



Security+ Session 3

with Michael J. Shannon - CISSP, Security+, CCNP-SEC, Palo Alto PCNSE7,
ITIL 4 Managing Professional, and OpenFAIR

DNSSEC

- DNSSEC adds a layer of trust on top of DNS by providing authentication as the root DNS name servers help verify domains
- Information published by the root is vetted by a thorough security procedure, including the Root Signing Ceremony
- To facilitate signature validation, DNSSEC adds a few new DNS record types:
 - RRSIG - Contains a cryptographic signature
 - DNSKEY - Contains a public signing key
 - DS - Contains the hash of a DNSKEY record
 - NSEC and NSEC3 - For explicit denial-of-existence of a DNS record
 - CDNSKEY and CDS - For a child zone requesting updates to DS record(s) in the parent zone

Domain Naming System/Secure (DNSSEC)

- DNSSEC allows you to sign your company's DNS records so that any system that has an authenticating DNS resolver will automatically verify if the records are valid or have been compromised by a MITM attack
- Remember: DNSSEC does not provide confidentiality of DNS data
- There are no protections against DoS/DDoS attacks
- Also: Cisco Umbrella (OpenDNS)



Secure Shell (SSH)

- Management access should be limited to secure protocol alternatives as in SSH instead of Telnet
- SSH2 is preferable to SSH1 whenever possible
- SSH2 uses symmetric encryption for the bulk data encryption and asymmetric algorithms in their key management processes
- SSH2 uses DH for key exchange

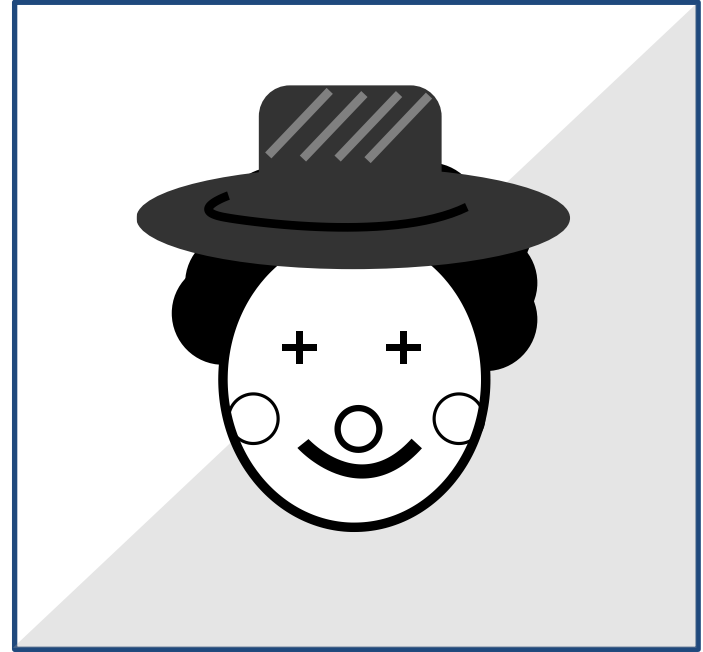


Configuring SSH on a Cisco IOS router

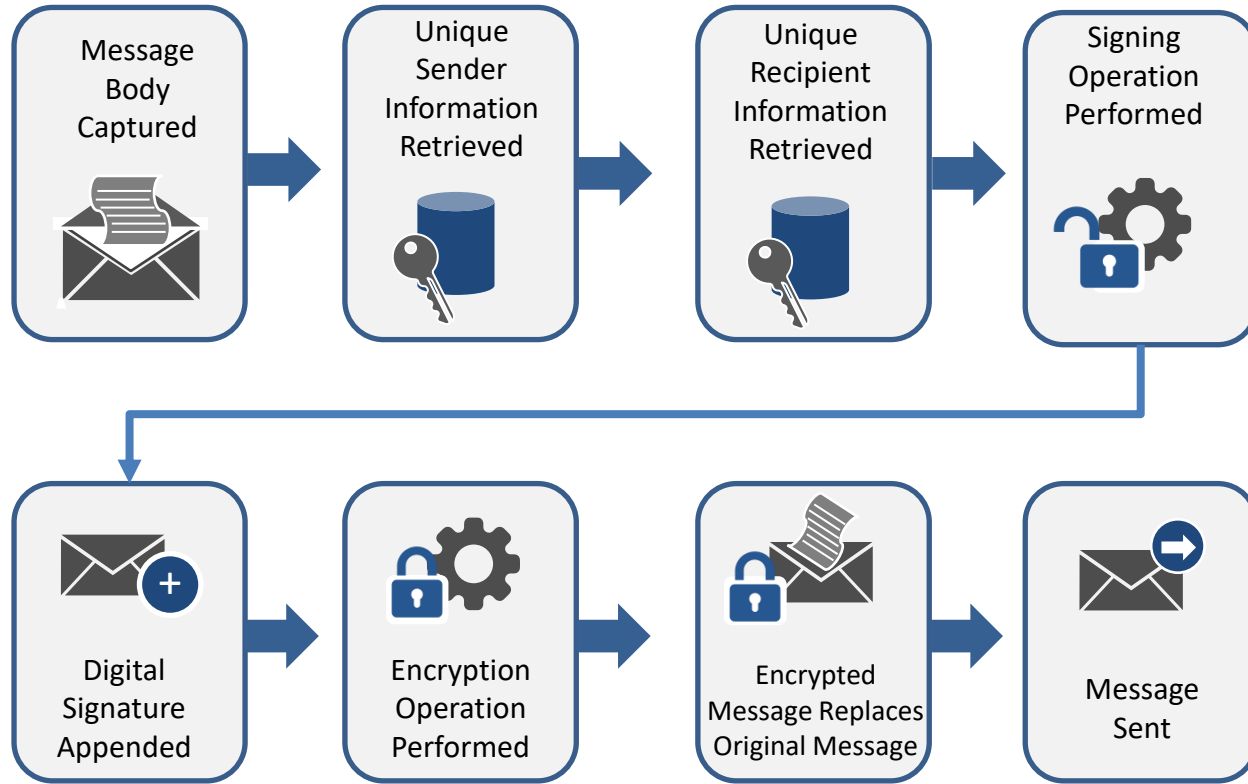
```
Router(config)#hostname SecplusR1
SecplusR1(config)#ip domain-name example.com
SecplusR1(config)#crypto key generate rsa general-keys modulus 2048
The name for the keys will be: SecplusR1.example.com
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)
*Apr 9 19:01:50.517: %SSH-5-ENABLED: SSH 1.99 has been enabled
SecplusR1(config)#username admin secret S3curitY3Plu5
SecplusR1(config)#line vty 0 15
SecplusR1(config-line)#login local
SecplusR1(config-line)#transport input ssh
```

Secure MIME (S/MIME)

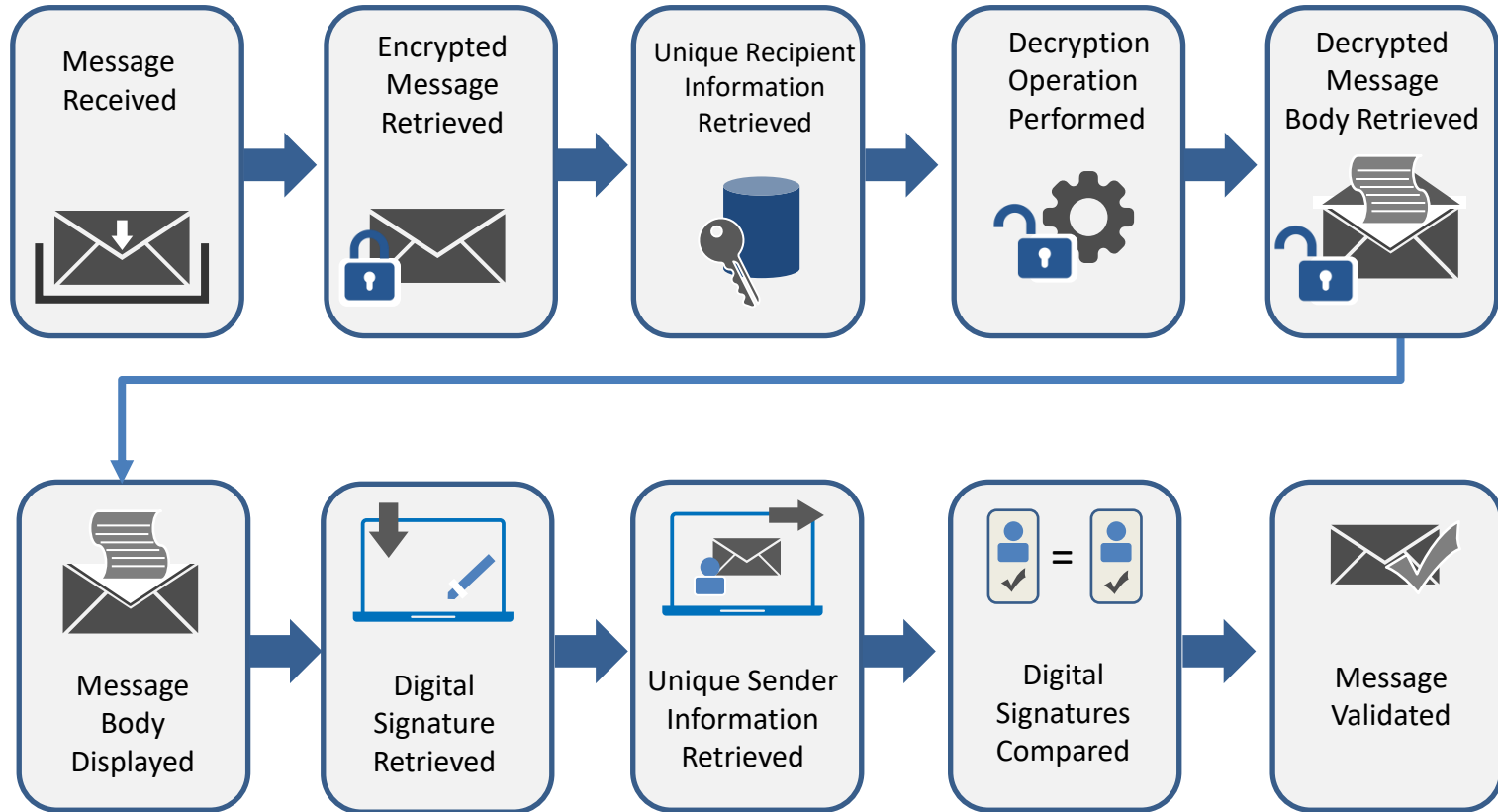
- Simple Mail Transfer Protocol (ESMTP) is natively not secure
- S/MIME version 3 has gained wide acceptance as the standard for email message security
- S/MIME provides two security services:
 - Digital signatures
 - Message encryption
- Digital signatures are the most common S/MIME service providing authentication, data integrity, and non-repudiation



Secure MIME (S/MIME)



Secure MIME (S/MIME)



Secure Real-Time Transport Protocol (SRTP)

- Secure Real-Time Transport Protocol (SRTP) extends the RTP protocol by providing enhanced security techniques
- Provides encryption, integrity, and authentication verification of data and messages transported by RTP
- Released in 2004 by Cisco Systems and Ericsson

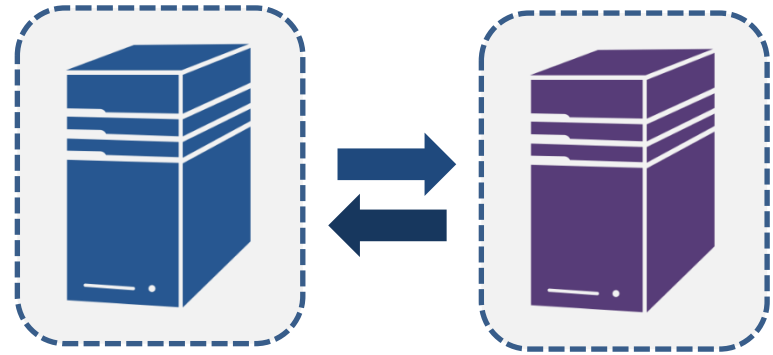


Lightweight Directory Access Protocol/Secure (LDAPS)

- LDAP was based on X.500 but is a lighter, cross-platform, and standards-based solution
- LDAP servers are easy to install, maintain, and optimize but they are without solid security of the queries, updates, and valuable information in the LDAP directory
- LDAPS (TCP 636) is LDAP over SSL/TLS
- SASL (Simple Authentication and Security Layer) BIND also offers authentication services using mechanisms like Kerberos or a client certificate sent with TLS

File Transfer Protocol/Secure (FTPS)

- FTPS is essentially the File Transfer Protocol with SSL/TLS Security
- IT extends the FTP protocol by adding SSL/TLS functionality
- Also called FTP over TLS and FTP Secure
- Typically server-to-server
- Uses AES, RSA/DSA and X509v3 certificates
- Explicit vs. implicit



Secure File Transfer Protocol (SFTP)

- IETF designed version of FTP that provides secure data access and transfer over an SSH2 channel
- It is a function of the SSH Protocol and is also called SSH File Transfer Protocol
- Both the commands and data are encrypted
- Platform-independent
- Slower than SCP



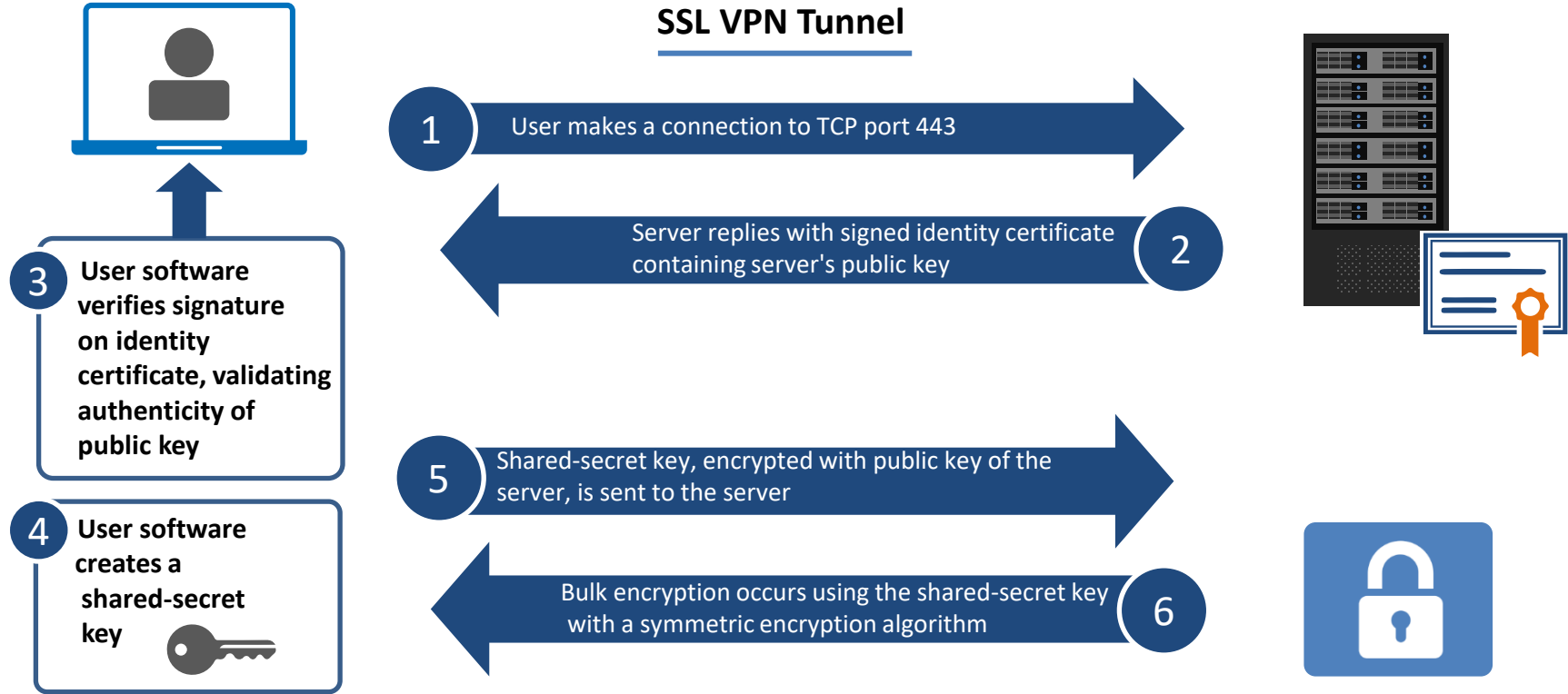
Simple Network Management Protocol (SNMPv3)

- SNMP deservedly has a bad security reputation in the past versions 1 and 2c, which are both clear text protocols and use community strings for authorization
- All versions of SNMP use a tree-structured MIB
- SNMPv3 can be configured in three modes:
 - **noAuthNoPriv:** no cryptographic hash or encryption (passwords)
 - **AuthNoPriv:** cryptographic HMAC (SHA1 or SHA2) to secure authentication credentials and provide integrity, but no data encryption
 - **AuthPriv:** HMAC for integrity and secure authentication credentials and also encryption (AES) for data

Transport Layer Security (SSL/TLS)

- SSL/TLS is the most ubiquitous certificate-based peer authentication in use on the Internet (HTTPS)
- Transport Layer Security (TLS) is standardized by IETF
- TLS 1.3 is the most recent published version
- Also used with SMTP, LDAP, and POP3
- The only mandatory cipher suite includes RSA for authentication, AES for confidentiality, and SHA for integrity and digital signatures
- RFC 7457 – Summarizing Known Attacks on Transport Layer Security

Transport Layer Security (SSL/TLS)

