Welcome Back to the CISSP Bootcamp

Your instructors:

Michael J Shannon

and

Carl Mullin

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

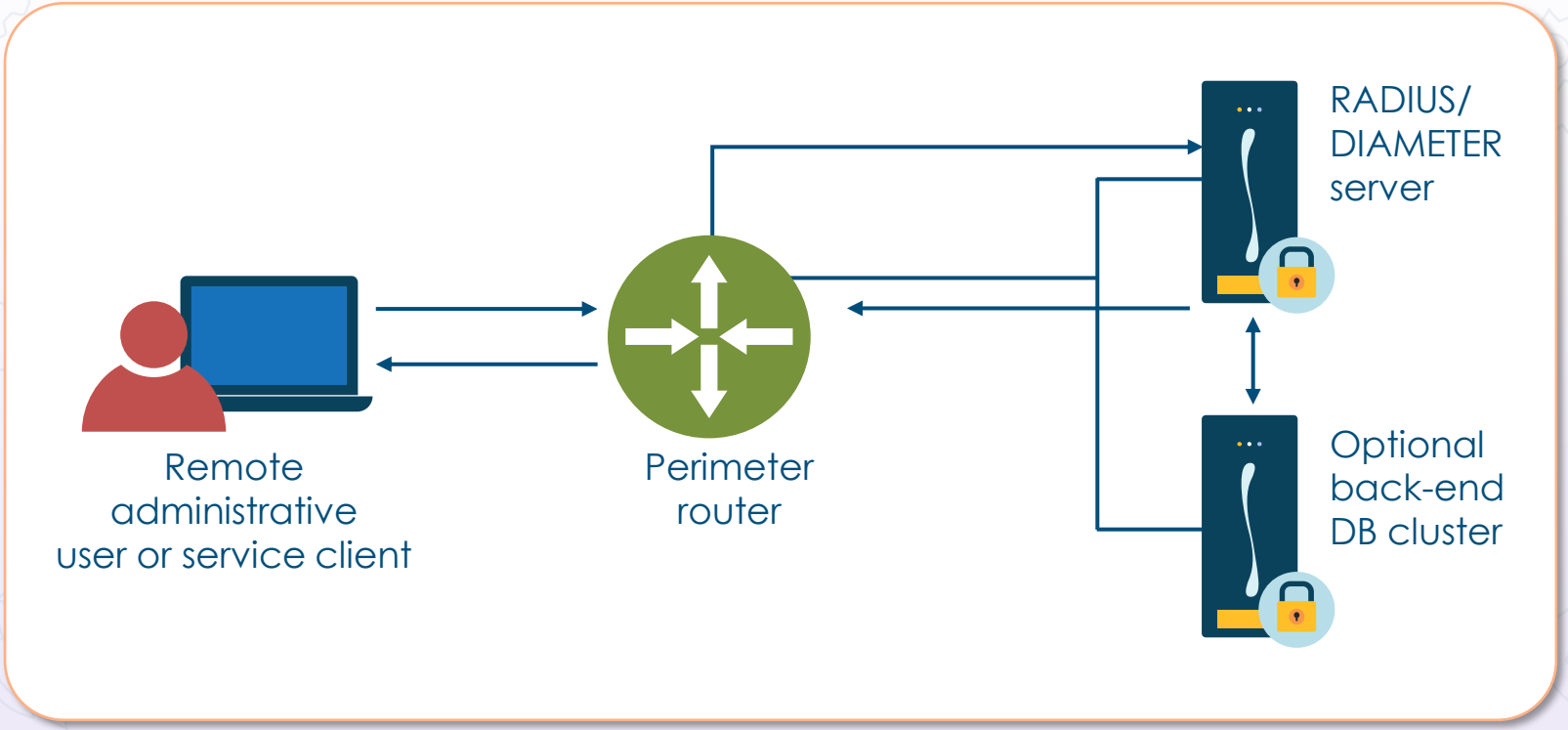
Remote Authentication Dial-In User Service (RADIUS)

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

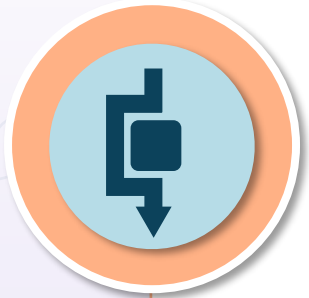
RADIUS

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

RADIUS/DIAMETER

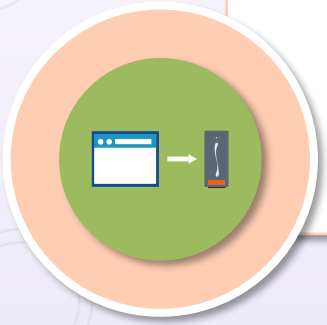


TACACS+



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

TACACS+



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

Security Assertion Markup Language (SAML)

SAML 2.0

- SAML is an XML-based open-source SSO standard
- SAML is used by many cloud SSO connections for thousands of large enterprises, government agencies, and service providers that communicate on the Internet
- A key advantage of SAML is open-source interoperability
- Some large companies now require SAML for Internet SSO with SaaS applications and other external ISPs

Security Assertion Markup Language (SAML)

