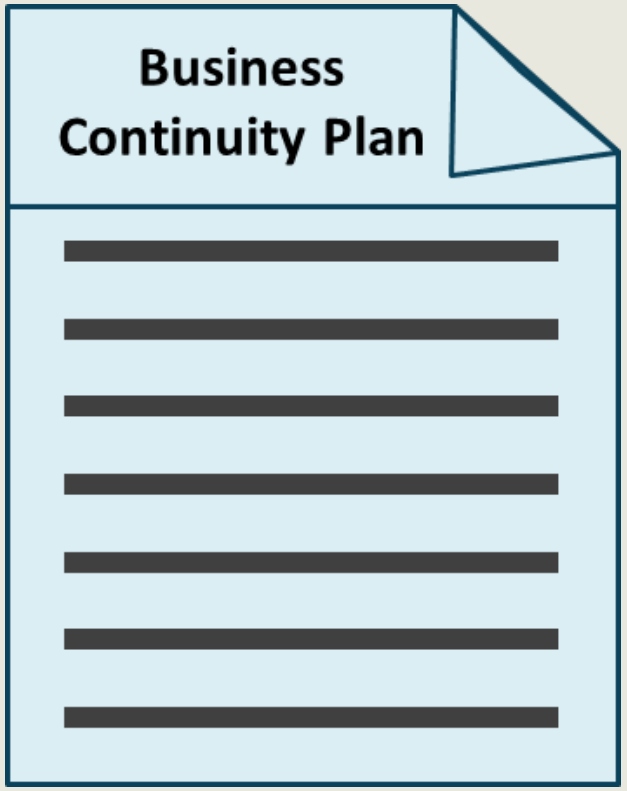
- Innovative technology that has emerged over the last decade to lower the risks and costs associated with big data, especially in litigation and internal corporate and government investigations
- The e-discovery process includes four phases
  1. Identifying and collecting documents
  2. Sorting through data by relevance
  3. Creating production sets
  4. Data management

Business Continuity Planning (BCP/COOP)



BCP/COOP

- Ensures business operates a pre-determined level when disaster strikes
  - Documents approved by executive management
- Outlines risk to business
  - Populates risk register/ledger
  - Requirements to mitigate incidents
- Identifies procedures needed to recover from a disaster
  - What is an acceptable amount of time?
  - How to reduce the impact of the disaster

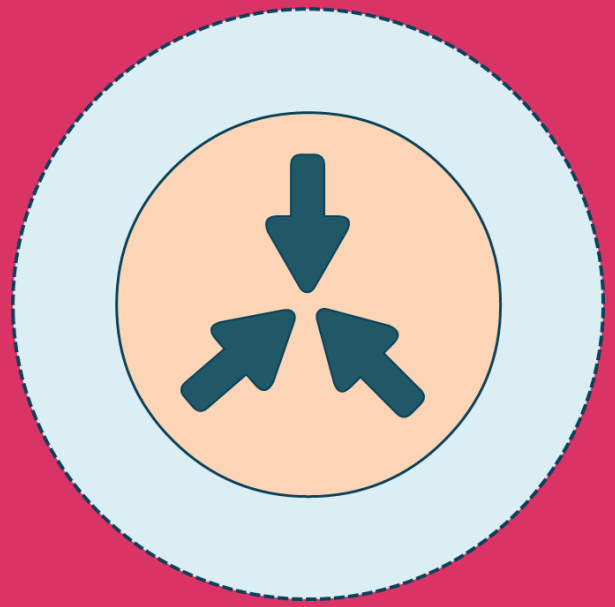


NIST SP 800-34, Revision 1

BCP according to NIST

1. Develop a continuity planning policy statement
2. Conduct the business impact analysis (BIA)
3. Identify preventive controls
4. Create contingency strategies
5. Develop an information system contingency plan
6. Ensure plan testing, training, and exercises
7. After-action report
8. Ensure plan maintenance