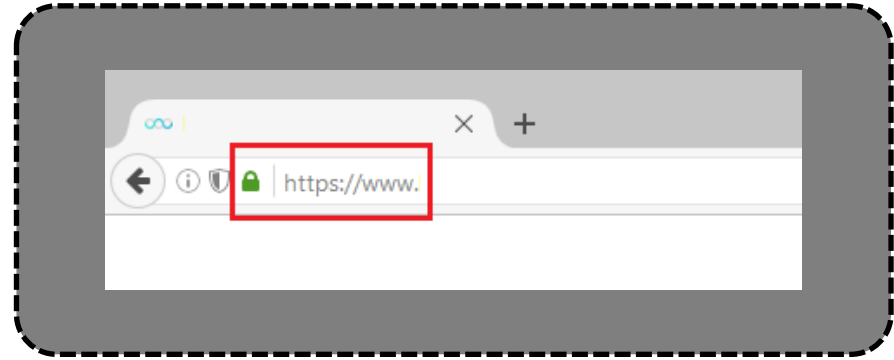


Hypertext Transfer Protocol/Secure (HTTPS)

- The most widely used protocol on the Internet for any secure commercial transaction, financial service, contract, agreement, file transfer protection, voice and video services
- It is basically HTTP over SSL/TLS
- Mozilla is deprecating non-HTTPS secured search results in order to help hasten the global adoption of HTTPS
- A cryptographic key exchange happens when you first connect to a secure web site and all ensuing activities on the web site are encrypted
- It is still possible to see that particular web sites have been visited – but not the web pages you read, or data transferred

Hypertext Transfer Protocol/Secure (HTTPS)

- If a padlock icon is shown, then the web site is secure
- If the icon is green, it signifies that the web site has presented your browser with an Extended Validation Certificate (EV)
- This verifies that the SSL certificate presented is accurate for the domain name, and the domain name belongs to the entity you would expect to own the web site



Secure Post Office Protocol and IMAPS

- These are versions of the POP (POPS) and IMAP (IMAPS) email protocols that run over SSL/TLS
- IMAP over SSL (IMAPS) is assigned the port number 993
- Encrypted communication for POP3 is either
 - Requested after protocol initiation using the STLS command
 - Connected to the server using SSL/TLS on well-known TCP port 995



Popular Use Cases for Secure Protocols

- Voice and video
 - Time synchronization (NTPv3/v4)
 - Email and web
 - File transfer
 - Directory services
 - LDAPS
 - Kerberos
- Remote access
 - Domain name resolution
 - Routing and switching
 - Authentication
 - Network address allocation
 - DHCPv6
 - Subscription services

Industry-standard Frameworks and Reference Architectures

- Regulatory vs. non-regulatory
 - Regulatory: HIPAA, SOX, General Data Protection Regulation (GDPR)
 - Non-regulatory: NIST, ITIL 4, ISO/IEC, COBIT5, CIS, ISACA
- Country-specific vs. international
 - U.S: FISMA, GLBA, COBIT5, HIPAA
 - INTL: GDPR, ITIL4, ISO/IEC, AGATE, IDABC, OBASHI
- Industry-specific frameworks
 - PCI-DSS for credit card companies
 - Sarbanes-Oxley (SOX) for financial services
 - HIPAA for PHI security and privacy



Benchmarks/Secure Configuration Guides

- Benchmarking is known as a technique to improve an organization's information security management by establishing a standard
- Determining the organization's maturity level by performing gap analysis against the best practices and implementing risk controls as agreed
 - Center for Internet Security (CIS)
 - Common Secure Configuration (NIST)
 - Security Configuration Guidance - National Security Agency
 - OWASP Top 20
 - CMMI

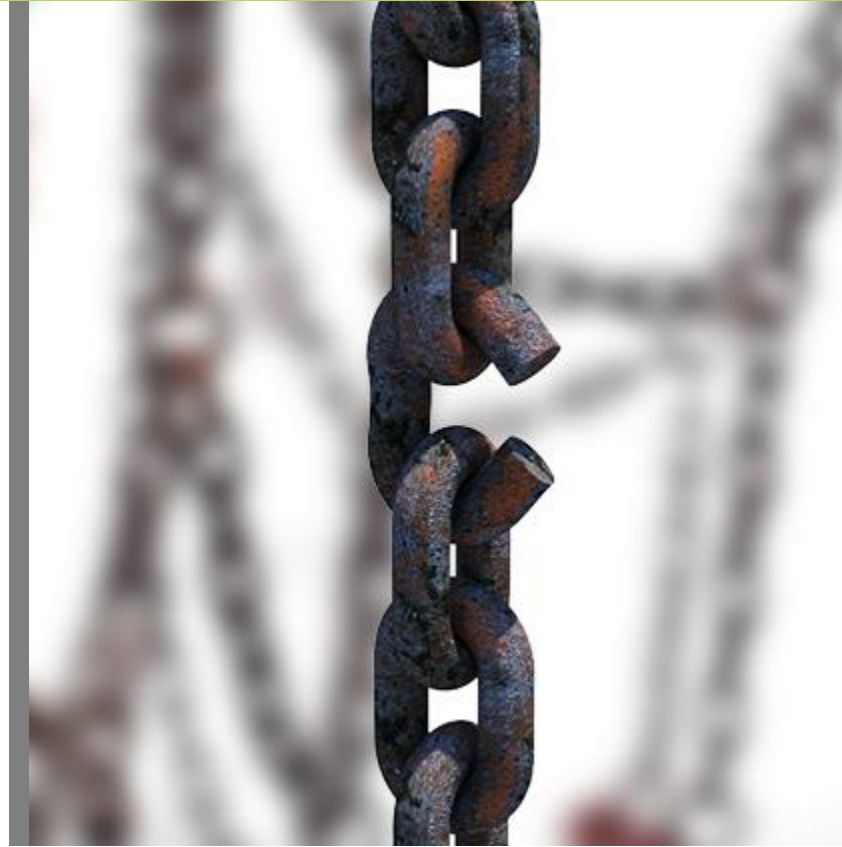
Principles of Secure Design

- Defense in depth
 - Providing end-to-end layered security with several components
- Compartmentalization
 - Creating security domains and zones



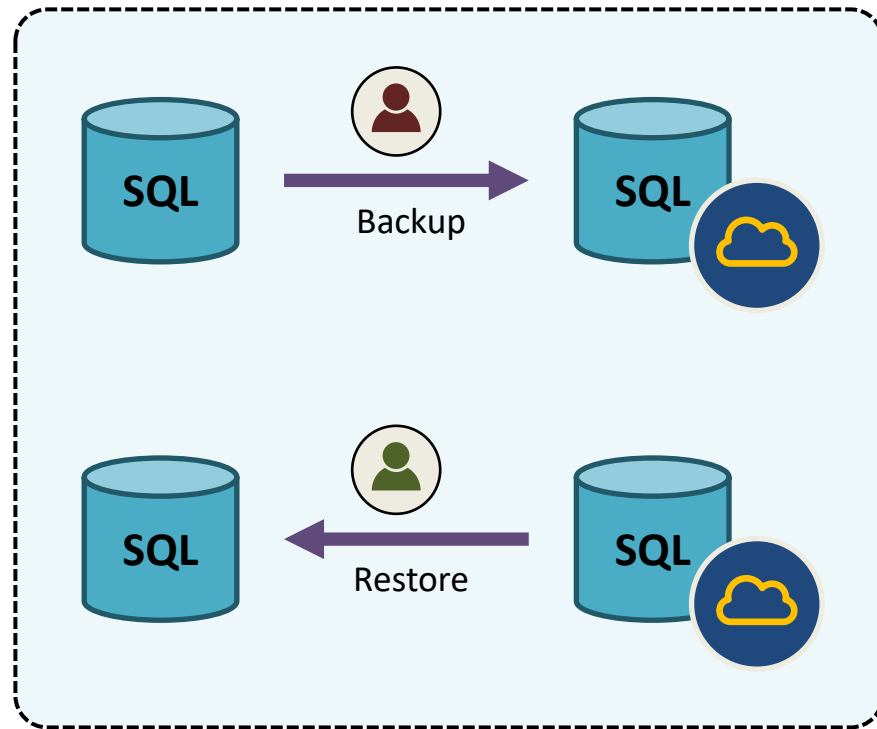
Principles of Secure Design

- Least privilege
 - Applies need-to-know approach
- Weakest link
 - Says a process or system is only as strong as its weakest component



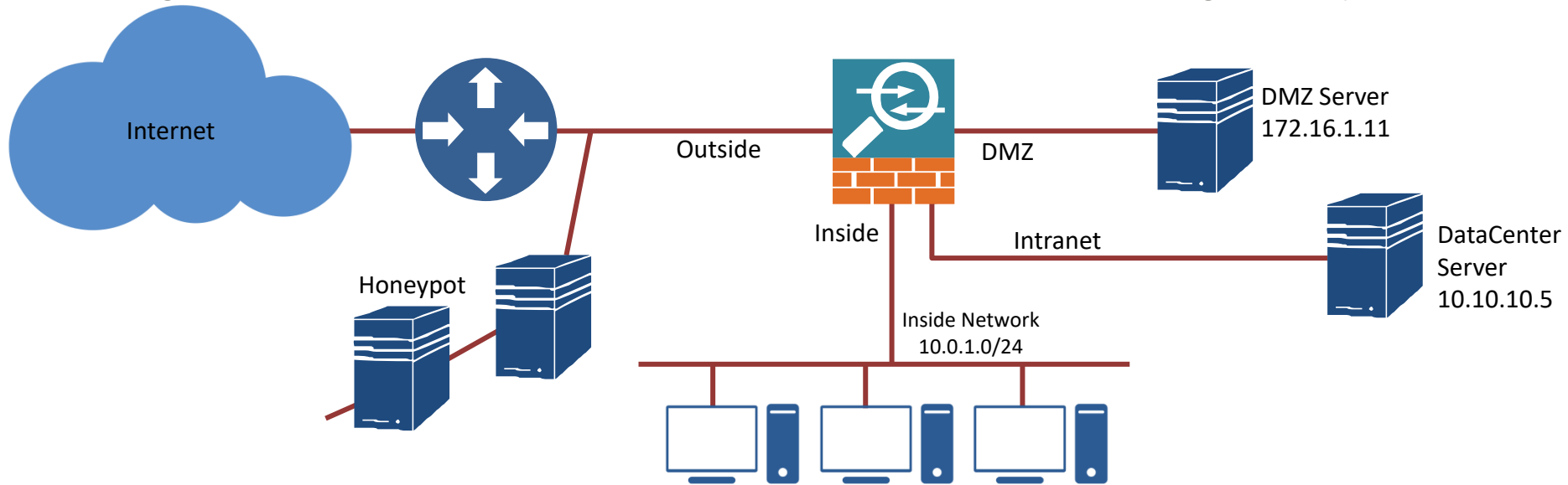
Principles of Secure Design

- Separation and rotation of duties (dual operator)
 - Processes where more than one entity is required to complete a particular task
- Mediated access
 - Proxies and other controls act on behalf of the participants



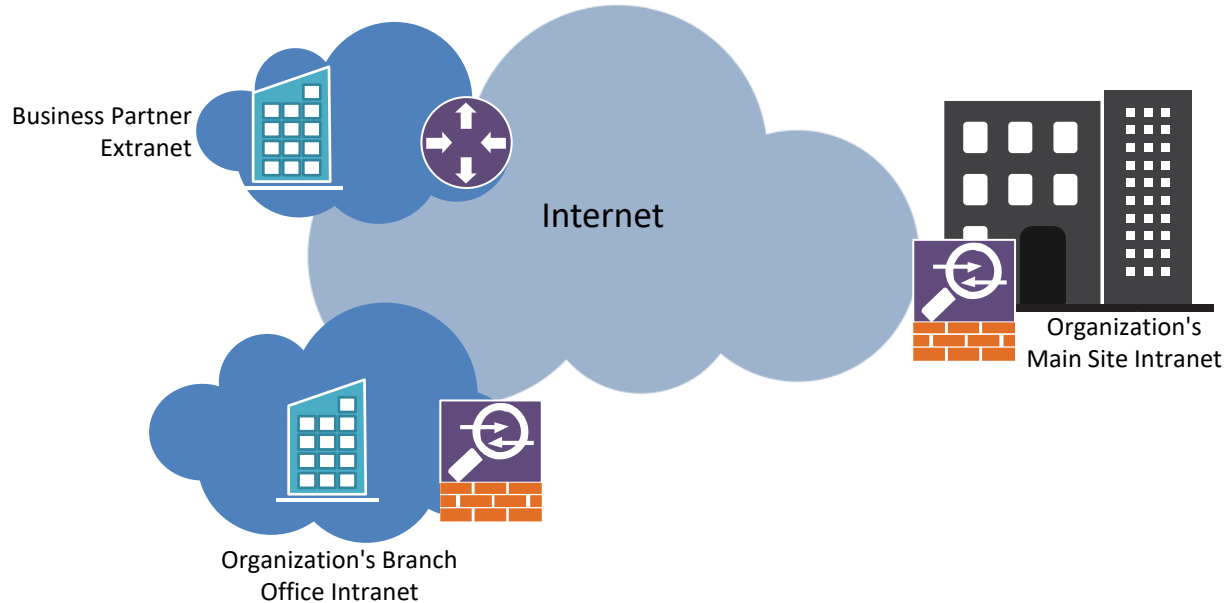
Zones and Topologies

- DMZ (Public Access Zone)
 - Contains systems with services that are accessed from outside the organization – FE servers, bastions (jump hosts), NAT gateways



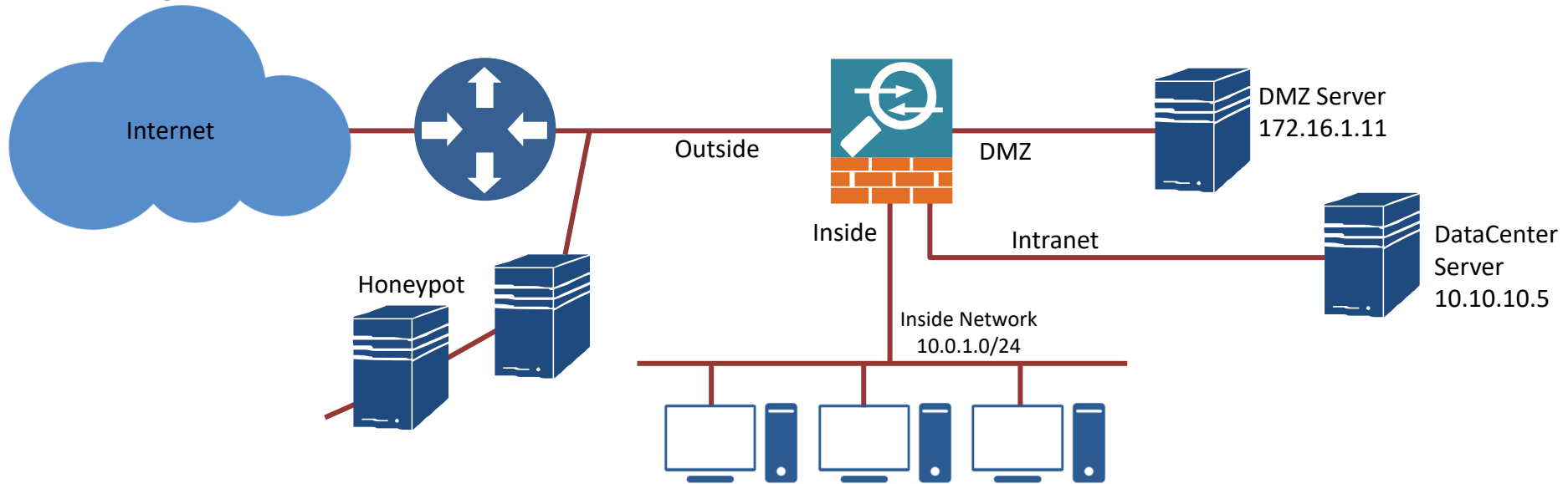
Zones and Topologies

- Extranet (PartnerNet)
 - A network with resources under the control of another organization that our organization needs access to



Zones and Topologies

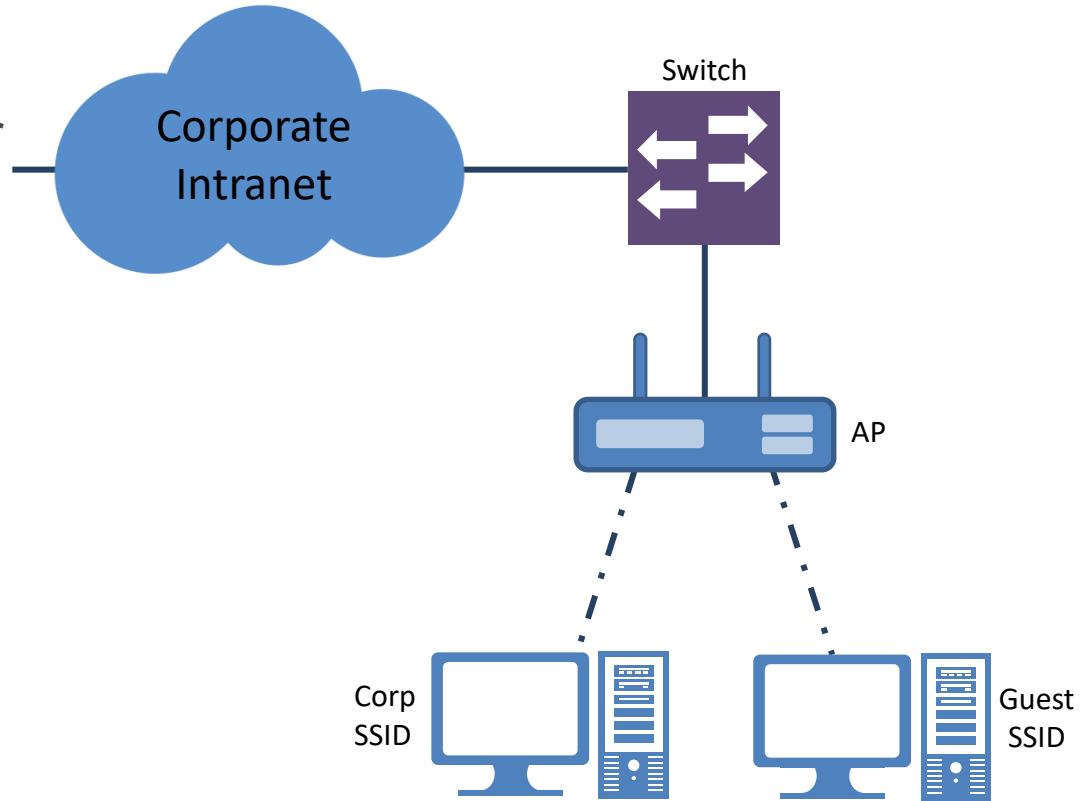
- Intranet
 - A network with resources under the control of our organization that our organization needs access to (HR, SharePoint, Policies, etc,)