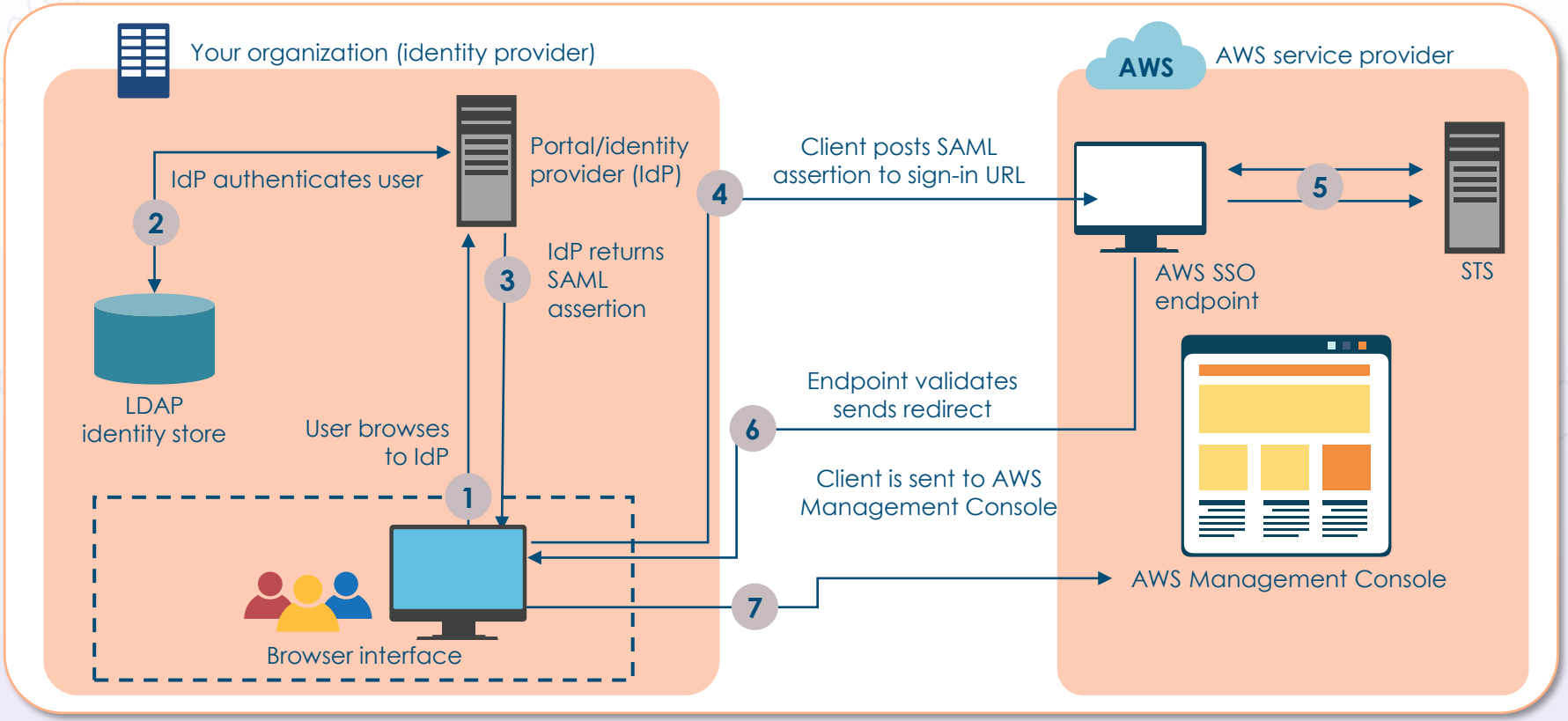
Identity provider

- The SAML identity provider declares the identity of the user along with additional metadata in an assertion
- Directory services like LDAP and Active Directory are common identity providers

Service provider

- The service provider takes the assertion and passes the identity data to an application or service
- Common service providers are cloud services and social media sites

SAML 2.0 at AWS



SSO Vulnerabilities

- ***Single point of failure*** – when a single credential is used without leveraging other factors
- ***Collusion attacks*** – secret cooperation between two or more system entities to launch an attack. For example, collusion between the principal and service provider or collusion between the principal and identity provider
- ***Denial-of-service attacks*** – preventing authorized access to a system resource or delaying system operations
- ***Man-in-the-middle attacks*** – active wiretapping where the attacker intercepts and selectively changes data in transit to spoof one or more entities
- ***Replay attacks*** – when a valid data transmission is maliciously or fraudulently repeated, possibly as part of a masquerade attack
- ***Session hijacking*** – active wiretapping in which the attacker seizes control of a previously established communication association

OAuth

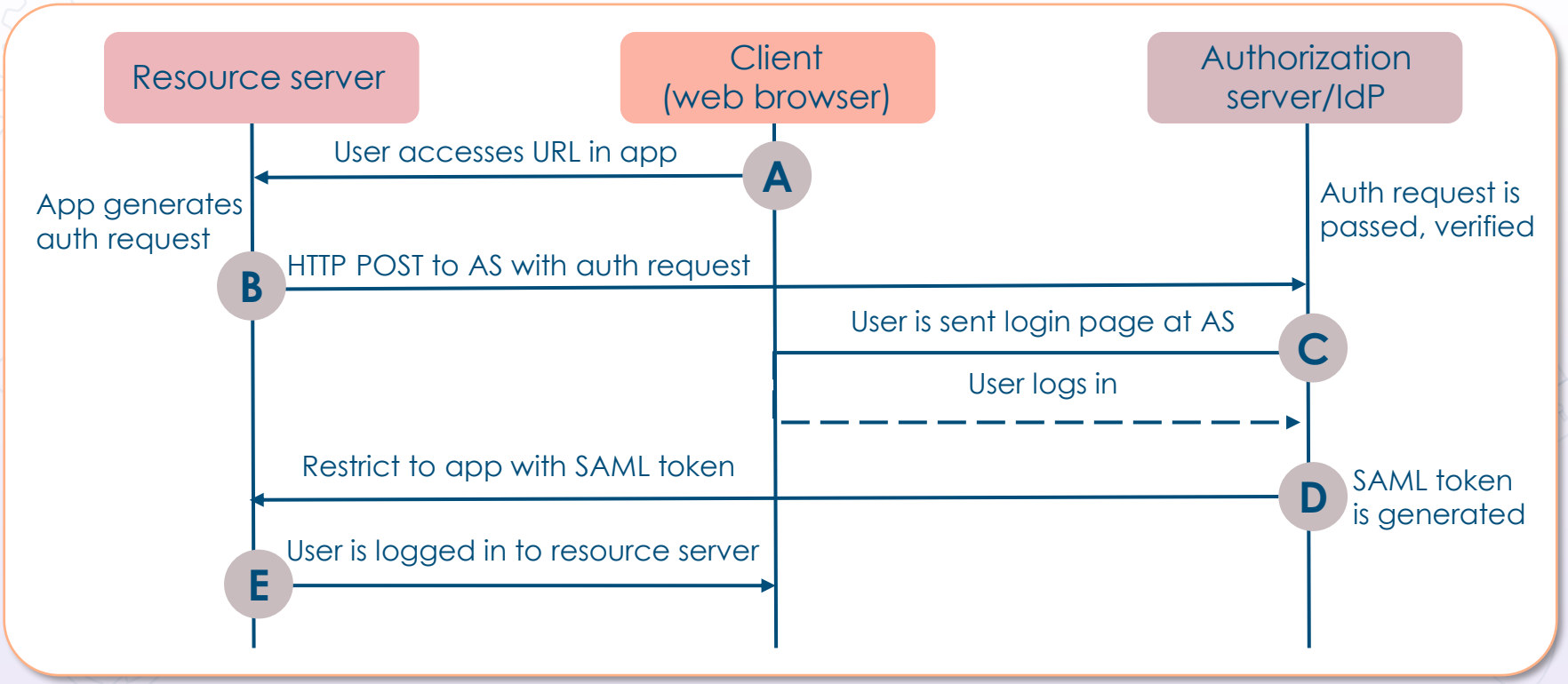
- OAuth 2.0 is an open authorization framework that allows a third-party application to get limited access to an HTTP service
- Developers use OAuth to publish and interact with protected data in a safe and secure manner
- Service provider developers can use OAuth to store protected data and give users secure delegated access
- OAuth is designed to work with HTTP and basically allows access tokens to be issued to third-party clients by an authorization server with the approval of the resource owner
- The third party then uses the access token to access the protected resources offered by the resource server