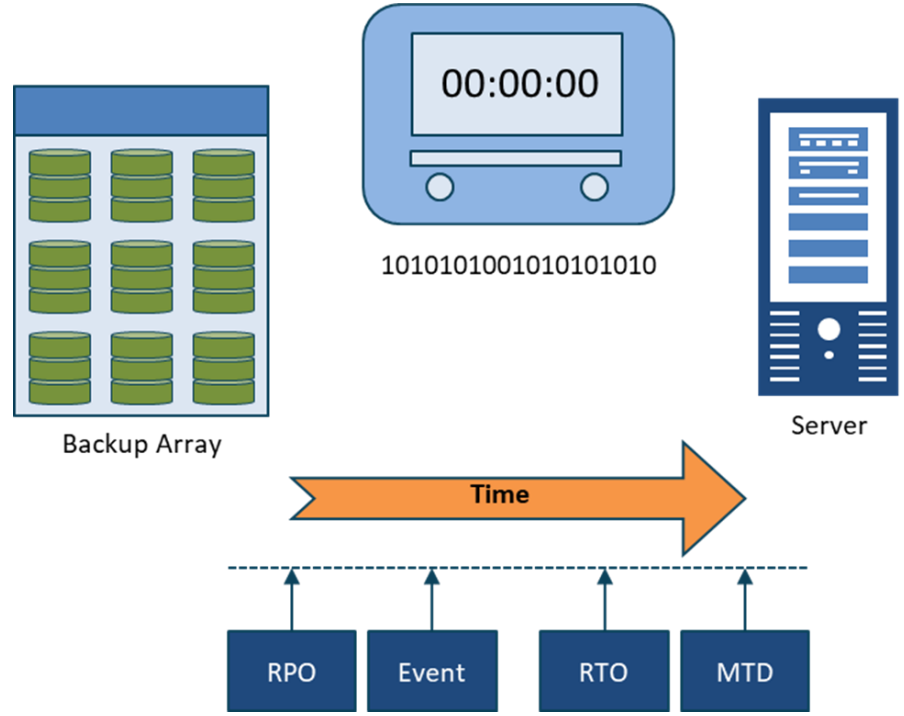
Business Impact Analysis



- The risk assessment aspect of the Business Continuity Plan (BCP) or (COOP)
- Identify critical functions to the business and prioritize them based on need for survival
- Identify the risks associated with the critical functions
- The probability of the risk occurring (likelihood)
- The impact the risk will have (magnitude)
- Identify how to eliminate the risk or reduce the risk

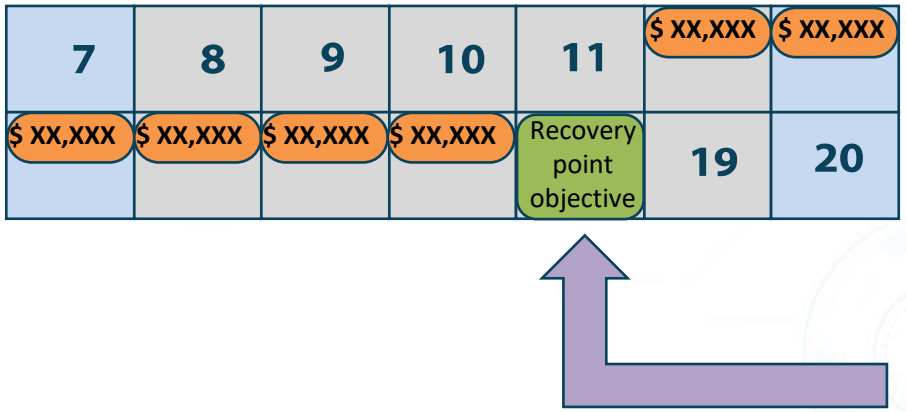
Recovery Time Objective (RTO)