Zones and Topologies

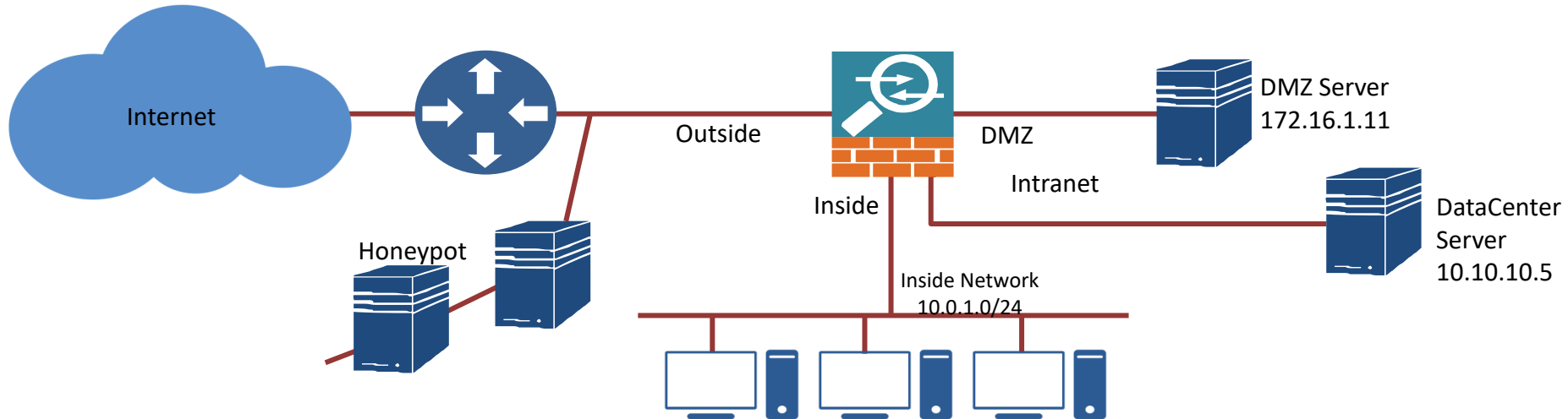
- Wireless

- Different wireless SSIDs for different functions
 - Guest/Captive portals
 - Limited connectivity to resources
 - Corporate
 - Full connectivity to resources
 - Conferencing
 - Restricted



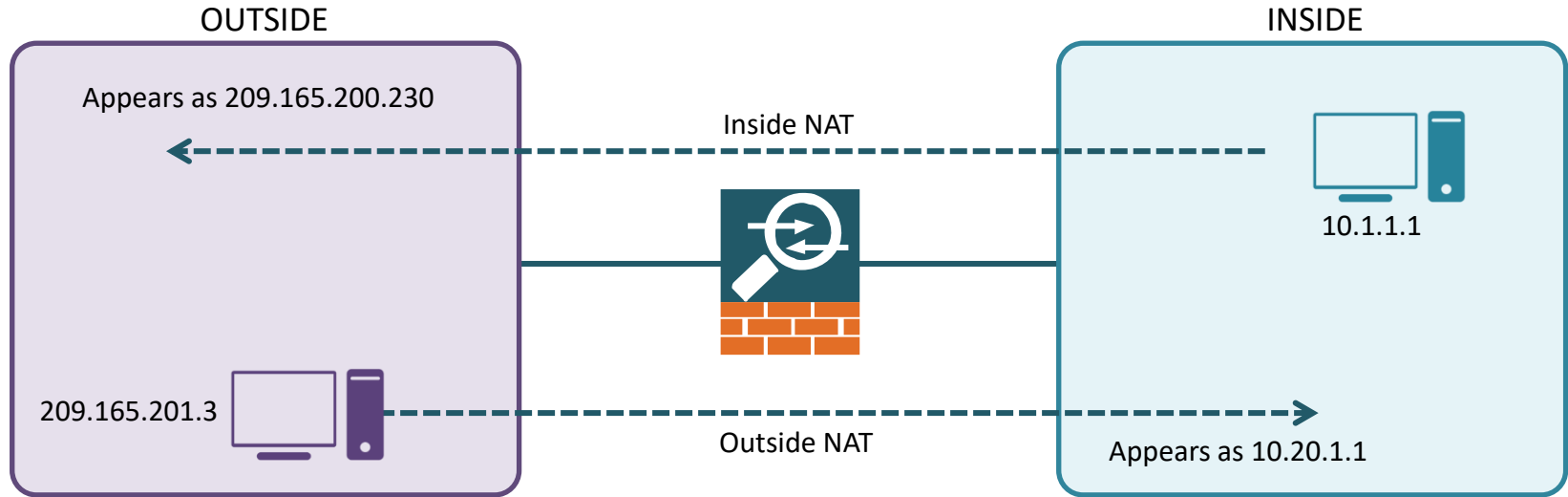
Zones and Topologies

- Honeypots and honeynets
 - Isolated sites and services with data that appears to be valuable to an attacker
 - Entice malicious users to connect
 - Track and log all activity



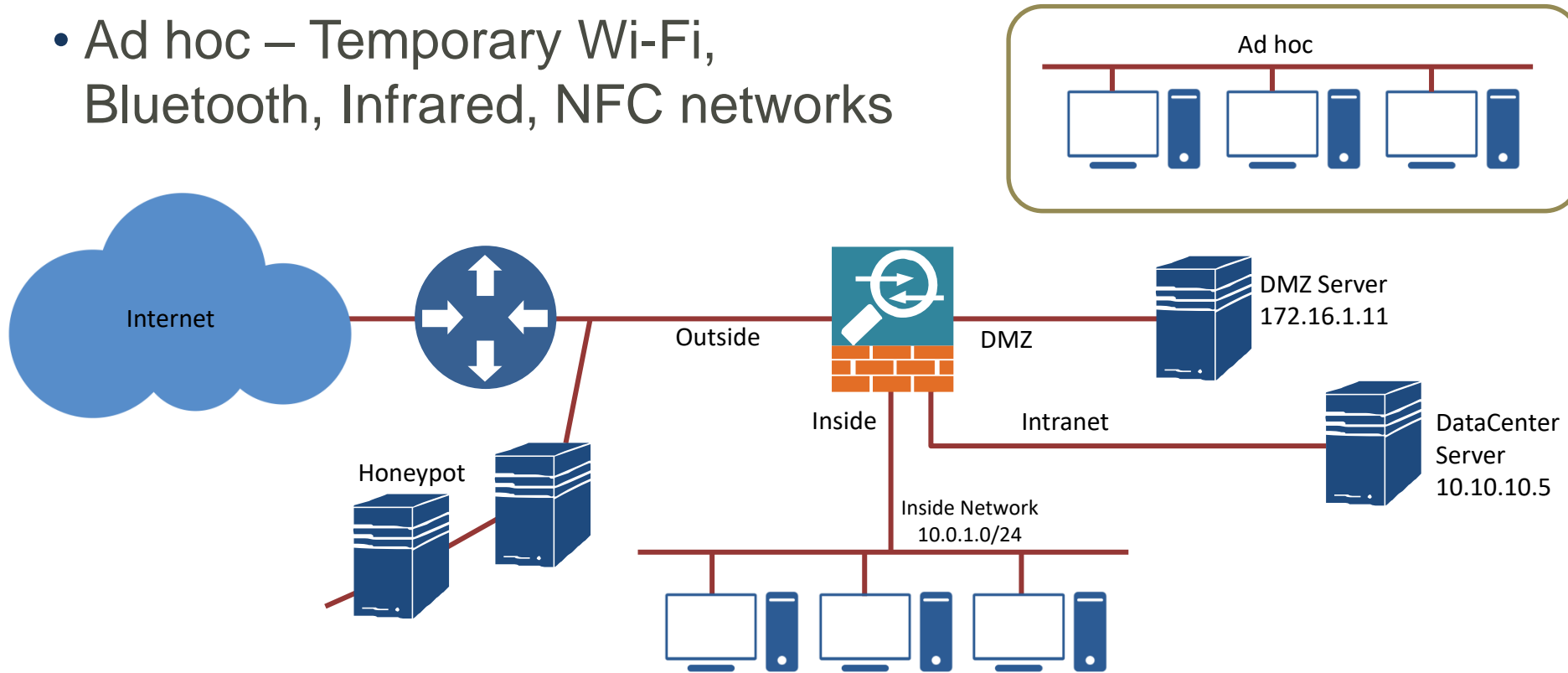
Zones and Topologies

- NAT – translate addresses between different zones or sites
 - Dynamic, Static, PAT, Dynamic PAT, Bidirectional (Twice)

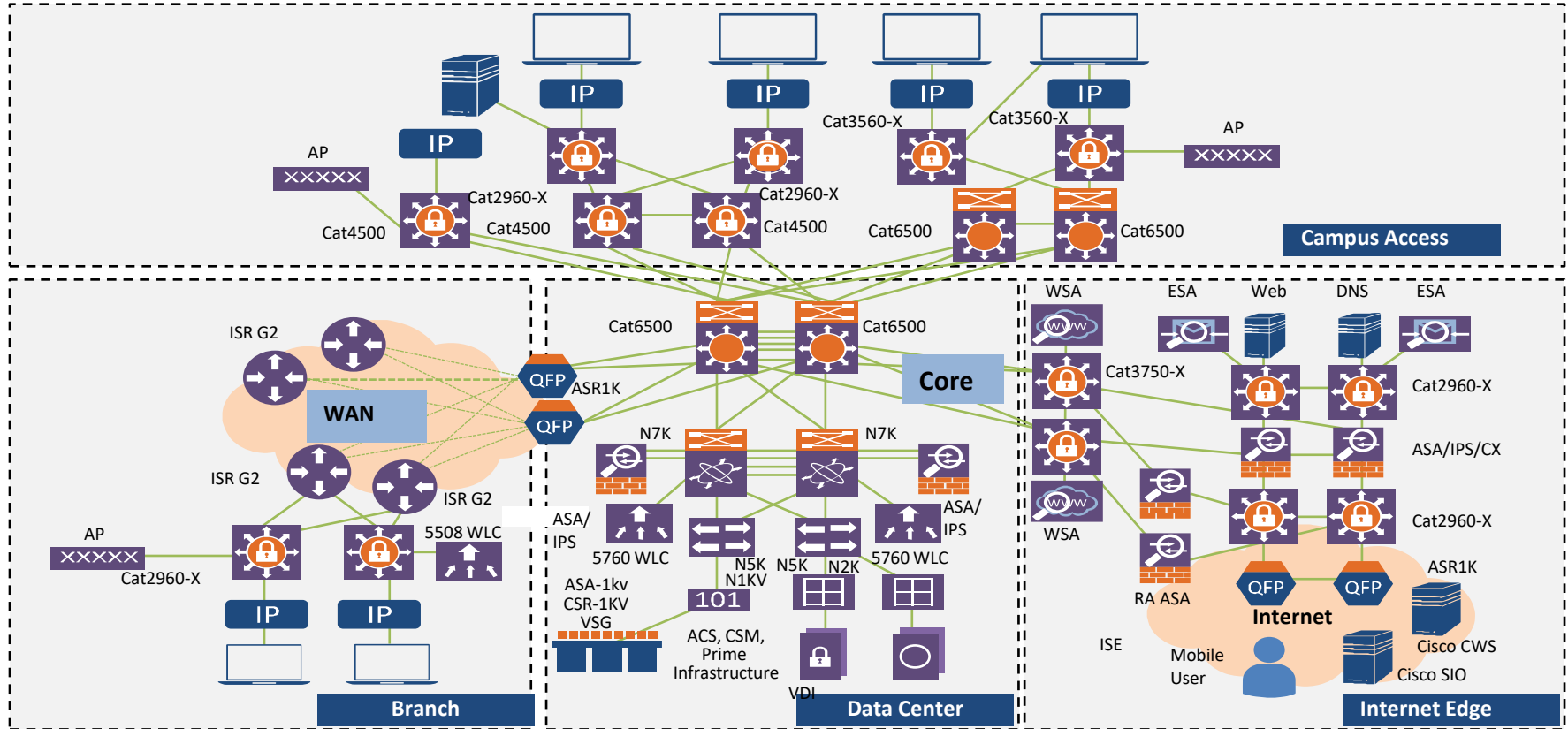


Zones and Topologies

- Ad hoc – Temporary Wi-Fi, Bluetooth, Infrared, NFC networks

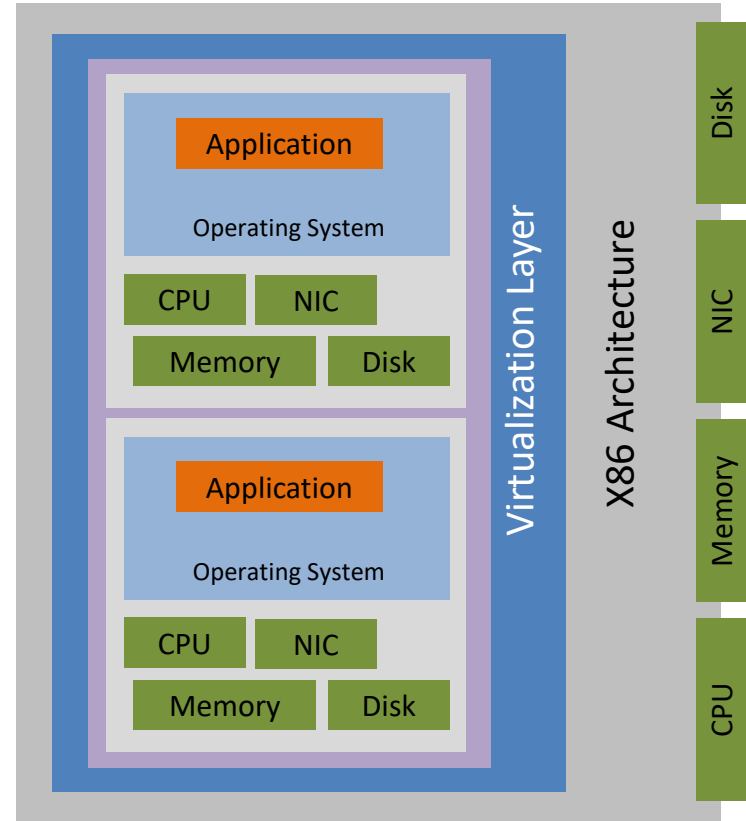


Segregation, Segmentation, and Isolation



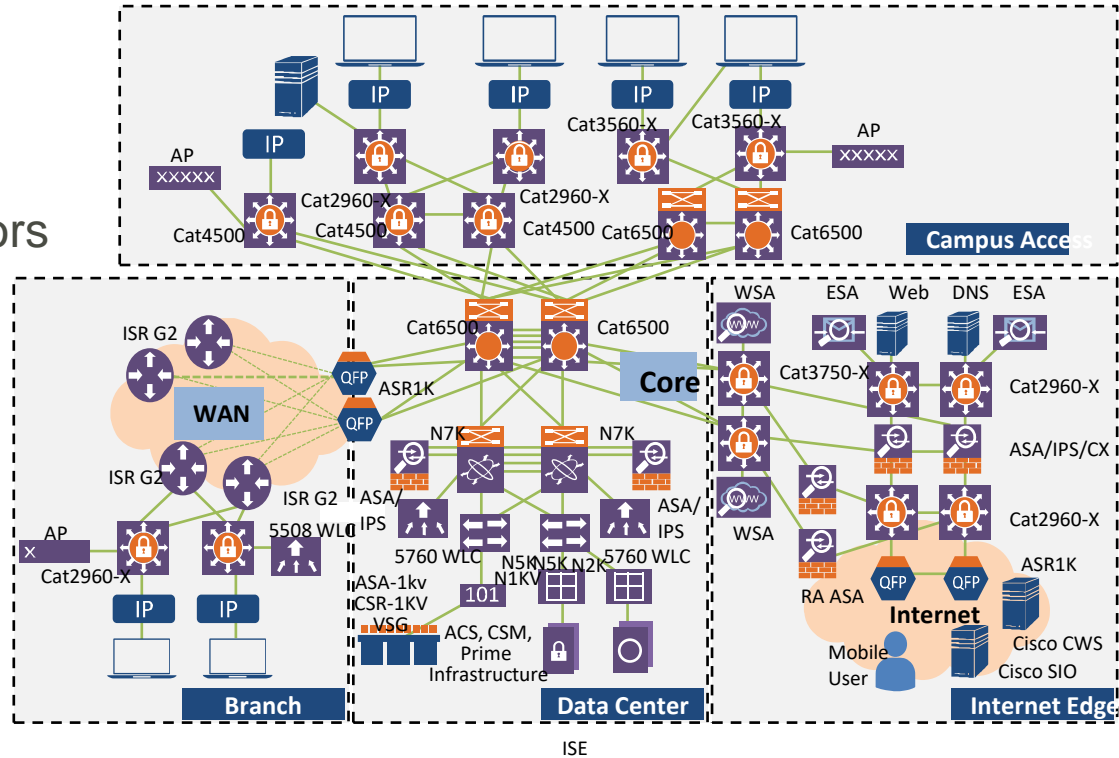
Segregation, Segmentation, and Isolation