OpenID Connect (OIDC)

OIDC

- OIDC 1.0 is a basic identity layer on top of the OAuth 2.0 protocol
- It verifies the end-user identity using an authorization server (AS)
- It can get basic profile information about the user with an interoperable REST-like methodology
- Supports web-based, mobile, and JavaScript clients
- OpenID is extensible as functionality can be added

OAuth/OIDC Process



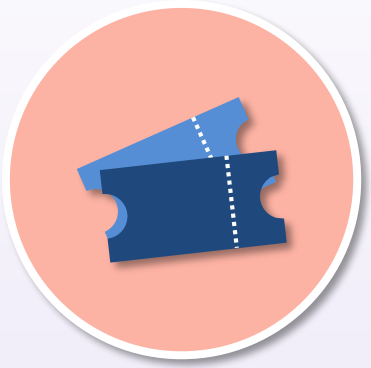
Shibboleth

Connects users to both interorganizational and intraorganizational applications and services

Empowers sites to make well-informed authorization choices for discrete access to protected online resources while maintaining user privacy

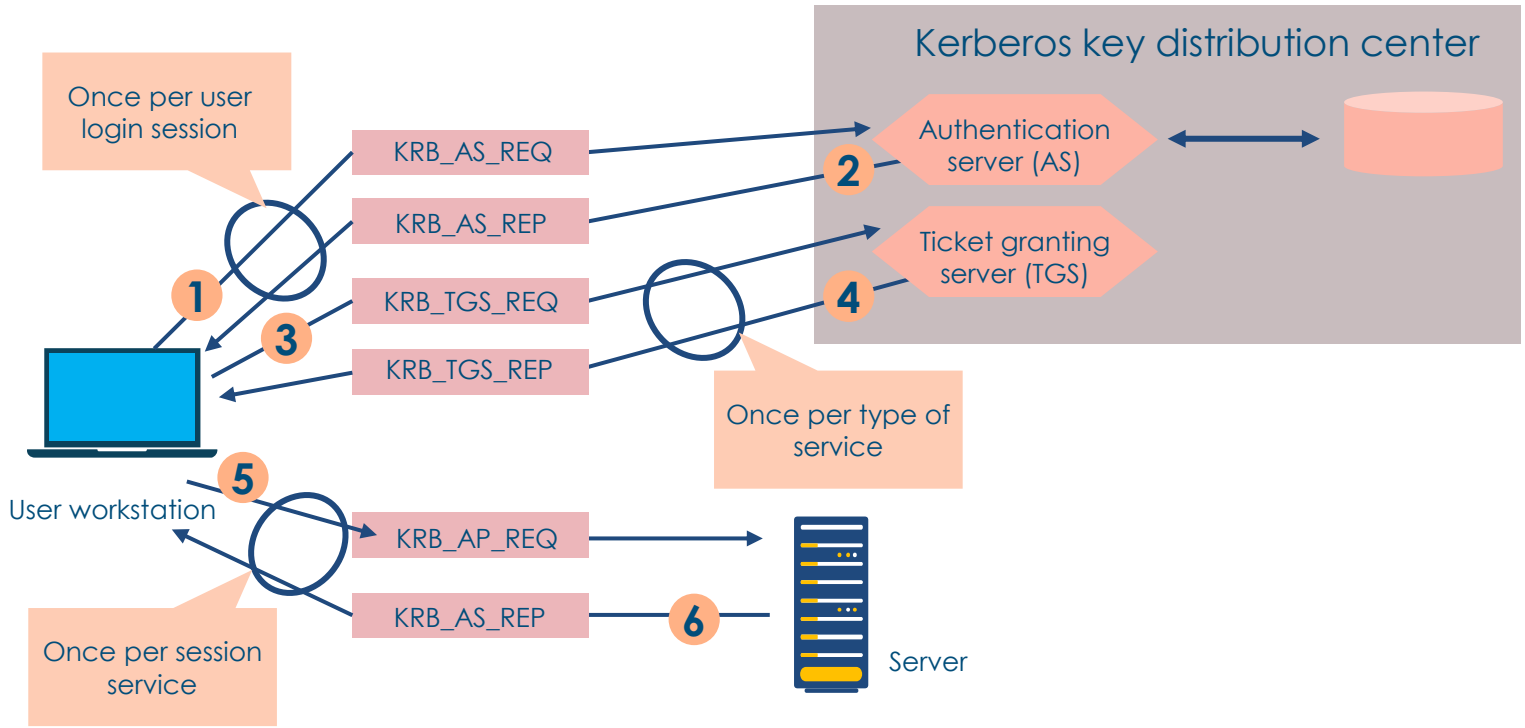
Is free, open source, and popular with universities and public service organizations

Kerberos



- SSO authentication using a secret key cryptosystem
- Uses a ticket for the assertion or token
- Performs mutual authentication
- All communications can be encrypted
- Depends on a trusted third party called a key distribution center (KDC)

Kerberos


Kerberos key distribution center
Authentication server (AS)
Ticket granting server (TGS)
Once per user login session
KRB_AS_REQ
KRB_AS_REP
KRB_TGS_REQ
KRB_TGS_REP
1
2
3
4
Once per type of service
User workstation
5
KRB_AP_REQ
KRB_AS_REP
6
Server
Once per session service

Provisioning and Deprovisioning

- From the standpoint of IAM, provisioning involves the administration of user accounts and the assignment of access privileges, often by group membership
- Onboarding of devices and certificates is often handled using enterprise mobility management (EMM)
- When executed properly, a provisioning solution should deliver standardized and automated service desk IT processes for on-boarding, transfers, periodic access audits, and off-boarding of
  - enterprise employees and contractors
  - third party business partners,
  - and customers

Key Enterprise Challenges

Ever-increasing costs of user account management and help desk/service desk implementations