- The amount of time available to recover the resource, service, and function
- Must be less than Maximum Tolerable Downtime (MTD)
- Any solutions must be accomplished within this time frame or it is considered loss
  - Add physical security
  - Add redundancy
  - Purchase insurance
  - Invest in backup generators
  - Invest in faster devices
  - Safeguard media off-site

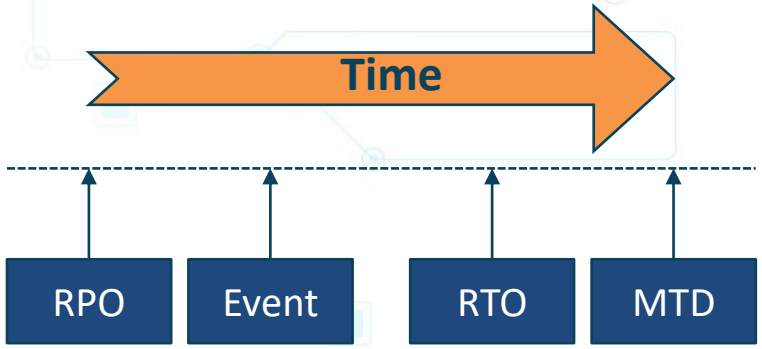


Recovery Point Objective (RPO)

- The point in time, relative to a disaster, where the recovery process begins
  - How much work can be lost if a disruption occurs?
  - What impact will it have?
  - How do we make sure we don't lose more than "X" information?

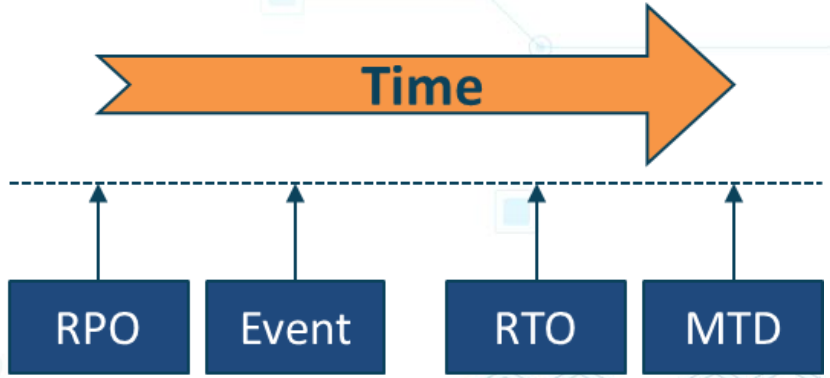


SUN	MON	TUE	WED	THU	FRI	SAT
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			



Maximum Tolerable Downtime (MTD)

- Absolute maximum amount of time that a resource, service, or function can be unavailable before we start to experience a loss
- Factors to consider include
  - finances
  - life/safety
  - regulatory
  - legal/contracts
  - reputation, and
  - property



Mean Time Between Failures (MTBF)

- A measure of how reliable a hardware system or component is
- For most devices, the measure is in thousands or tens of thousands of hours between failures
- For example, an SSD drive may have a mean time between failures of 10 years

Mean Time To Repair (MTTR)

- How long does it take to repair?
  - Measures time to fix
  - Average value predicted based on experience and documentation
  - (Total down time)/(number of breakdowns)

Disaster Recovery Planning (DRP)

- Ensuring that the company can recover to an established baseline of continuity after any kind of high-level incident
- The tasks and processes that will be conducted when a disaster or catastrophe strikes
- Incident can affect a single drive, an entire server, a VLAN, an area of the facility, an entire floor or building, or the entire site or campus

Disaster Recovery Planning (DRP)

- Outlines the technical aspects involved for restoration
  - Recovery sites: hot, warm, cold, mobile, cloud, shared
  - Order of restoration (most critical to least critical)
  - Backups, snapshots, and restores
  - Contact information
  - Communication plans
  - Chain of authority
  - Step-by-step instructions
  - Locations of documents, software, and keys

Thank You for Attending!

Your instructors:

Michael J Shannon

and

Carl Mullin

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