- Virtualization - placing resources on the same physical server but separating them virtually
 - VMware vSphere
 - Red Hat Virtualization
 - Microsoft Hyper-V
 - Citrix Hypervisor
 - Oracle VM Server
 - KVM



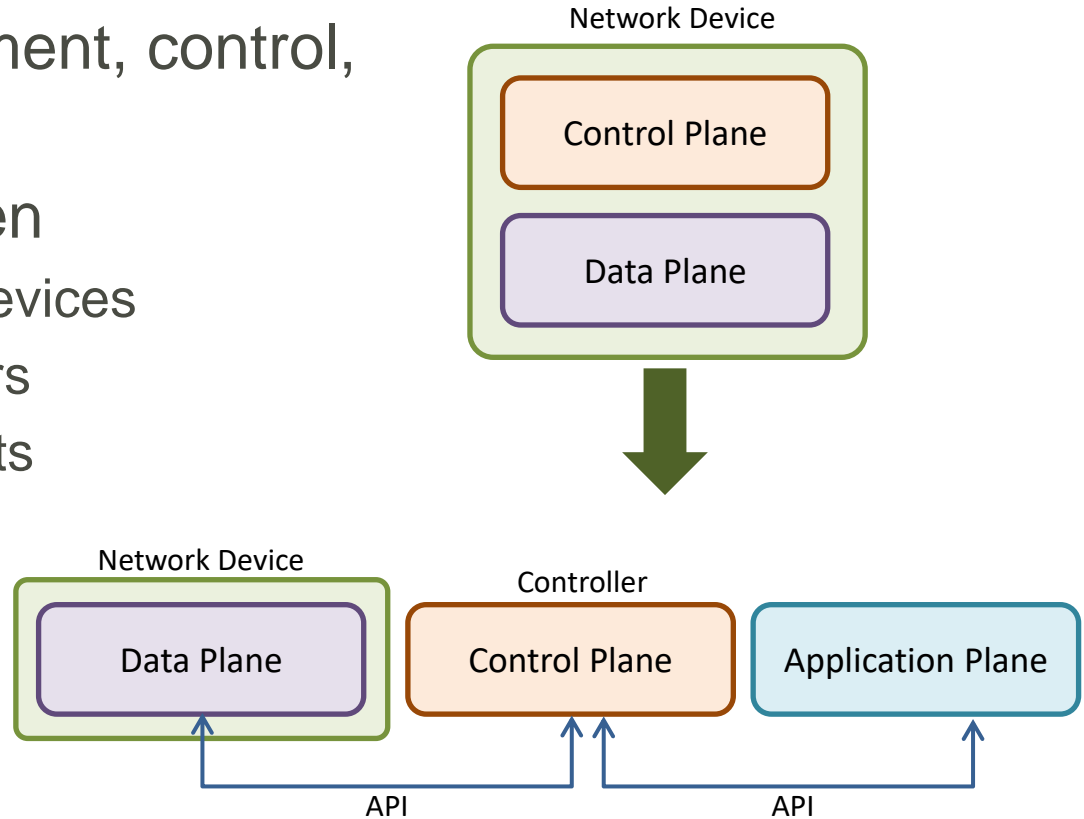
Device and Technology Placement

- Access and aggregation switches
- Routers and MLS
- Firewalls and VPN concentrators
- Sensors and collectors
 - IPS, SNMP, NetFlow, Syslog
- SIEM systems
- Filters and proxies
- SSL/TLS accelerators and listeners
- Load balancers
- Taps and port mirrors



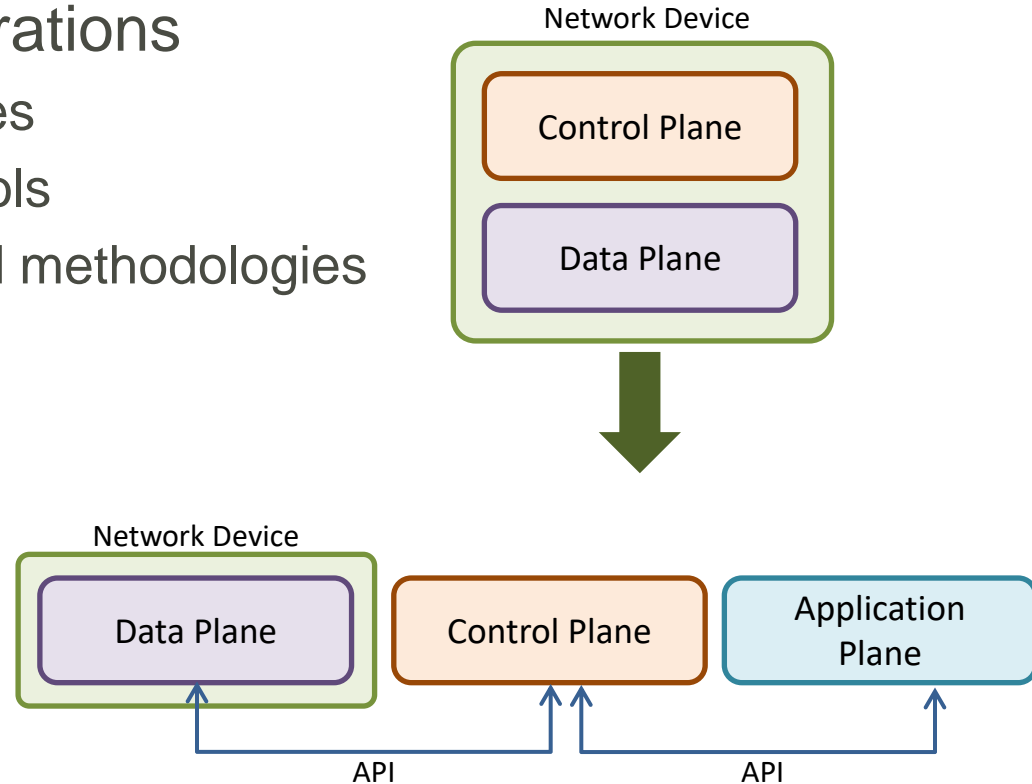
Software Defined Networking

- Separation of management, control, data traffic
- Communication between
 - Controllers and network devices
 - Applications and controllers
 - Admins and all components
 - Redundant controllers



Software Defined Networking

- Important security considerations
 - Clearly defined trust boundaries
 - Strict role-based access controls
 - Only use proven protocols and methodologies
 - Open standards
 - Evaluate CIA continuously
 - Secure all communications
 - Secure key management
 - Deny all by default
 - Accountability and traceability



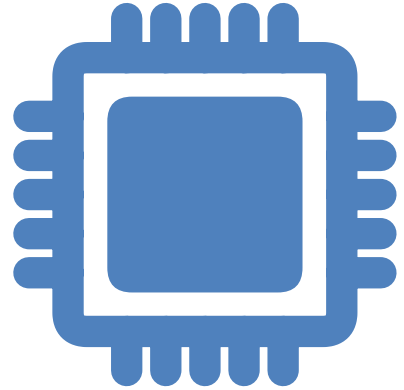
Hardware Root of Trust

- Hardware root of trust
 - Anchoring the trust worthiness of a system to hardware not software
 - Hardware solutions are more secure than software solutions
 - Less susceptible to attacks since security solutions are on-chip
- Foundations of a Trusted Execution Environments (TEE) or Trusted Computing (TC):
 - TPM – module embedded in a system
 - SED – self-encrypting drives
 - HSM – dedicated crypto processor



Hardware Root of Trust

- TPM – Trusted Platform Module
 - Computer chip (microcontroller)
 - Installed on the device or built into PCs, tablets, phones
 - Tamper-resistant security chip
 - Stores info needed to authenticate the platform
 - Passwords, certificates, encryption keys
 - 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)
 - Privacy (ensures system is protected from prying eyes)



Hardware Root of Trust

- SED – self-encrypting drives
 - FDE – full disk encryption
- Hardware-based data encryption
 - All contents on the drive are encrypted including keys at all times
 - Encrypts data as written, decrypts data as read
 - Invisible to the end user and can't be turned off
 - Less susceptible to threats when compared with software-based encryption
 - Stolen keys, repurposed drives, theft of device, end-of-life
 - Provides:
 - Pre-boot authentication, endpoint security, device authentication
 - Encryption, key management, network access control, policy compliance



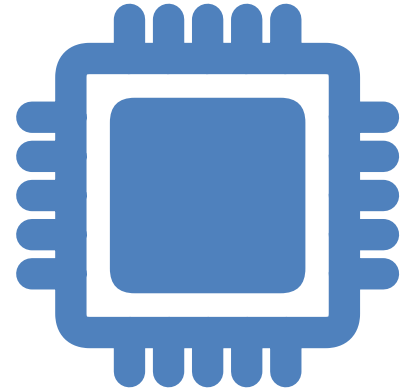
Hardware Root of Trust

- HSM – hardware security module
 - Dedicated crypto processor
 - Hardened, tamper-resistant device
 - Module in a PC, server
 - Dedicated appliance
 - Responsibilities
 - Managing, processing, generating, storing keys
 - Verifying digital certificates
 - SSL connection accelerator
 - Encrypting sensitive data
 - Verifying the integrity of stored data



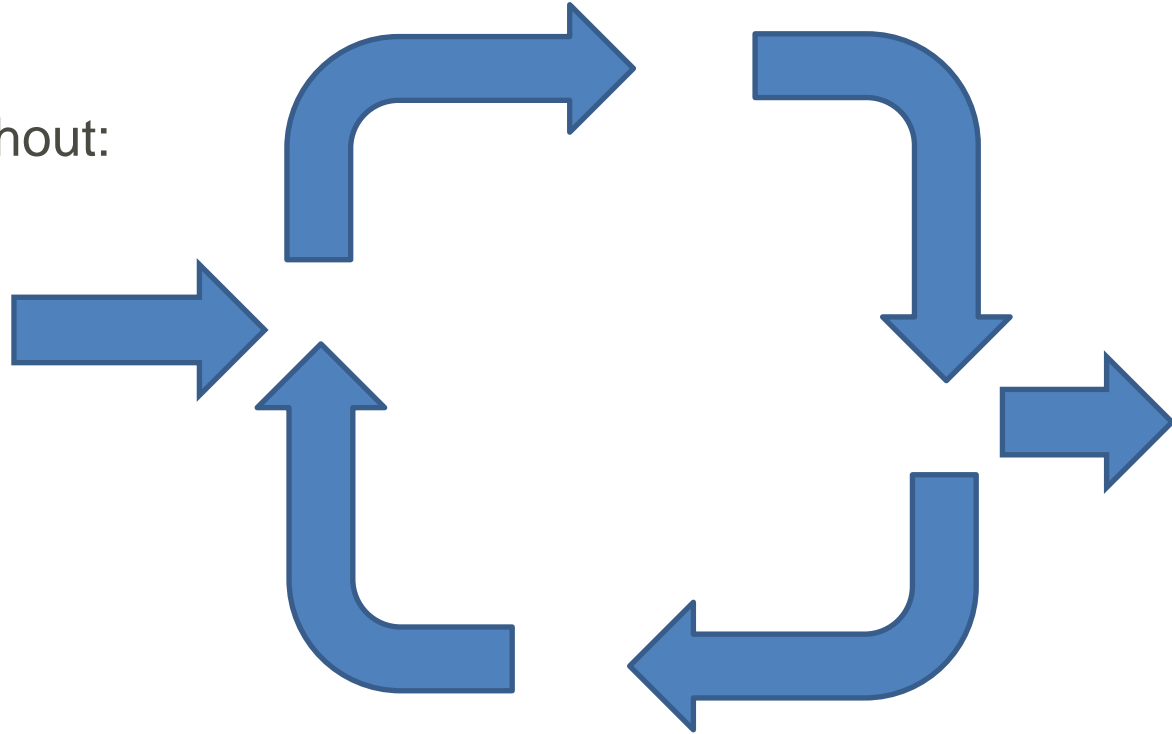
Secure Boot

- UEFI – Unified Extensible Firmware Interface
 - Replaces legacy BIOS (basic input/output system)
- Low-level software for booting the device
 - Tests hardware components (POST)
 - Gets the OS up and running
- Offers the ability to protect the device at a lower level with passwords
 - Restricts people from booting device
 - Restricts people from booting from removable devices
 - Prevents users from changing BIOS or UEFI settings without permission
 - Prevents users from booting other OSs or installing over current



Supply Chain

- Supply chain
 - Maintain security throughout:
 - Chain of custody
 - Least privilege access
 - Separation of duties
 - Persistent protection
 - Compliance
 - Testing and verification
 - User training



EMI and EMP

- EMI/EMP
 - Disturbance that affects an electrical circuit or short burst of energy
 - Disrupts and/or damages electronic equipment
 - Can be natural or man-made
 - RF waves, motors, lighting, lightning, explosion, sun, power surges, meteors, weapons
 - Protection
 - Shielded rooms
 - Shielded enclosures
 - Shielded components
 - Line filters
 - Surge protectors



Operating System Security Considerations

- Operating systems provide applications with access to hardware resources
 - This access must be tightly controlled and secured
 - Multiple processes will be running at the same time
 - Types
 - Network
 - Server
 - Workstation
 - Appliance
 - Kiosk
 - Mobile OS

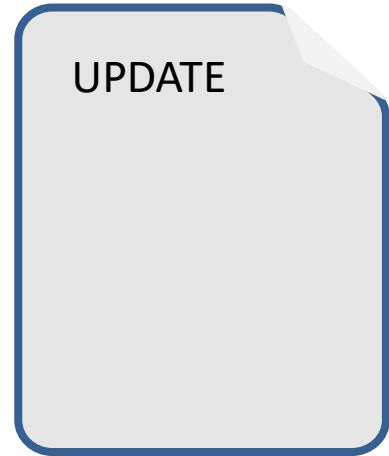
Linux

Microsoft

Windows

Operating System Security Considerations

- Patch management
 - Keeping the operating system up to date
 - When a bug is found, it needs to be fixed ASAP
- Least functionality
 - Prevent threats
 - Only design the systems for its intended purpose
- Application whitelisting/blacklisting
 - Controlling which applications are allowed and not allowed
 - Ensures only approved applications are installed on O/S



Operating System Security Considerations

- Secure configurations
 - Disabling unnecessary ports and services
 - Prevent attacks
 - Don't run a service or process if it is not needed on the device
 - Disable default accounts and passwords
 - Prevents hacking
 - Many OSs have a default admin account or root account
- Enable firewalls, IDS/IPS, anti-malware
 - Prevents unwanted access - many OSs have built-in features that should be enabled at a minimum
- Execute at user level unless elevated privileges are needed



Securing Peripherals

- Wireless keyboards
- Wireless mice
- Displays
- Wi-Fi-enabled MicroSD cards
- Printers
- Multi-function devices (MFD)
- External storage devices
- Digital cameras



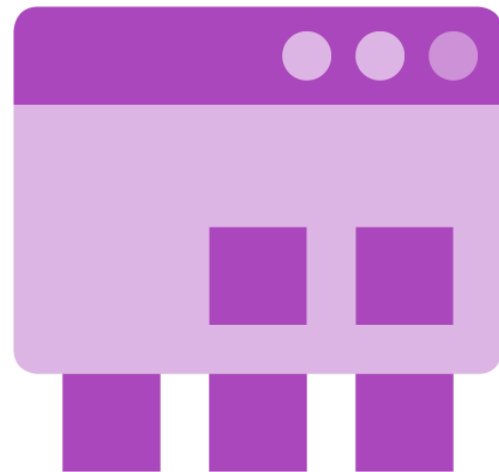
Secure Development Concepts

- Sandboxing
 - Testing new or untrusted software, code, or configurations in a separate environment to:
 - Protect production systems and data
 - Protect production code and malware
 - Protect production applications
 - Examples:
 - A physical or virtual test network
 - A virtual machine on a test PC or a production PC
 - Private Cloud deployments (AWS, GCP, Azure, IBM, Oracle)
 - Application containers (Docker and Kubernetes)



Secure Development Concepts

- Environments
 - Development
 - Where the work is done
 - Test
 - Where developed items are tested
 - Staging
 - Where integration is tested
 - Production
 - Where the fully tested solution meets the real world



Secure Development Concepts

- Secure baseline
 - Allows you to compare and contrast
 - What does it run like without the changes?
 - How is security without the changes?
 - What does it run like with the changes?
 - How is security with the changes?
 - » What is the impact to security once changes have been applied?
 - Documentation of change impact
 - Must be able to revert back to baseline (fallback)
 - Virtual machine and drive snapshots
 - Source code versioning
 - Integrity Measurements (at rest, in transit, in use)



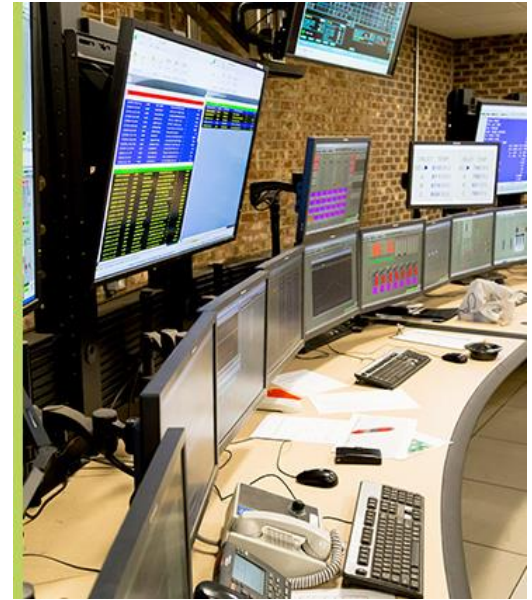
Supervisory Control and Data Acquisition (SCADA)

- SCADA – subset of industrial control systems (ICS)
 - Control and management system architecture
 - Water management systems
 - Electric power companies
 - Traffic signals
 - Mass transit systems
 - Environmental control systems
 - Manufacturing systems