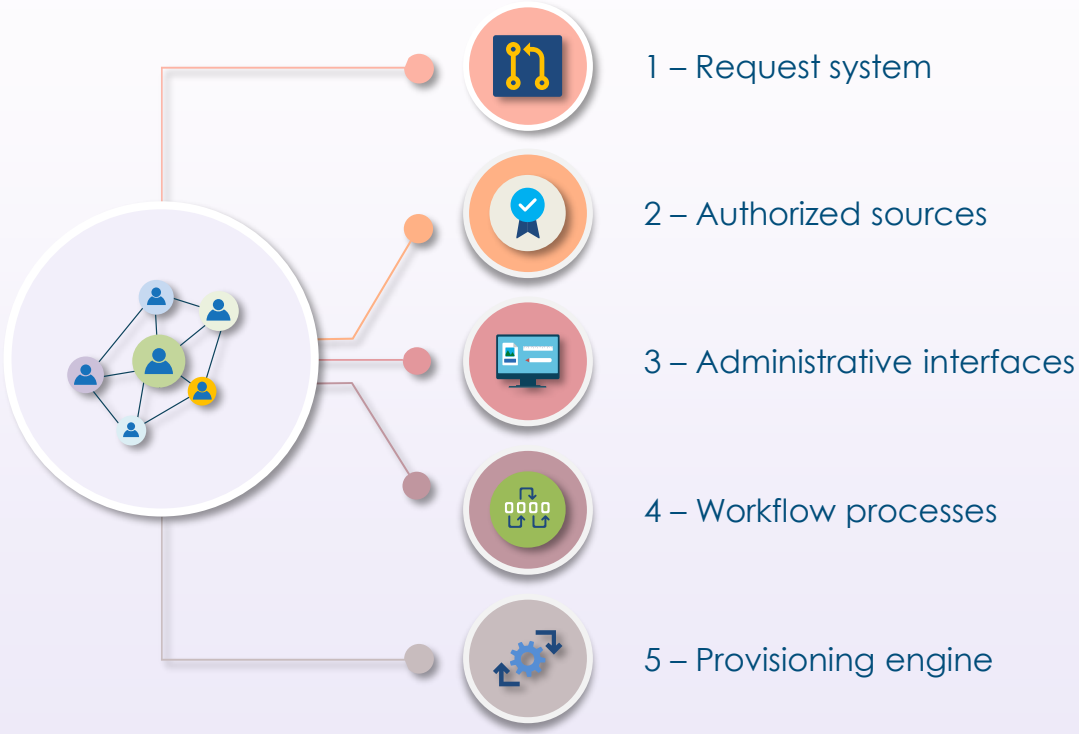
Low priority for proper account creation, approval processes, and auditing

High cost of constant compliance audits of user account administration practices

Complicated provisioning processes that are unique to different business applications, systems, and platforms

Lack of timely account suspension and deletion policies and processes for terminated groups and users

Provisioning System Components



1 – Request system

2 – Authorized sources

3 – Administrative interfaces

4 – Workflow processes

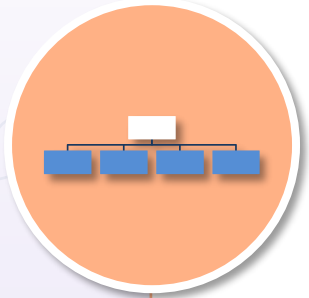
5 – Provisioning engine

Provisioning System Components

Role Definition

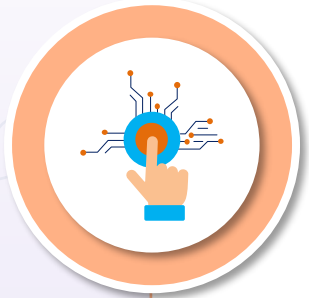
- If using a DAC model, the roles will usually be based on global group membership
  - Includes data and asset ownership, custodianship, stewardship, and processor/user
- If using ABAC, the authorization role profile can change based on various attributes and variables
  - What, when, where, and how
- CSPs like AWS and GCP use policies and roles applied to logical groups

Functional Organization



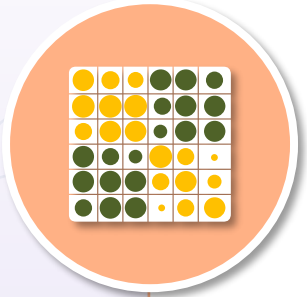
- Structured around the functions the enterprise need to be performed to deliver the value proposition(s)
- Functions may include human resources (HR), information technology (IT), sales, marketing, finance, facilities, and call centers
- This is the traditional top-down structure of organizations where resources are controlled by functional managers
- The "project/program management" role will be implemented by a team leader of a functional area under the supervision of a functional manager
  - Acts more like a "project coordinator" or "project expediter" and does not typically have the title of "project manager"
- The authority of the coordinators and expediters is very limited

Projectized Organization



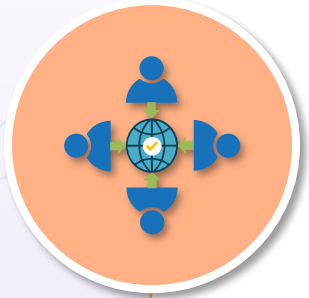
- Structured around projects and initiatives for the highest project management and service management effectiveness (flatter organization)
- The project and program managers assume more authority and control (ownership) of resources
- The initiative managers have a full-time role and will answer to a sponsor on the C-Suite or senior executive management or officers
- Team members are typically co-located within the same office, or virtually co-located, to take full advantage of communication efficiency
- There may be still be some functional units within the organization (HR), however, those units provide a supportive function only without authority over any project or program managers, supervisors, and team leaders

Matrix Organization



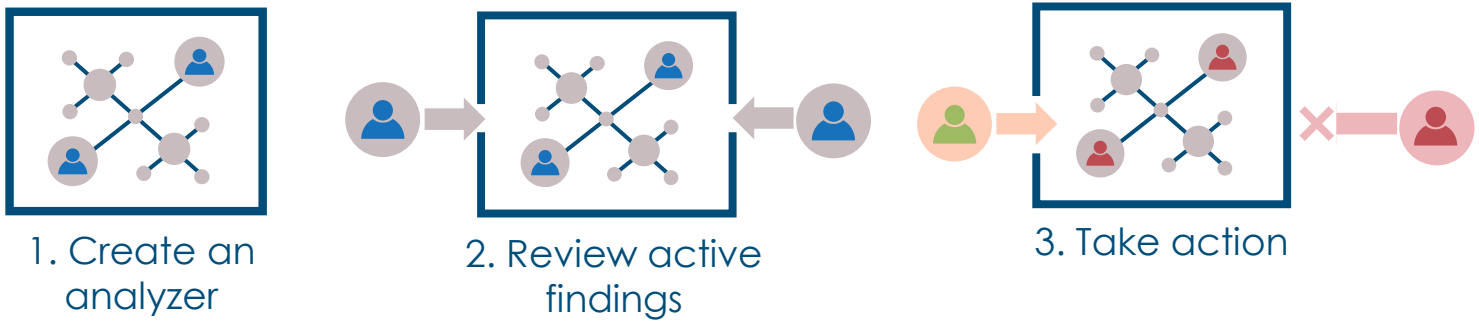
- Structures that perform as a combination of the attributes of functional and projectized organizations
- Matrix organizations can be further classified as weak, balanced, or strong depending on the relative power of the functional managers and the project managers
  - If the project/program managers are given a role of coordinator or expediter, then the enterprise is considered a "weak matrix"
  - If the project/program managers are granted much more authority on resources and budgets, the organization is considered a "strong matrix"
- The differences between a functional organization vs. a weak matrix and a projectized organization vs. a strong matrix are not very clear cut, which can make access control more challenging for security

Account Access Review



- Traditional techniques use permissions spreadsheets or documented matrices
- Should be an aspect of change and configuration management IT practices
- Automation and orchestration tools should be employed when possible
- Example: The AWS IAM service provides an Access Analyzer tool to help administrators recognize possible security risks in the environment by analyzing the resource-based JSON policies using proprietary machine learning engines

AWS IAM Access Analyzer



Managing Account Lifecycles

Account access audits

- Security officers are often responsible for auditing the account and credential lifecycle:
  - administer the process of granting new user access to systems
  - modify roles when a user changes jobs
  - review when a user's job requires new access
  - review access on a regular basis and modify discrepancies
  - remove the access of terminated users
  - implement user account and password policies
  - manage SSO and password managers

Privilege Escalation

Privilege escalation (or elevation) occurs when a subject gets unauthorized access to resources and data

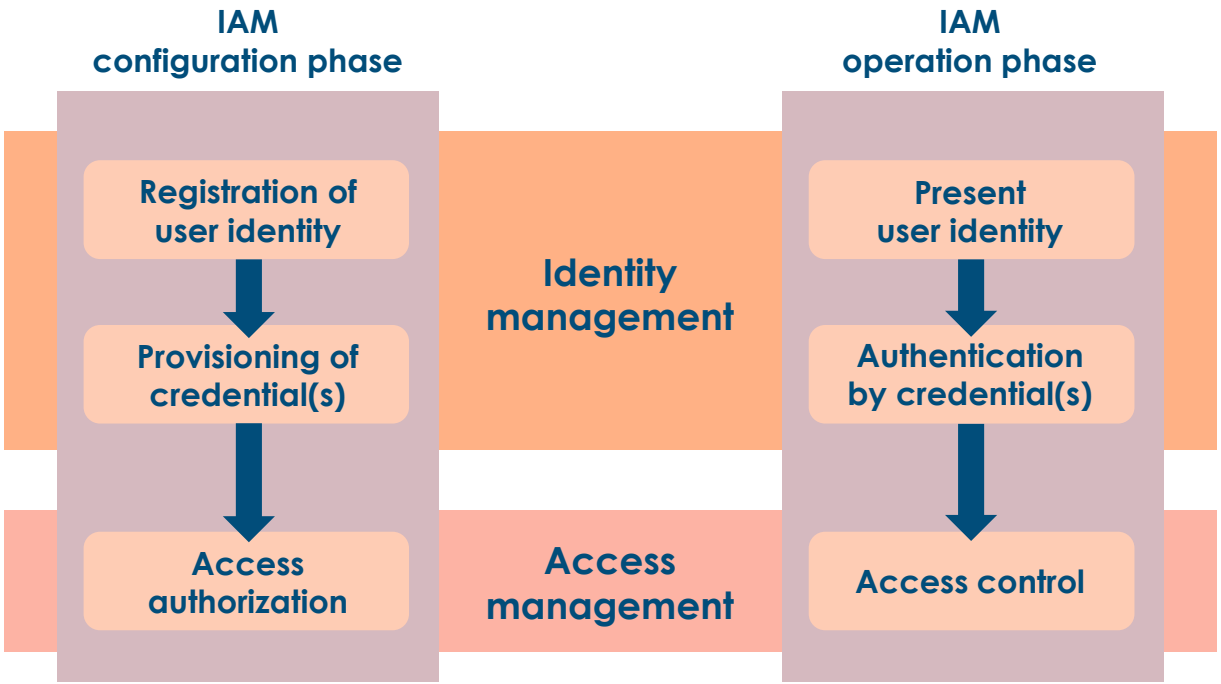
Can also occur when the least privilege principle is not enforced

The MAC model is optimal to prevent escalation

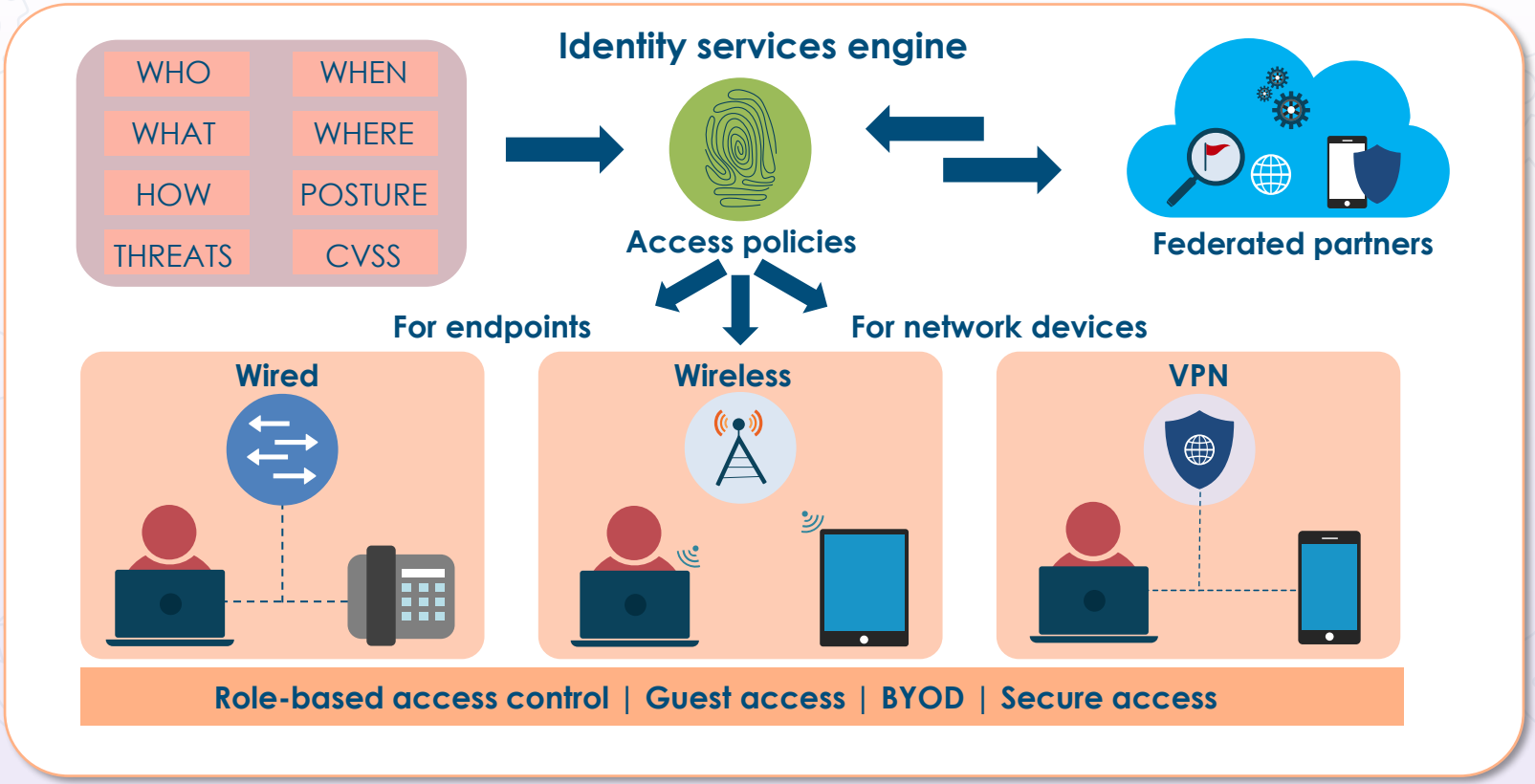
This is also a phase of the cyber attack kill chain