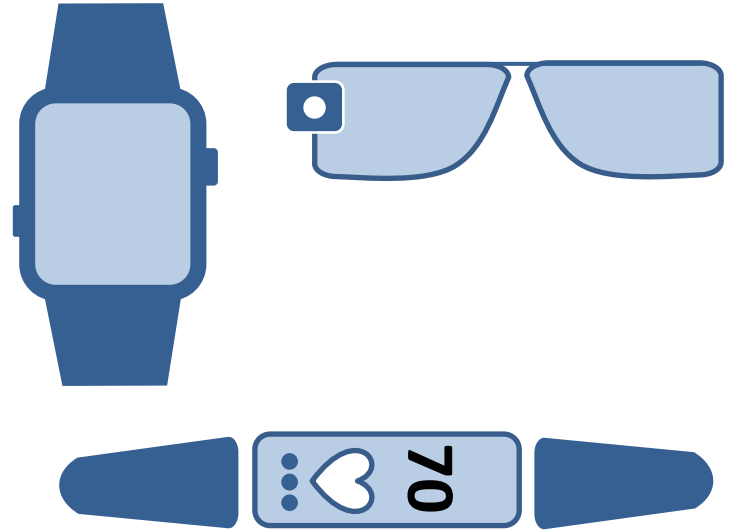
SCADA Security Concerns

- Cyber-terrorism/cyber-warfare/espionage and sabotage
 - Lack of security in design, operation, deployment
 - Lack of authentication between devices
 - Lack of authentication for users
 - Lack of security in proprietary protocols, services, and applications
 - Internet connectivity



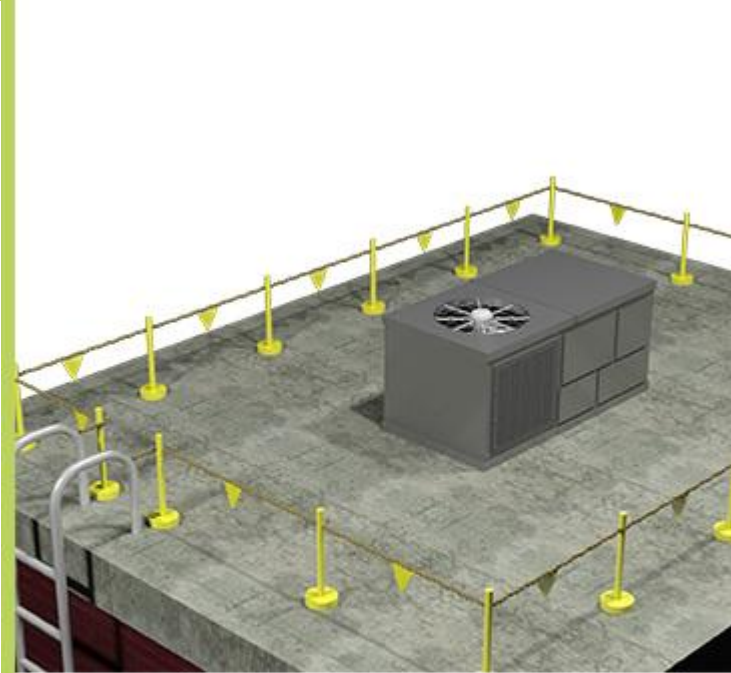
SCADA, IoT, and HVAC

- Smart devices/IoT
 - Wearable technology
 - Home automation
- Security is not a top priority
 - Privacy concerns
 - Lack of authentication and/or authorization
 - Lack of encryption
 - Poor application design
 - Lack of updates



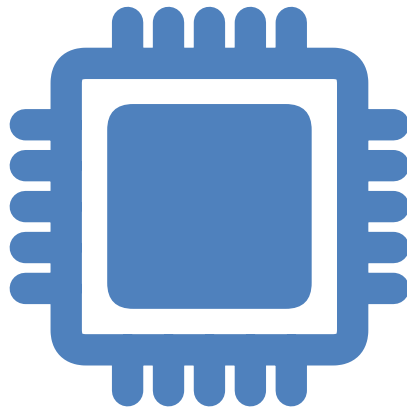
SCADA, IoT, and HVAC

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



SoC and RTOS

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



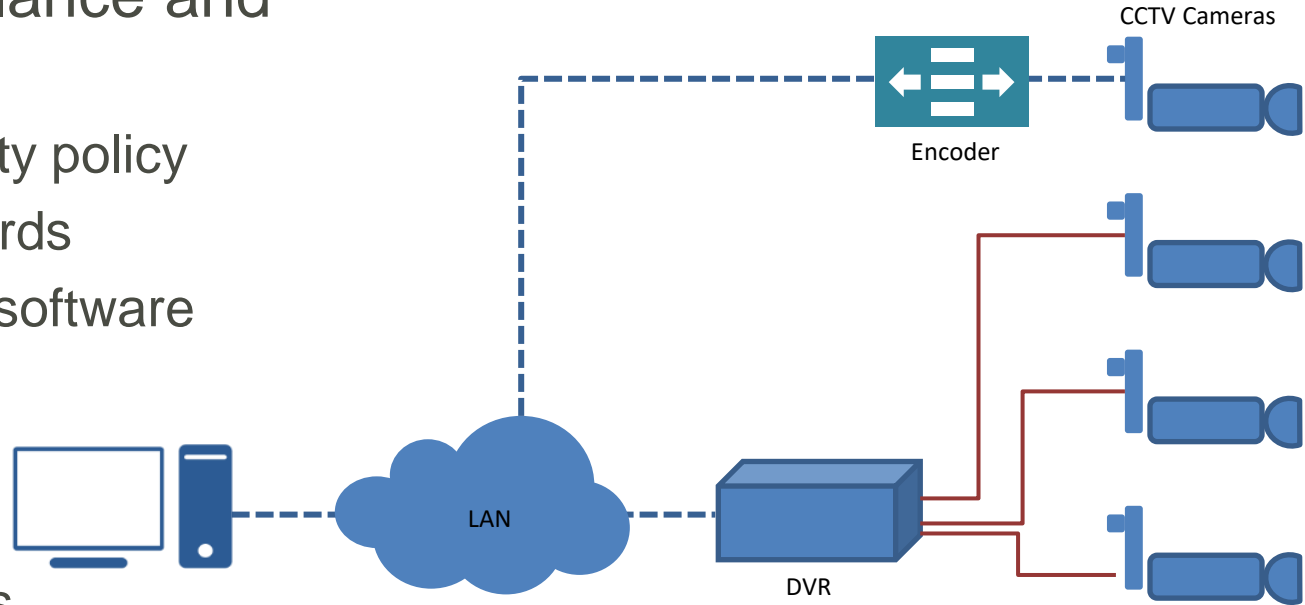
SoC and RTOS

- RTOS – real-time operating system
 - OS that serves real-time applications
 - Processes data immediately
 - Tenths of seconds
 - Security concerns
 - Code injection
 - Privacy
 - Exploiting shared memory
 - Priorities
 - DoS attacks
 - Inter-process communications



Camera System Concerns

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



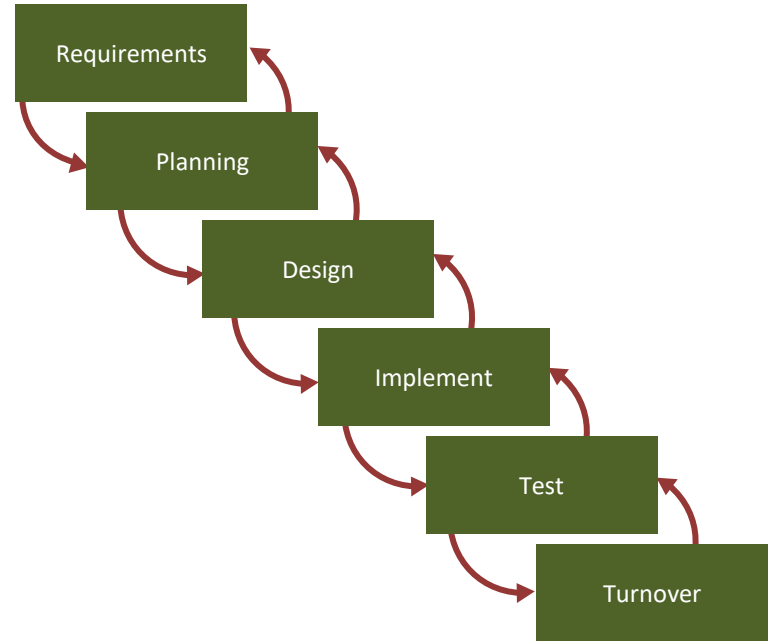
Additional Devices and Security Concerns

- Medical devices, vehicles, aircraft and drones (UAVs)
 - Privacy
 - Track, gather info about you
 - Safety
 - Remote access, take over



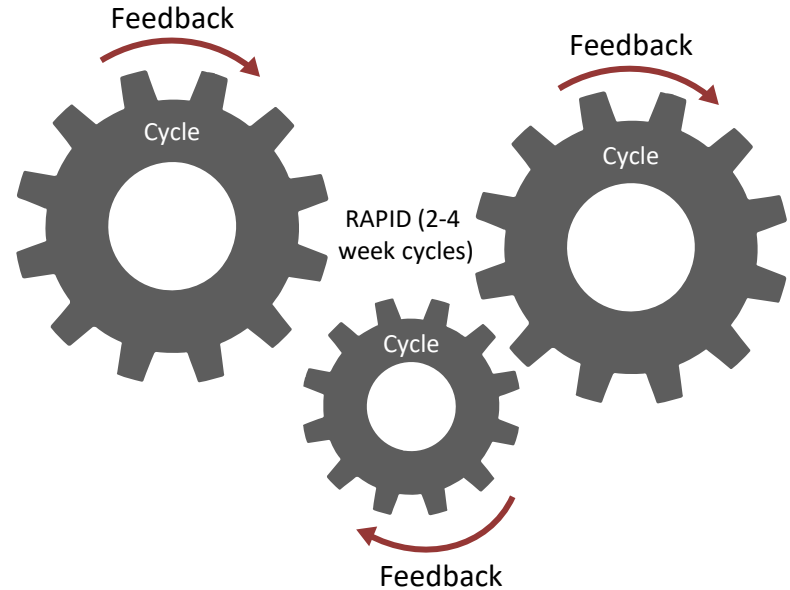
Development Life Cycle Models

- Waterfall
 - Sequential approach – often measured in years
 - Output of each phase is the input to the next phase
 - Little flexibility, not adaptable, very predictable, testing done in the end



Development Life Cycle Models

- Agile
 - Evolutionary approach – measured in weeks
 - Collaboration of cross-functional teams
 - Very flexible, adaptable, not predictable, testing done during development



Secure DevOps

- Security automation
 - Offers consistency and greater frequency
- Continuous integration
 - Consistently improving and updating your software at a high standard
- Baselining
 - A method of building upon an existing verified product (code)
 - A method of ensuring integrity is maintained
 - Trusted base









Secure DevOps

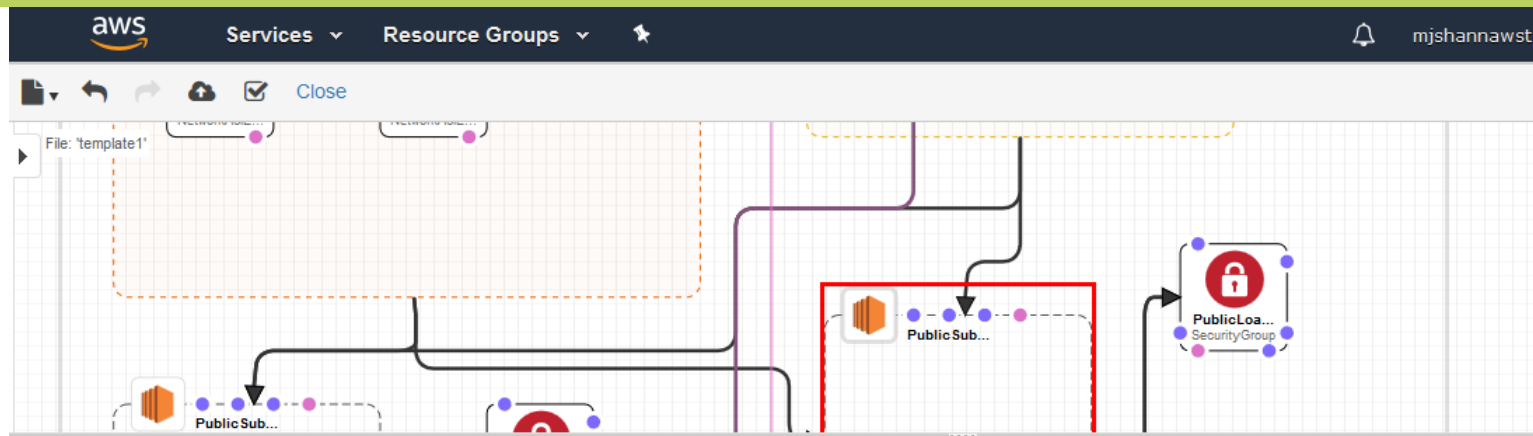
- Immutable systems
 - The process of replacing instead of patching
- Infrastructure as code
 - Infrastructure treated the same as code is treated
 - Example: AWS Cloud Formation



Infrastructure as Code

Template Name	Description	View	View in Designer	Launch
A single Amazon EC2 in an Amazon VPC	Creates a VPC and adds an Amazon EC2 instance with an Elastic IP address and a security group.	View	View in Designer	Launch Stack 
Amazon VPC with static routing to an existing VPN	Creates a private subnet with a VPN connection that uses static routing to an existing VPN endpoint.	View	View in Designer	Launch Stack 
Autoscaling and load-balancing website in an Amazon VPC	Creates a load balancing, auto scaling sample website in an existing VPC.	View	View in Designer	Launch Stack 
Amazon VPC with DNS and public IP addresses	Creates a VPC with DNS support and public IP addresses enabled.	View	View in Designer	Launch Stack 
Publicly accessible Amazon EC2 instances that are in an Auto Scaling group	Creates a load balancing, autoscaling group with instances that are directly accessible from the Internet.	View	View in Designer	Launch Stack 
Amazon EC2 with multiple dynamic IP addresses in an Amazon VPC	Creates an Amazon EC2 instance with multiple dynamic IP addresses in a VPC.	View	View in Designer	Launch Stack 

Infrastructure as Code



temp...

Choose template language: ☒ JSON ☐ YAML

```
1 {
2   "AWSTemplateFormatVersion": "2010-09-09",
3   "Description": "AWS CloudFormation Sample Template VPC_AutoScaling_With_Public_IPs.template: Sample template showing how to create a load
4   "Parameters": {
5     "KeyName": {
6       "Description": "Name of an existing EC2 KeyPair to enable SSH access to the instances",
7       "Type": "AWS::EC2::KeyPair::KeyName",
8       "ConstraintDescription": "must be the name of an existing EC2 KeyPair."
9     },
10    "SSHLocation": {
11      "Description": "Lockdown SSH access to the bastion host (default can be accessed from anywhere)",
12      "Type": "String",
13      "MinLength": "8",
14
```


Development Concepts

- Version control
 - Track changes to code
 - Document who, what, when, why
- Change management
 - Direct, control, and support changes in code efficiently
 - Planned or unplanned
- Provisioning and deprovisioning
 - Providing or removing software access to employees, customers, partners, and contractors



Secure Coding Techniques

- Proper error/exception handling
 - Captured in logs, protect the logs, and hide from users
- Proper input validation
 - Verifying the input before entering it into the system
- Normalization
 - Ensuring there is no redundancy in data, and that like items are stored together



Secure Coding Techniques

- Stored procedures
 - Precompiled groups of code, statements, and commands that can be called at a later time
- Code signing
 - Digitally signing code to prove author and ensure integrity
- Encryption
 - Ensure the confidentiality of the code in transit, at rest, in use



Secure Coding Techniques

- Obfuscation/camouflage
 - Deliberately use code that humans have a hard time understanding
- Code re-use
 - Already existing, tested, validated code can be used again
- Dead code
 - Remove unnecessary, inoperative code



Secure Coding Techniques

- Server-side vs. client-side execution and validation
 - Both are acceptable
 - Client-side is more efficient
 - Server-side is more secure
- Memory management
 - Allocate memory/buffer when needed, release it for re-use when no longer needed
- Use of third-party libraries and SDKs
 - May violate user's privacy, may damage the quality of the application

Secure Coding Techniques

- Data exposure
 - What information can and can't be shared internally and externally?
 - Critical in database and storage applications
 - Strict access controls
 - Digitally sign all API calls
 - Use abstracted views instead of direct access



Code Quality and Testing

- Static code analyzers
 - Analysis performed on non-executed code
- Dynamic analysis
 - Analysis performed on executed code
 - Fuzzing – using malformed inputs to determine how application responds
 - Find unexpected input validation errors
- Stress testing
 - Testing the application beyond its intended limits

Code Quality and Testing

- Sandboxing
 - Testing the code in an isolated environment
- Model verification
 - Did we build it right to meet the needs?
 - Did we perform the right tests and enough tests?



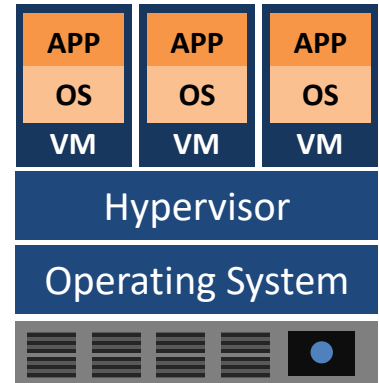
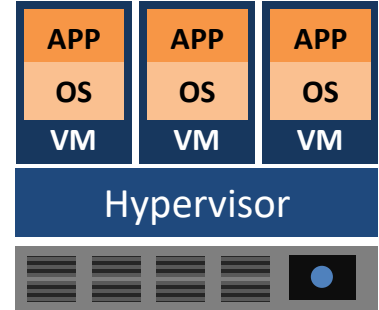
0101010

Compiled vs. Runtime code

- Compiled code
 - Source code that is converted into machine code
 - Detection of syntax errors
 - Dependencies are verified
 - Libraries
 - Connectors
 - Header files
- Runtime code
 - The machine code that is running when the user is using the software
 - Detection of logic errors

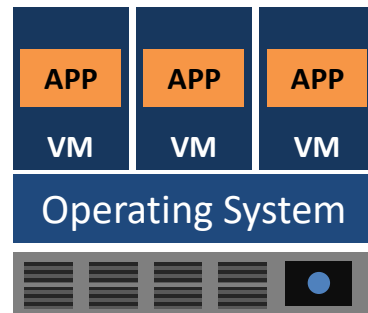
Hypervisors

- Software that runs virtual machines
 - Controls interaction between the VMs and the hardware
- Type I – (bare-metal or native)
 - Runs directly on the underlying hardware
 - XenServer, KVM, Hyper-V, ESXi
- Type II – (hosted)
 - Runs on the OS installed on the hardware
 - Oracle VirtualBox 6, VMWare Player/Workstation



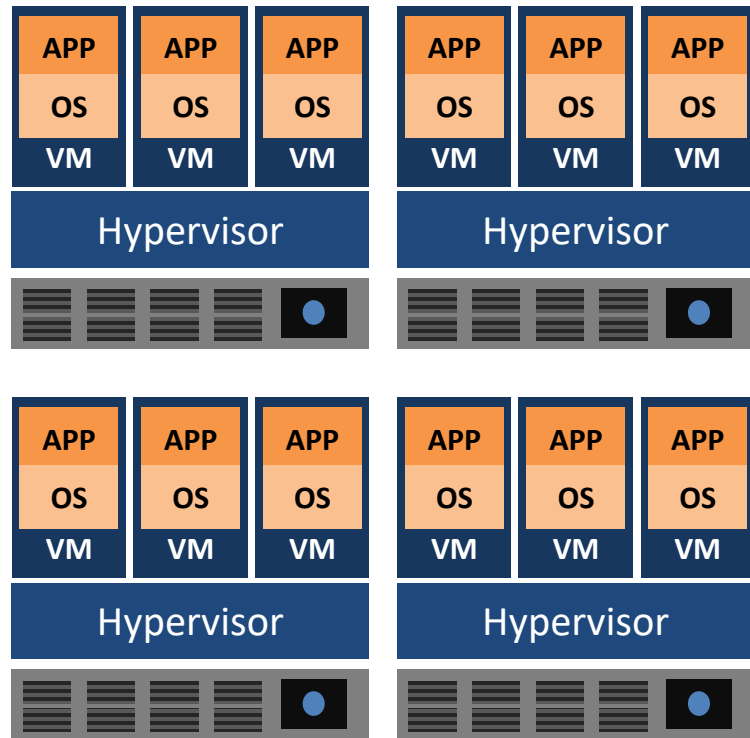
Hypervisors

- Application cells/containers
 - Abstracting applications from the platform into containers
 - Provides portability and isolation
 - Less overhead than VM
 - Docker and Kubernetes are common container platforms



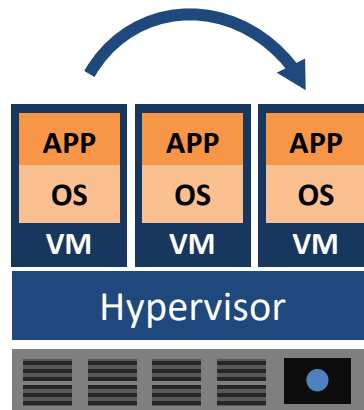
VM Sprawl and Escape

- VM sprawl
 - When the number of VMs overtakes the admin's ability to manage them and the available resources
- VM sprawl avoidance
 - Enforce a strict process for deploying VMs
 - Have a library of standard VM images
 - Archive or recycle under-utilized VMs
 - Implement a Virtual Machine Lifecycle Management tool



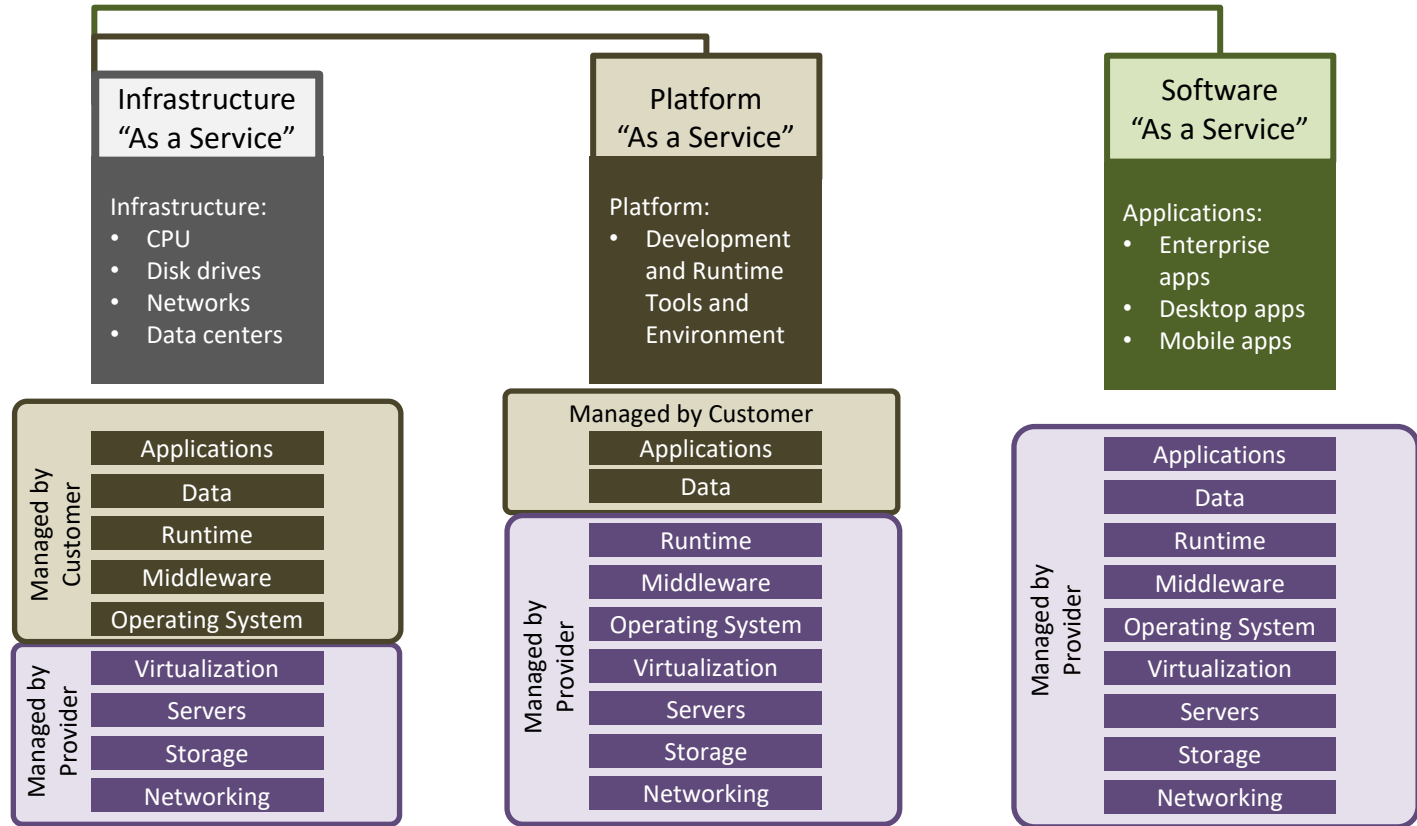
VM Sprawl and Escape

- VM escape
 - When a process running in the VM interacts directly with the host OS
 - Serious threat to VM security
- VM escape protection
 - Patch VMs and VM software regularly
 - Only install what you need on the host and the VMs
 - Install verified and trusted applications only
 - Use strong passwords
 - Control VM access



Cloud Computing Types

- IaaS
- PaaS
- SaaS



Cloud Deployment Models

- Private
 - Deployed within the organization by the organization for the organization
- Public
 - Deployed by a provider within their organization for other organizations to use
- Community
 - Private or public but only shared between trusted groups
- Hybrid
 - Combination of public and private

Cloud Storage Models

On-premise

- Build your own network and storage
- High investment costs
- High operational costs
- Backup your own data
- Access depends on budget
- Availability depends on budget

Hosted

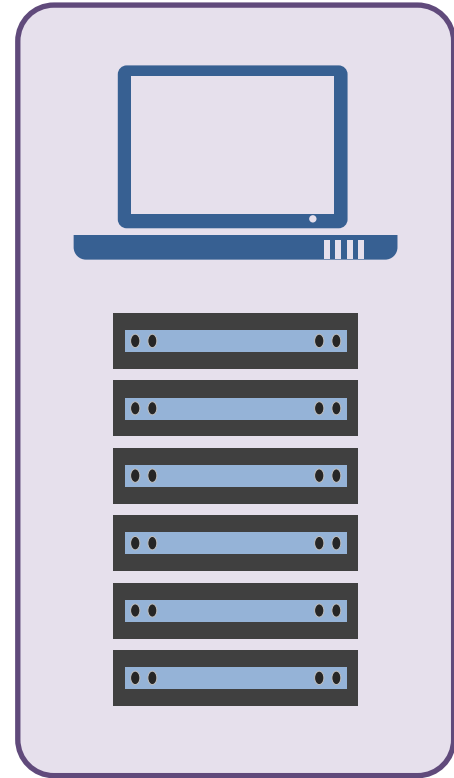
- Lease network and storage
- No investment costs
- Medium operational costs
- Backups performed for you
- Access depends on implementation
- Availability depends on implementation

Cloud

- Lease network and storage
- No investment costs
- Low operational costs
- Backups performed for you
- Access anywhere anytime
- Highly available
- Mobility

Virtual Desktop Infrastructure

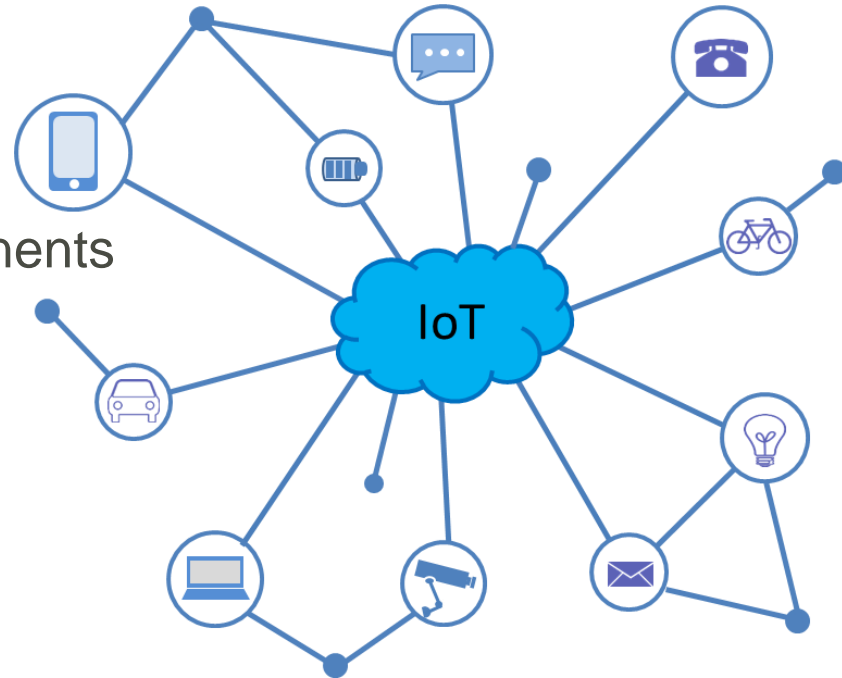
- VDI/VDE stands for Virtual Desktop Infrastructure/Virtual Desktop Environment
 - Desktop is hosted as a VM on a server in a data center
 - All updates, backups, processing done on server
 - Desktop is accessed from a PC, thin client, or mobile device
 - Minimal resources required with no local data stored



Internet of Things (IoT) Security

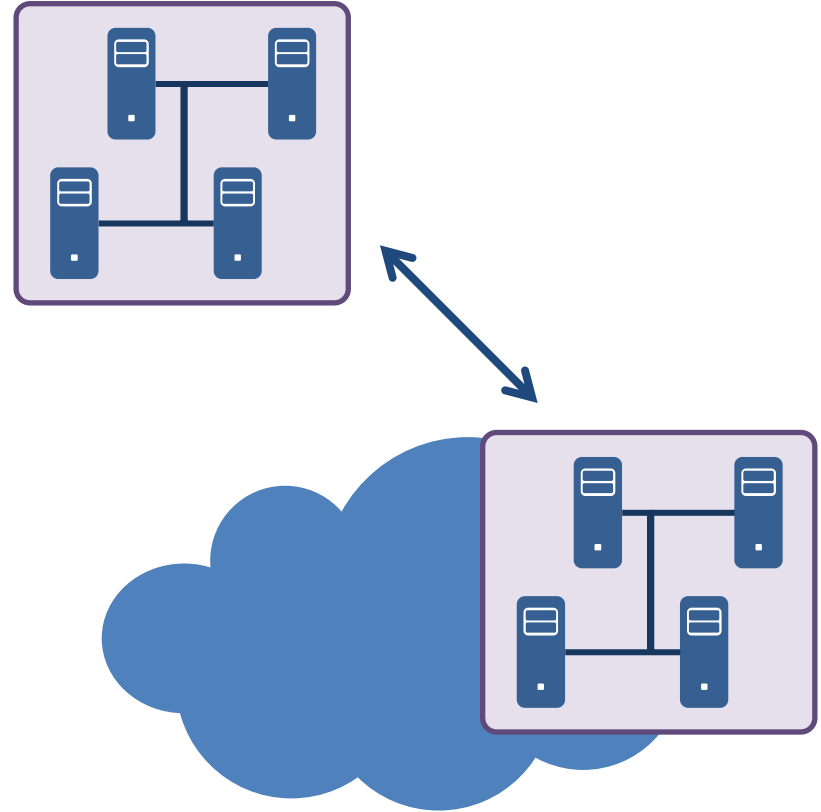
- OWASP Top 10 IoT Vulnerabilities

1. Weak, guessable, or hardcoded passwords
2. Insecure network services
3. Insecure ecosystem interfaces
4. Lack of secure update mechanisms
5. Use of insecure or outdated components
6. Insufficient privacy protection
7. Insecure data transfer and storage
8. Lack of device management
9. Insecure default settings
10. Lack of physical hardening



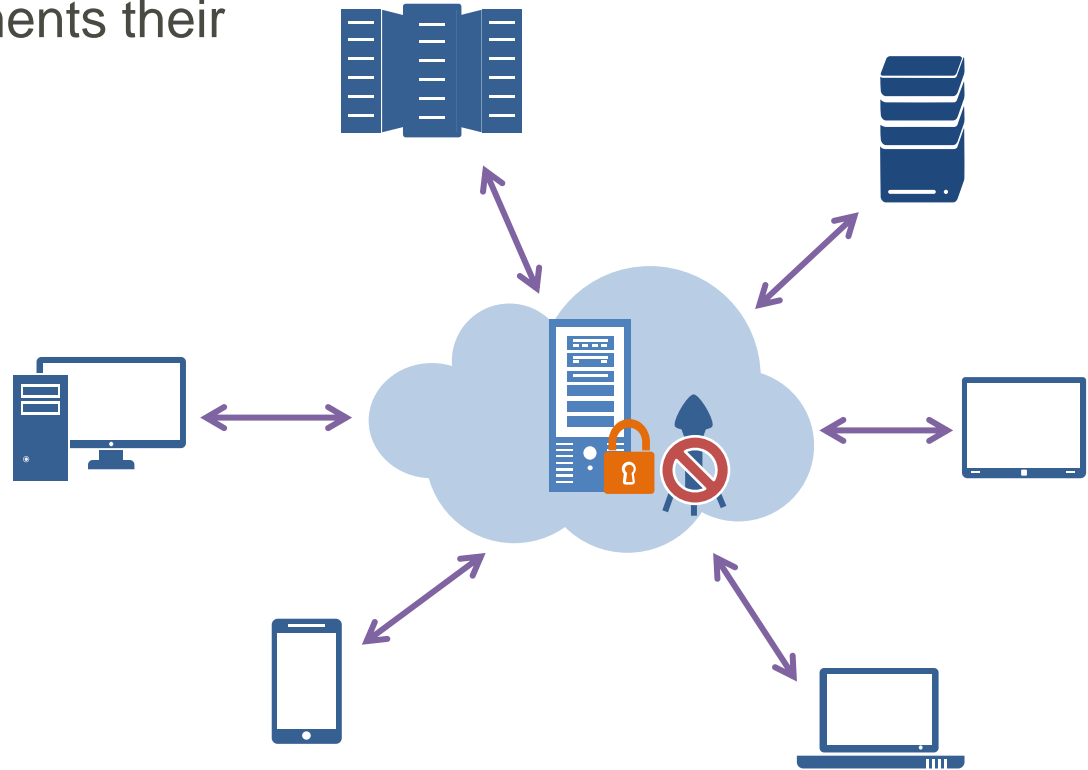
Cloud Access Security Broker (CASB)

- Cloud access security broker
 - Software service implemented between cloud customer and provider
 - Could be on-premise or in-service provider cloud
- Acts as a gatekeeper
 - Used to enforce enterprise security policies while cloud resources are being accessed
 - Extends organizations policies beyond local infrastructure
- Provides visibility, compliance, data security, threat protection