Must fix flaws in system or application through assessments

Implementing Identity Management (IdM)



Using Identity Services Engines



Identity Management Use Cases

Enable guest network access at ease

Guest and secure Wi-Fi

Intent based network access across wired, wireless, and VPN

Secure access

See what's on your network and where they are located

Asset visibility

Enforcing access based on asset visibility

Asset enforcement

Deeper visibility and control on desktop and mobile device apps

Compliance

Identity Management

Onboarding and management of wired and wireless BYOD

BYOD

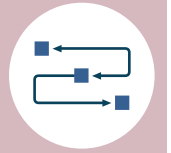
Share real-time threat intelligence to automate threat response

Threat containment

Software defined segmentation without VLANs or IP-based policies

Segmentation

Exchange context between technology partners for better fidelity

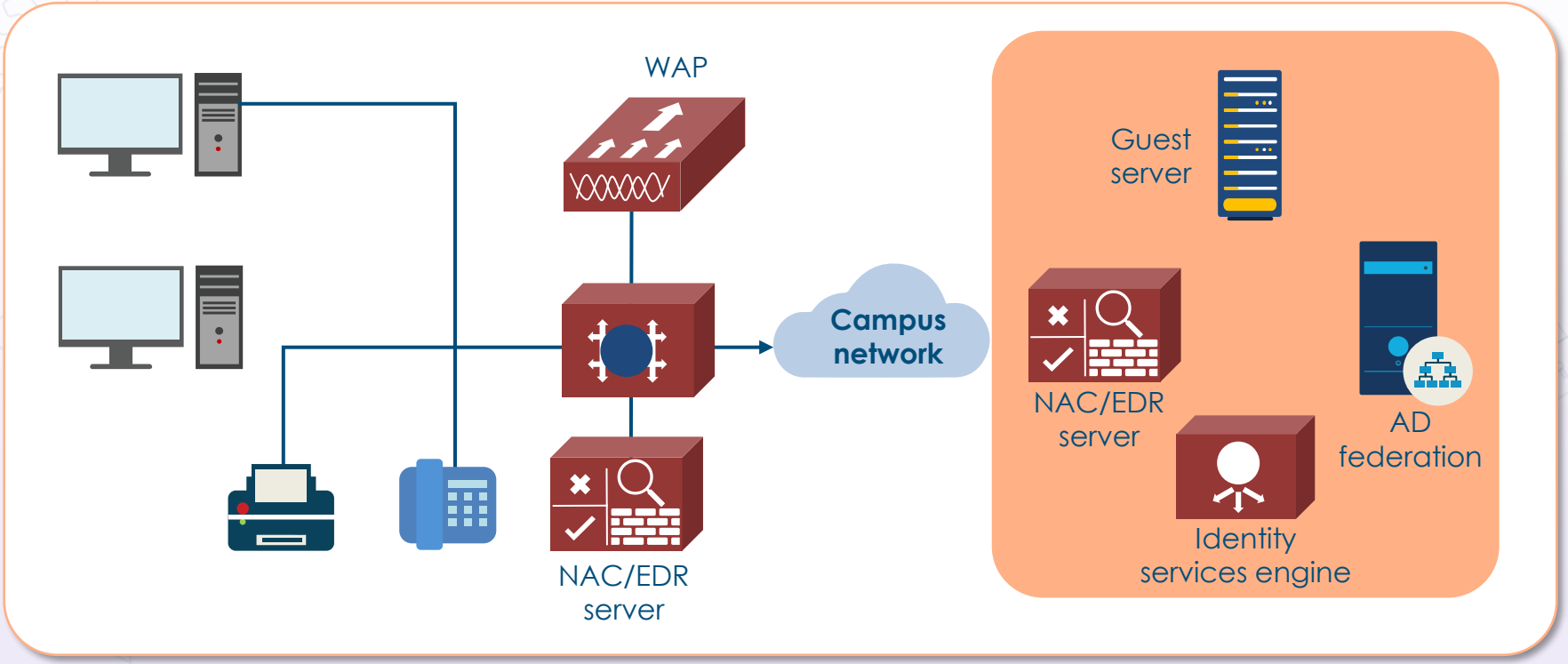


Integrations

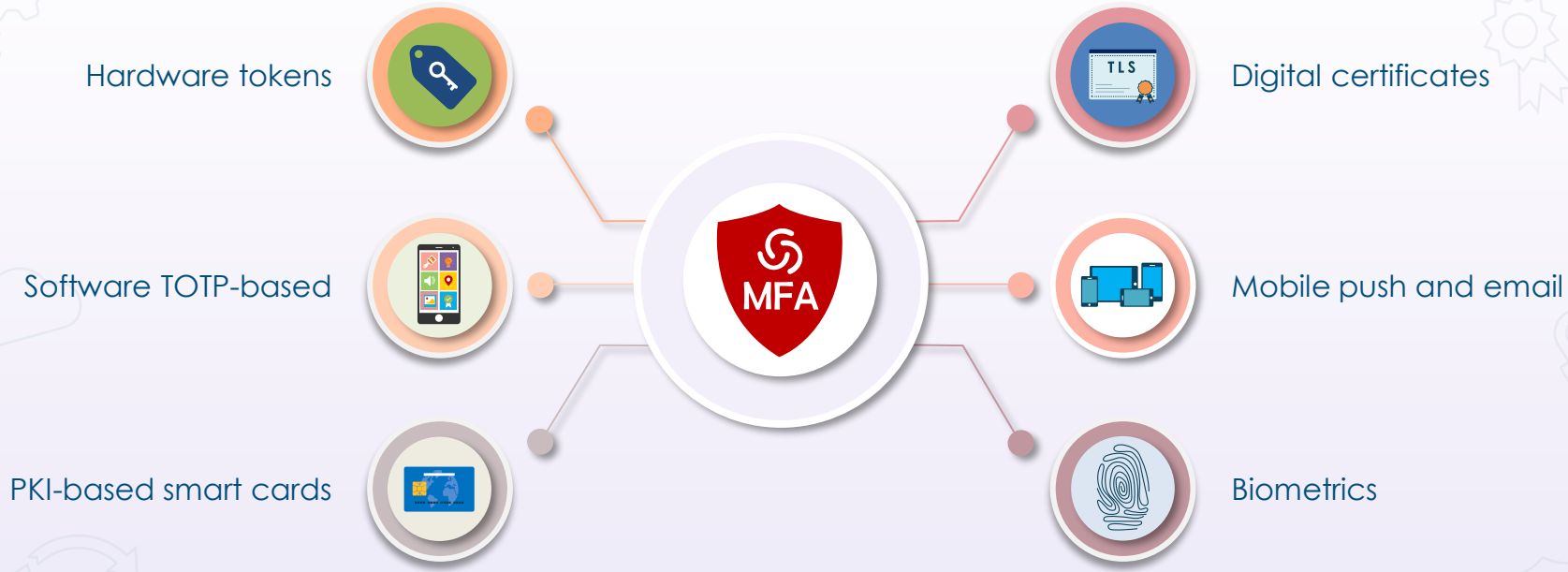
Role-based network device administration over TACACS+

Device admin

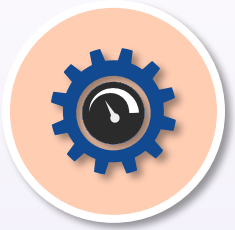
NAC and 802.1X Solutions



Multifactor Authentication (MFA) Mechanisms



Accounting



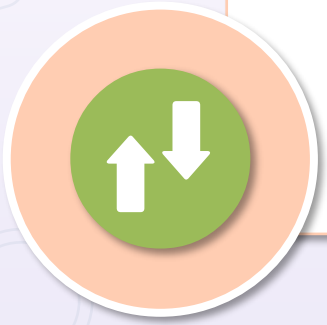
Billing and chargeback

- Accounting is often performed to determine when the subject started, when they finished, and for how long
- The data is used for chargeback or "showback" against departmental budgets and business unit allocations

Auditing and visibility

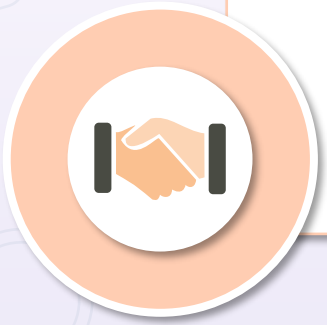
- The primary use case is to get visibility in order to collect meaningful metrics for optimization, utilization, and continual improvement
- It is critical to hold highly privileged access users accountable to policies and acceptable practices
- SIEM systems, NetFlow collectors, RADIUS/DIAMETER

Session Management



- Session management typically refers to the technique of securely handling one or several requests to a web-based application or service from a subject
- The session begins when a user authenticates their identity using a password or another authentication credential such as an assertion, token, or ticket
- A software application or network operating system is responsible for managing the session lifetime

Session Management



- With TLS, record and handshake protocols manage the process of protecting symmetric session keys with an asymmetric cryptosystem
- Additional security mechanisms such as elliptic curves, ephemeral keys, secure cookies, OCSP, forward secrecy and HTTP Strict Transport Security (HSTS) can enhance the session security

Identity Registration and Proofing

Registration

- There must be a registration authority that serves as an identity provider (IdP)
- This could be a back-end NoSQL database, directory service like OpenLDAP or Active Directory, RADIUS/DIAMETER, or security solutions that specialize in MFA and biometric solutions
- Only the necessary data about the subject is given to the requester

Proofing

- Identity proofing collects attributes or digital documents (DocuSign) to support a claim of identification for a specific subject to validate the veracity of the claim
- Identity proofing is usually executed during a registration or enrollment process
- Knowledge-based authorization using data from public records is common

Microsoft Forefront Identity Manager

- Microsoft Forefront Identity Manager (FIM) is a self-service identity management software suite for controlling identities, credentials, and role-based access control policies over heterogeneous environments
- FIM can also embed self-help tools in Microsoft Outlook so that end users can manage routine tasks such as resetting their own passwords without service desk assistance
- It also permits users to generate their own security and email distribution lists and determine who to put on the lists
- The newest solution is Microsoft Identity Manager (MIM), which adds a hybrid experience, privileged access management capabilities, and support for new platforms

Client-side vs. Server-side

- The security manager must have visibility into all client-server channels and interactions as part of risk management
- From a development standpoint, you can use server-side or client-side execution and validation – both are acceptable
  - Client-side is more efficient
  - Server-side is more secure
- Advanced SIEM systems and SOAR implementations are valuable in assisting the security operations center in achieving maximum real-time visibility into all enterprise client-server interactions

Client-side Attacks and Controls

Client-side

- Client-side attacks specifically target the software on the desktop itself, such as web browsers, media players, POP3 and IMAP4 email clients, productivity suites, and more
  - Cross-site scripting type 0 is a common client-side attack against web clients using gadgets and other streaming applets
- Countermeasures include the following:
  - Patch management
  - Security suites
  - Next-generation EDR
  - Cloud-based security and CASBs

Server-side Attacks and Controls

Server-side

- Server-side attacks (also called service-side attacks) are launched directly from an attacker (the client) to a listening service
  - The "Conficker" worm of 2008+ spread using several vectors, including a server-side attack on TCP port 445, exploiting a weakness in the RPC service
  - Variants of Conficker still reappear, especially in Europe
- Countermeasures include the following:
  - Patch management
  - Infrastructure security (firewalls, IPS, WAF)
  - Secure virtualization and compartmentalization
  - Infrastructure as a Service (IaaS)

Database Security: Scoping

"Why before how"

- Determine the "why" or the use and purpose of the data before the "how" of its structure and schema
- A scope is the outline of a description about why we are working on a problem and why certain data will solve the problem or achieve a goal
    - Context
    - Needs
    - Vision
    - Outcome
- Scoping often involves removing baseline security controls that do not apply, such as removing privacy controls where private data is nonexistent

Database Security: Tailoring

- Tailoring involves modifying the baseline to become more applicable, such as modifying the data application timeout requirement from 20 minutes of inactivity to 10
- Scoping is more appropriate for controlling global recommendations through the removal of aspects not applicable to any specific environment
- Tailoring, on the other hand, involves modifying details regarding general data that is more precisely appropriate to an application or environment

Database Security: Tokenization

- Tokenization involves sending sensitive data through an API call (or batch file) to a provider that replaces the data with non-sensitive placeholders called tokens
- Unlike encrypted data, the tokenized data is irreversible and unintelligible

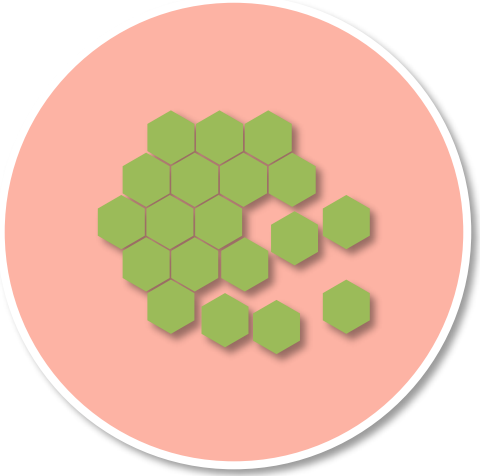
Tokenization vs. Encryption

Encryption	Tokenization
Mathematically transforms plain into ciphertext using an encryption algorithm and key	Randomly generates a token value for plain text and stores the mapping in a database
Scales to large data volumes with just the use of a small encryption key to decrypt data	Difficult to scale securely and maintain performance as database increases in size
Used for structured fields, as well as unstructured data, such as entire files	Used structured data fields, such as payment card or social security numbers
Ideal for exchanging sensitive data with third parties who have the encryption key	Difficult to exchange data, since it requires direct access to token vault mapping token values
Format-preserving encryption schemes come with a tradeoff of lower strength	Format can be maintained without any diminished strength of the security
Original data leaves the organization, but in encrypted form	Original data never leaves the organization, satisfying certain compliance requirements

"Tokenization vs Encryption," accessed May 5, 2021, https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/tokenization-vs-encryption.html.