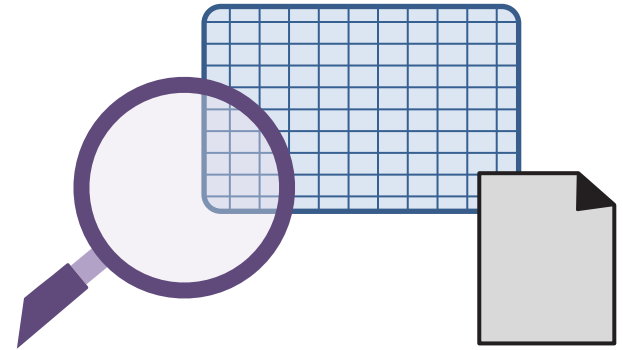
Security as a Service (SECaaS)

- A provider (MSSP) implements their security services into your environment via the cloud
 - Subscription based
 - cost effective solution
- Offerings
 - Authentication
 - Anti-virus
 - Anti-malware
 - IDS
 - Event management



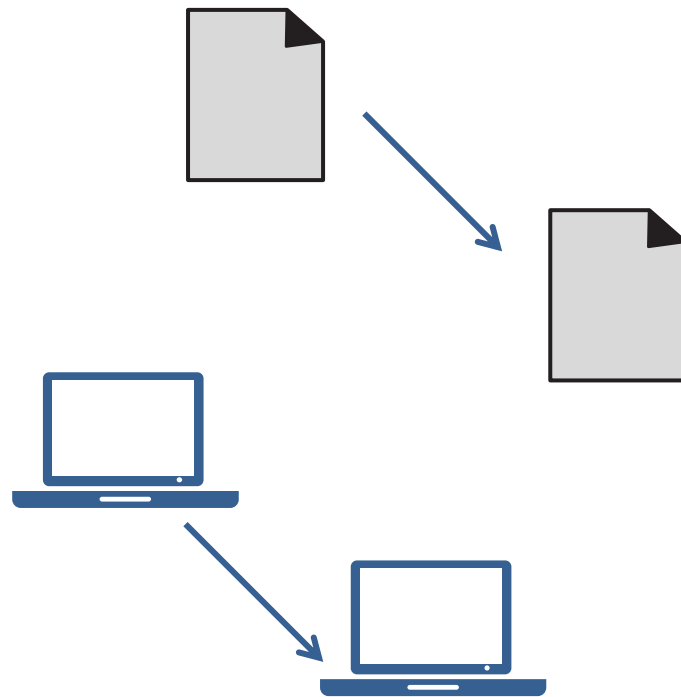
Automation and Scripting

- Automation
 - Automated Courses of Action (ACOA)
 - Automatic actions taken when cyber attack occurs
 - Continuous monitoring
 - Catch errors or faults early
 - Configuration validation
 - Reduce/detect human errors
- Scripting
 - Reduce human error when repetition exists



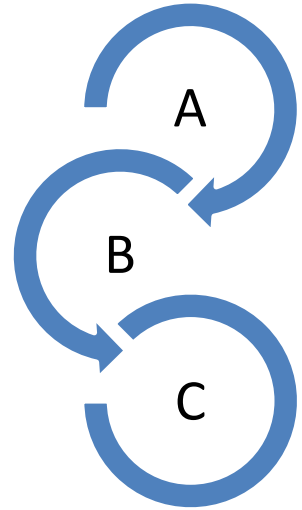
Templates and Master Image

- Templates
 - Reduce human error when repetition exists
 - Configuration templates
 - Coding templates
- Master image
 - “Single source of truth”
 - Reduces human error when repetition exists
 - Operating system image
 - Application image
 - Infrastructure image (SDN, CSP)



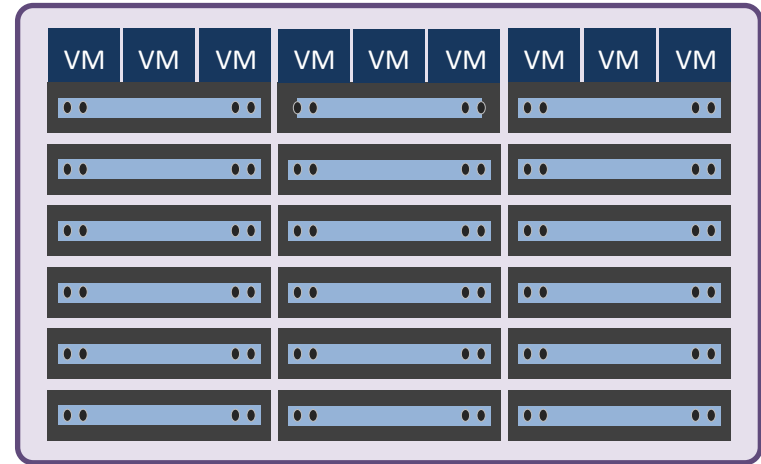
Resiliency Considerations

- Non-persistence
 - When settings or data are not saved at the end of a session
- Snapshots
 - Image of the state of a system at specific points in time
- Revert to known state
 - Restore system to a previous known good state that worked
- Roll back to known configuration
 - Revert system configuration to a state that worked
- Live boot media
 - Run the operating system from a CD/flash drive
- Repair broken systems

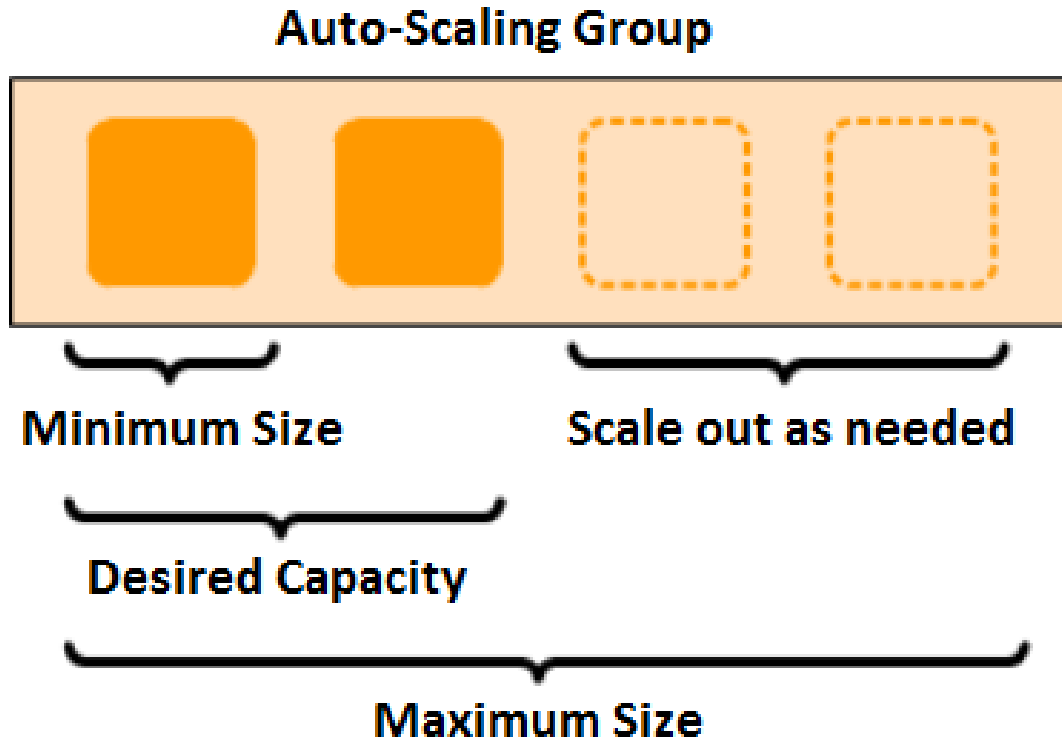


Adjusting to Demands

- Elasticity
 - Adapt based on the current demands
 - Automatically provision and de-provision resources as needed
- Scalability
 - The ability to enhance the functionality of the system by adding additional resources easily
 - CSPs offer auto-scaling groups behind load balancers

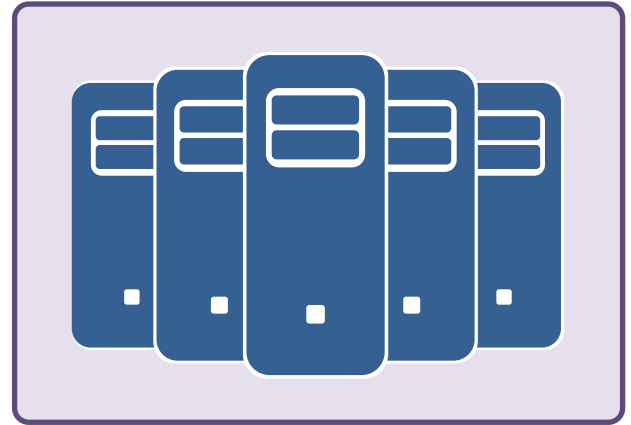


CSP Auto-Scaling



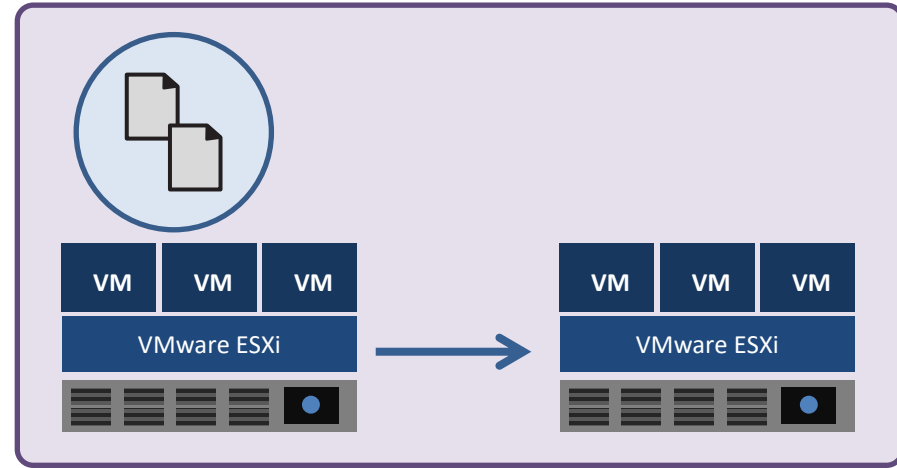
Adjusting to Demands

- Distributive allocation
 - Multiple systems, resources, processes being used at the same time to service a request
 - Working as a single unit
 - Maximizing performance
 - If a system, resource, process fails the others take on the additional load
 - Providing high availability through fault-tolerance



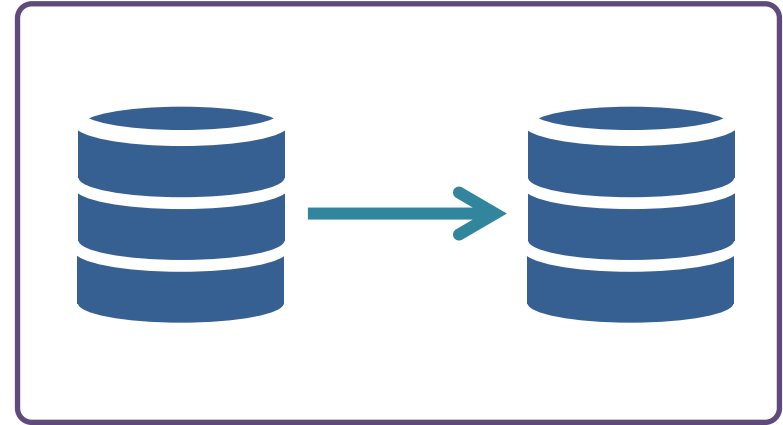
High Availability

- High availability
 - Ensure continuous operation and minimize downtime
- Fault-tolerance
 - Continue operation when failures occur
- Redundancy
 - Duplication of critical components
 - If one fails, the other can assume responsibility
 - Power supplies, interfaces, devices, locations, connections



RAID

- RAID - **R**edundant **A**rray of **I**ndependent **D**isks
 - Provides performance enhancement
 - RAID 0
 - Provides resiliency and fault-tolerance
 - RAID 1 - mirroring
 - RAID 5 - striping with parity
 - RAID 6 - striping with double parity



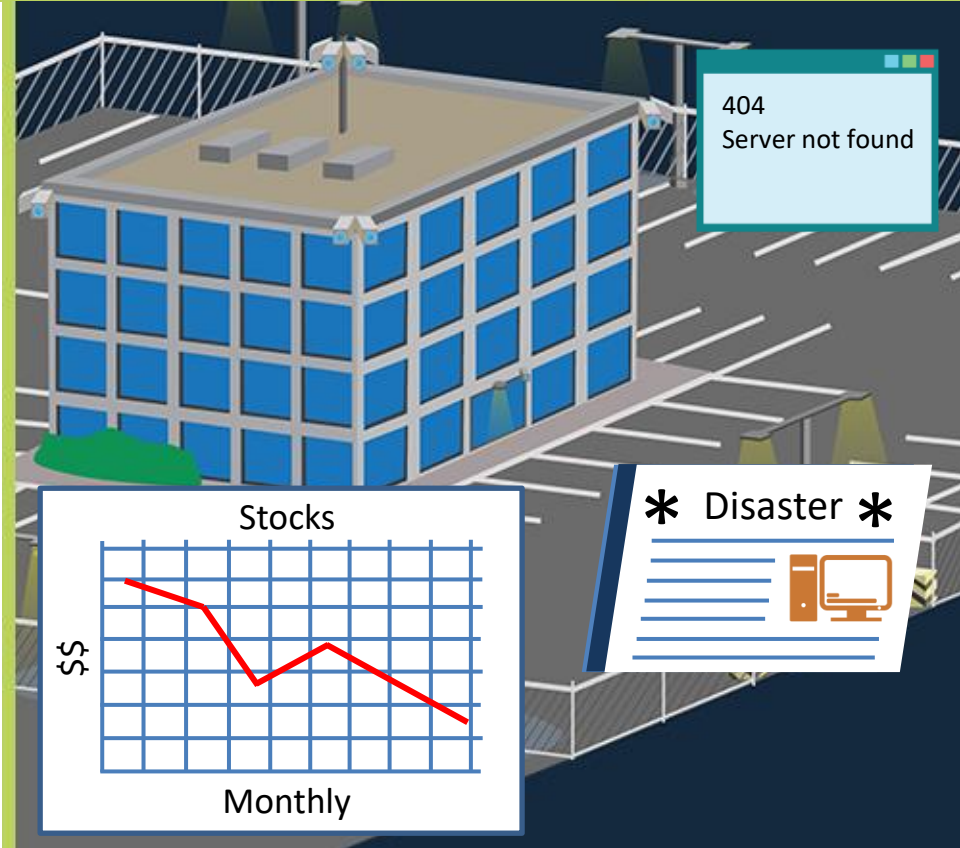
Introduction to Physical Security

- Aims to ensure the safety and CIA of resources in the organization
- Threats
 - Environmental
 - Man-made
 - Supply system
 - Political



Impact of Physical Security Breach

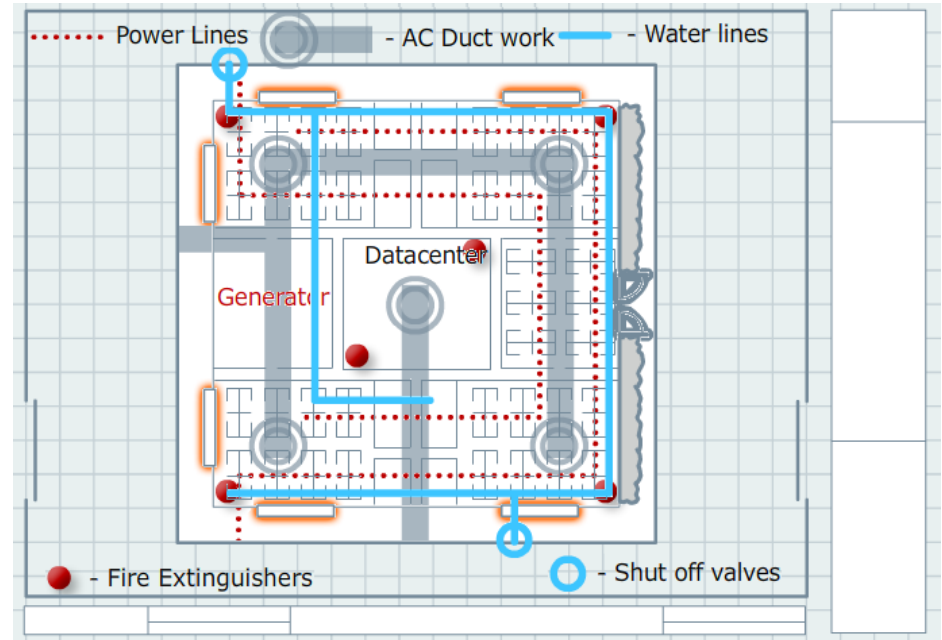
- Primary and secondary loss
 - Destruction of assets
 - Interruption to operations
 - Personnel re-allocated
 - Compromise to CIA
 - Public image is damaged
 - Loss of customers
 - Loss of revenue
 - Loss of life



Approach: outward-in or inward-out?

- **Defense-in-depth**

- Property perimeter
- Drive-ways and parking
- Protective barriers (fences, gates, and bollards)
- Facility entry/exit points
- Support systems (junction and demark boxes)
- Power and water lines
- Special areas
 - Dumpsters
 - Shredder collection



Lighting

- Use the proper method:
 - Mercury vapor
 - Sodium vapor
 - Quartz
 - LED
- Continuous lighting
- Trip lighting
- Standby lighting
- Emergency lighting
 - Generators (gas/propane/solar/
lithium battery)



Cameras

- Provide a way to monitor the premise for intruders
- Provide a way to deter intruders
- Provide a way to record intruders in action



Signage

- Deter individuals from doing something
 - Do Not Enter
 - No Trespassing
 - Beware of Dog
 - Caution Electric Fence
 - Authorized Personnel Only



Protective Barriers

- Protective barriers deter or prevent individuals from actions or control their movement
 - Fences and tire shredders
 - Landscaping and bollards
 - Gates
 - Class I: Residential gate operation
 - Class II: Commercial, such as parking lot or garage
 - Class III: Industrial/limited access (warehouse, factory, loading dock, etc.)
 - Class IV: Restricted access operation that requires supervisory control (prison, airport, etc.)



Security guard

- Typically 24x7, but varies per organization
 - Deters an individual from doing something they should not
 - Provides rapid security response if an intrusion occurs
- Considerations:
 - Hire or contract?
 - Certified or licensed?
 - Armed or unarmed?
 - Screening process?
 - Training?
 - Impact on insurance?



Motion Detection

- Photoelectric – break in a light beam
- Passive infrared – detecting infrared light
- Vibration – change in the level of vibration
- Acoustical – change in sound waves
- Microwave – change in radio waves
- Electro-mechanical – break in electrical circuit
- Electrostatic – change in an electrostatic field



Alarms

- Notification that something abnormal has occurred
 - Static light turns on a display panel
 - light flashes on a display panel
 - bell rings
 - Text/SMS message is sent
 - Horns blare
 - telephone rings



Secure Enclosures

- Safes are used to protect valuable items
 - Currency, deeds, precious metals, diamonds, securities, policies, failsafe passwords
- Should be attached to the physical infrastructure so it can't be moved, and the location needs to be carefully considered
- Considerations – fire and burglar-proof
 - Type of lock
 - Material of safe
 - Weight
 - Tensile strength
 - Relocking device
 - Alarm



Secure Enclosures

- Secure cabinets
 - Secured container designed to withstand burglary attempt
 - Usually fire resistant but not fire-proof
 - Used to store confidential and sensitive information on premises



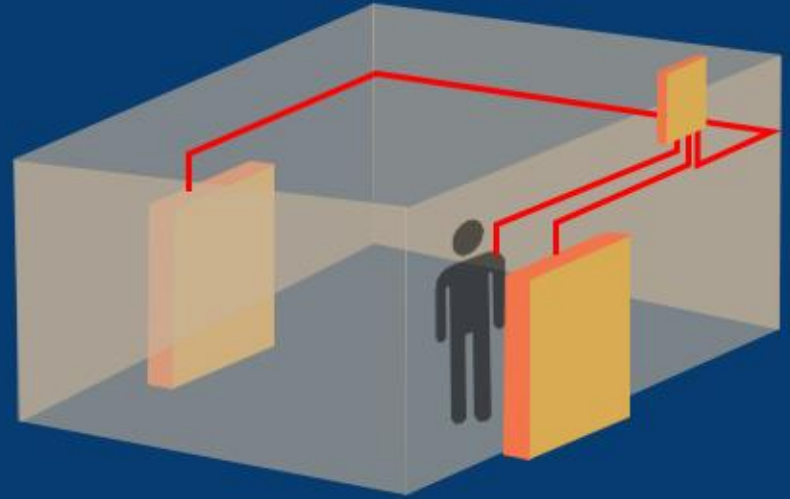
Protected distribution/Protected cabling

- Remember all cable runs and distribution frame (MDF rooms) rooms and closets
 - Under the floor
 - Above ceiling panels
 - Lock all doors to server rooms
- Cameras can be used along with other types of sensors



Controlling Access

- Mantraps and cages
 - Controls access to a facility or a section of a facility
 - One door open at a time
 - Authentication
 - One person at a time
 - Prevents piggybacking
- Faraday Cages are enclosures that block electromagnetic fields
 - EMI and EMP
 - Can be cages, bags, or other enclosures



Locks

- Most common physical security mechanism
- They technically only delay entry - not prevent it
- Locks are susceptible to:
 - Picking (tension wrench and pick)
 - Raking (wider pick)
 - Brute force (hammer, tire iron, firearm)



Types of Locks

- Key Lock - A lock that requires a key to open
- Warded Lock - Wards are obstructions to the keyhole that prevent all but the properly cut key from entering
- Wafer/Tumbler Lock - Wafers under spring tension are located in the core or plug of the lock and protrude outside the diameter of the plug into a shell formed by the body of the lock
- Deadbolt Lock - A bolt inserted into the frame of the door for added security
- Pin Tumbler Lock - the key moves pins so that a shear line can be obtained, thus allowing the key to turn the plug and operate the lock; more secure than warded and wafer/tumbler locks

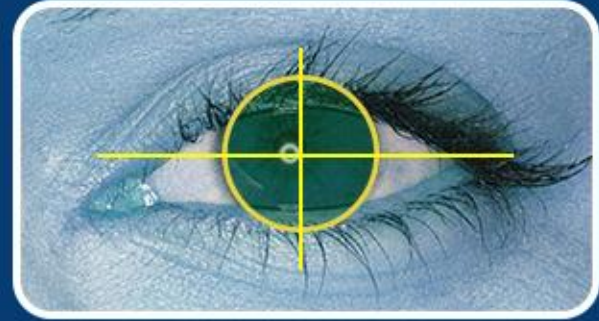


Types of Locks

- Interchangeable Core - A lock with a core that can be removed and replaced using a special-change key
- Combination Lock - A sequence of numbers in proper order are required to open the lock
- Electronic Combination Lock - Uses digital readouts and obtains its power from the energy created when the dials are turned; offers higher security than combination locks, but is much more expensive
- Keyless Lock - A push button lock that has buttons that are pushed in sequence to open the door; sometimes called a cipher lock
- Smart Lock - An inexpensive plastic card that is pre-authenticated to open a door; smart locks are used in most hotels

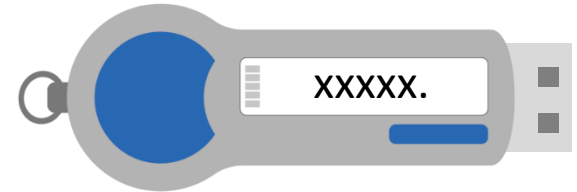
Biometrics

- Used as an access control authentication method
 - Highly accurate but very controversial
- Physiological characteristics of an individual (something you are)
 - Keyboard dynamics
 - Signature dynamics
 - Voice recognition
 - Fingerprint/veins in palm/palm print
 - Retina scan/iris recognition
 - Facial recognition
 - DNA



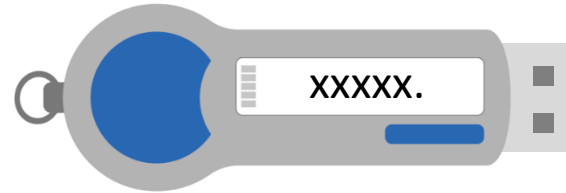
Physical Authentication Tokens

- Tokens are used to authenticate someone's identity
- May be used in an MFA implementation as “something you have”
 - Card with a chip, a USB stick, a key fob that may displays an authentication code - the output is typically only used once (OTP)
- Static tokens - same information used each time
- Synchronous tokens - information changes each time
 - Clock-based and counter-based
- Asynchronous tokens - Information changes each time
 - Not clock based
- PKI tokens



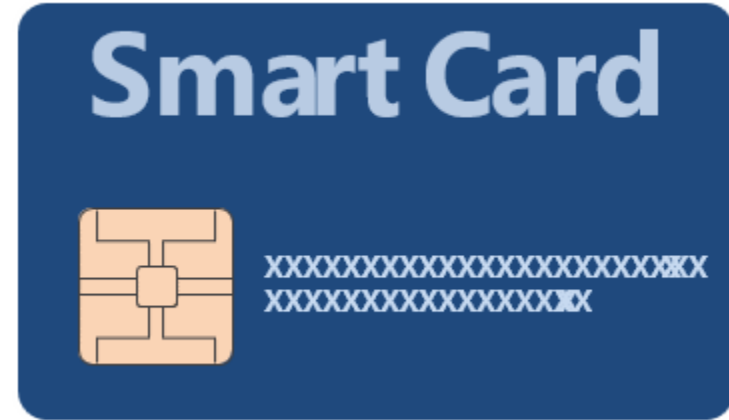
Physical Authentication Tokens

- Disconnected token
 - Built-in screen that displays authentication data
- Connected token
 - Must be connected/inserted into computer
 - Automatically transmit authentication data once connected
- Contactless token
 - Needs to be near the computer
 - Bluetooth/NFC
- Mobile device tokens
 - Software installed on phone that allows your phone to be the token



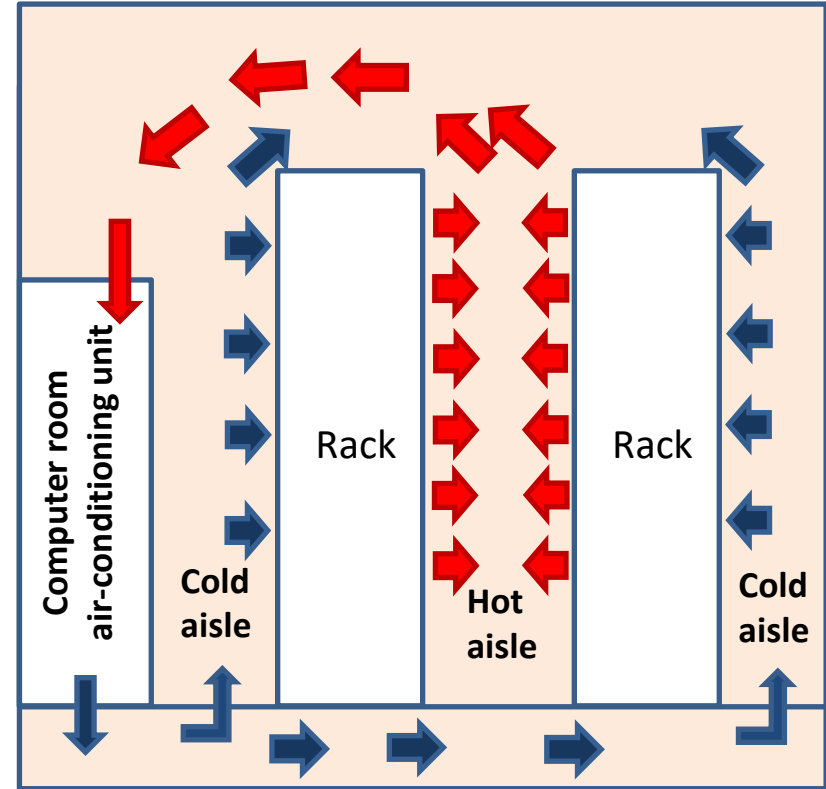
Physical Authentication Cards

- Used to authenticate an individual (something you have)
 - Contains authentication information credentials in an encrypted form
- Smart cards
 - Contact or contactless
 - Contains a microprocessor chip
- Memory cards
 - Like a smartcard but no microprocessor
- Key cards
 - Contact based
 - Contains magnetic strip that holds information



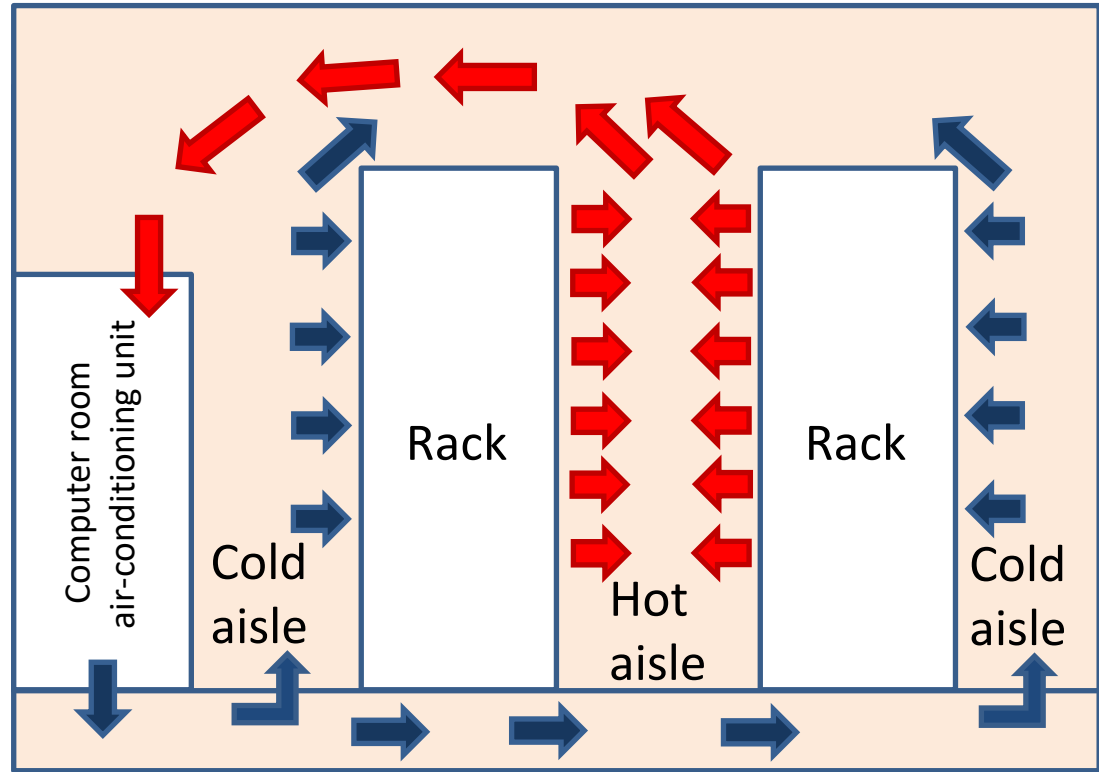
Environmental Controls

- Heating/ventilation/air-conditioning
 - Poor HVAC leads to extreme heat, cold, humidity, or dryness
 - Recommended temp: 72 to 76 degrees
 - Recommended humidity: 40 – 60%
 - Maintain hot and cold aisles
- Security concerns
 - Constant monitoring and alarms
 - Location in facility
 - Maintenance/pressurization
 - Chemical and biological accidents or attacks (DRP)



Environmental Controls

- Hot and cold aisles
 - Data center/network room/server room



Environmental Controls

- Fire controls
 - Prevention
 - Fire-rated construction materials, training, safety
 - Be prepared
 - Detection
 - Smoke and fire detectors, sensors
 - Control quickly, minimize damage
 - Suppression
 - Contain and extinguish the fire



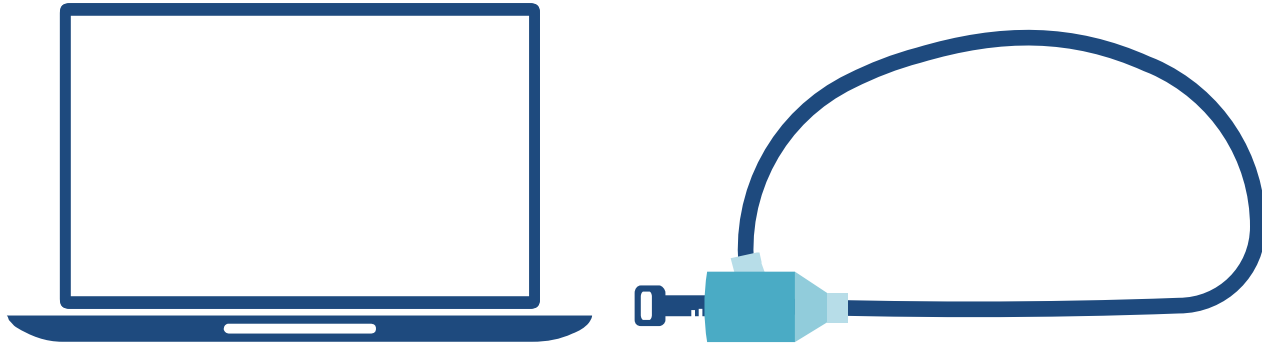
Types of Fire Extinguishers

- Type A - common combustibles, such as wood products, paper, and laminates
 - suppressed with water or soda acid
- Type B - combustible liquids, such as petroleum products and coolants
 - suppressed using halon or halon substitutes, carbon dioxide, dry powders, or soda acids
- Type C - electrical equipment and wires
 - extinguished using gas, dry powders, or carbon dioxide
- Type D combustible metals
 - can be suppressed only with dry powder



Additional Security Considerations

- Cable locks
 - Used to secure devices to a desk, shelf
 - Prevents theft of the device



Additional Security Considerations

- Screen filter
 - Limits the viewing angle of a display
 - You have to be viewing it straight on to see the image
 - Prevents shoulder surfing



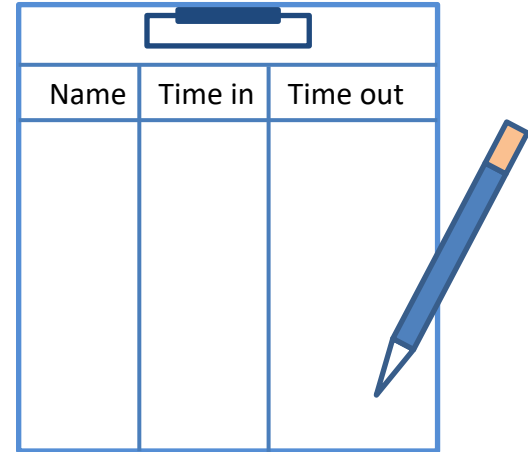
Logging and Key Management

- Document all activities in redundant logs!
- Keep track of physical and digital keys/cards
 - Who has what key, who has what access, who created the key, why
- What do you do when a key is lost?
 - Physical key
 - Change door locks, issue new keys
 - Digital key/card
 - Revoke key and issue a new key/card



Logging and Key Management

- Sign-in/sign-out log
 - Ensures you have a record of who enters and leaves the premises
 - Guests
 - Contractors
 - Maintenance
 - Interviewees
 - Employees



The illustration shows a sign-in/sign-out log sheet. It is a rectangular table with a blue border. At the top center, there is a blue clipboard icon. The table has three columns: 'Name', 'Time in', and 'Time out'. The 'Name' column is the widest, followed by 'Time in', and then 'Time out'. The table is currently empty, with only the header row filled. To the right of the table, there is a blue pen with an orange eraser and a blue body, pointing towards the bottom right corner of the table.

Name	Time in	Time out