Database Security: Abstraction

Mediated access



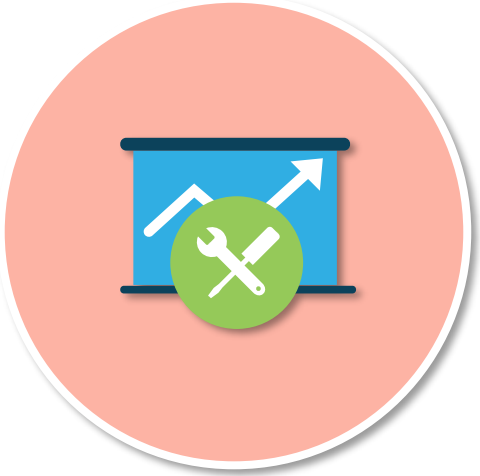
- Abstraction is a method to make logical and physical data models more flexible by redefining and combining some of the data elements, entities, and relationships within the model into more generic terms
- Abstraction also involves removing details in order to make something applicable to a wide class of scenarios, while preserving the important properties and essential aspects from concepts or subjects
- Can practically involve using more views and indirect access to the underlying raw data

Database Security: Hashing

- In a database management system, hashing transforms a string of characters into a typically shorter fixed-length value or key that represents the original string
- Hashing is often used to index and retrieve items in a database because it is faster to find the data item using the shorter hashed key than using the original value
- Salting relates to password hashing
  - A value appended to password to create a different hash
  - The added value is called a "salt" and protects against brute force attacks
  - A "pepper" is secret and must not be stored with the output

Supervisory Control and Data Acquisition

SCADA



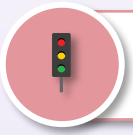
- SCADA represents the software used to collect and send data to other facility systems
- Programmable Logic Controllers (PLC) are a vulnerable hardware component
- Industrial control systems that are not air-gapped introduce various threats

SCADA Examples

Facility and manufacturing control and management systems

Water management, electric, and nuclear power grid

Solar and wind farms



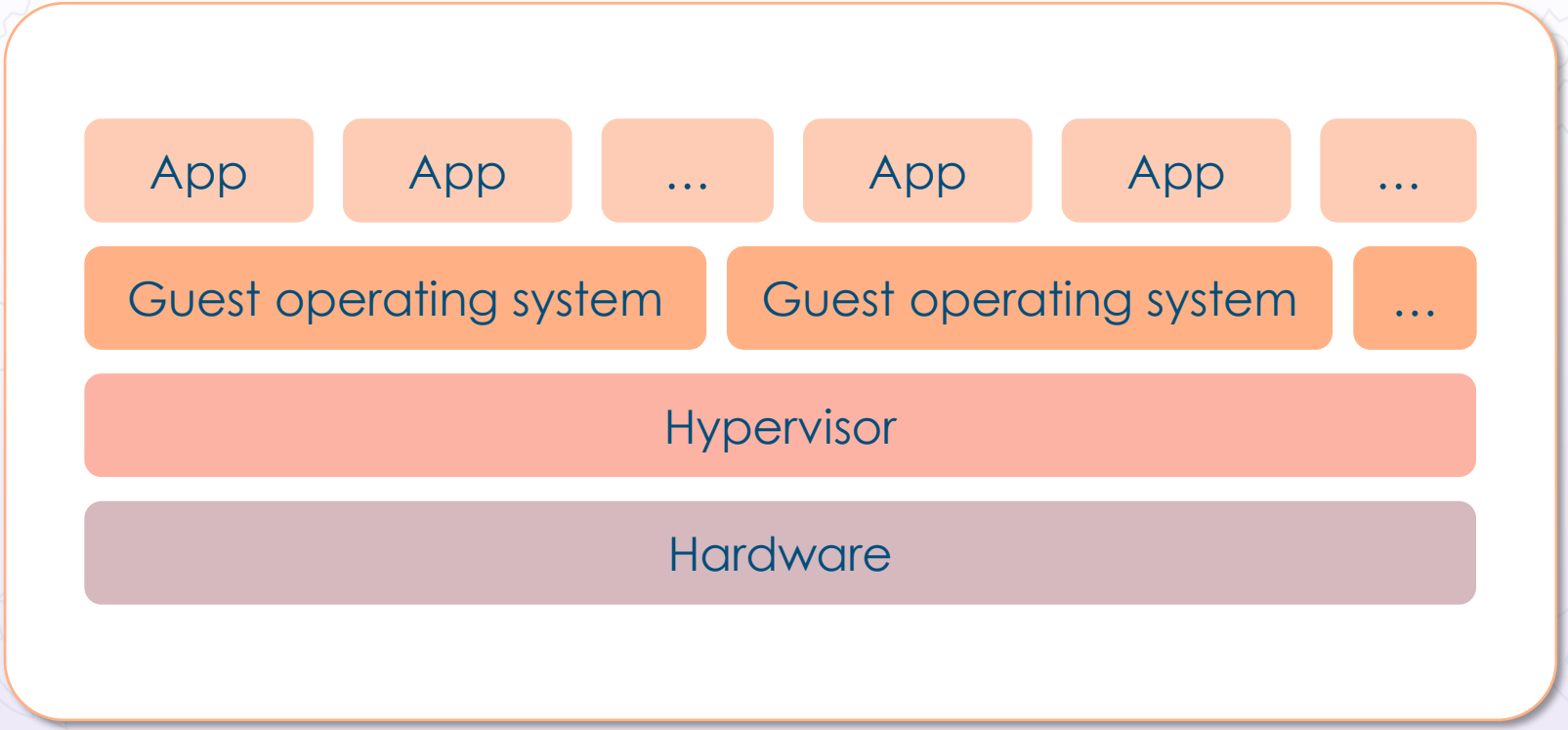
Traffic signals and mass transit systems

Environmental control systems and manufacturing systems

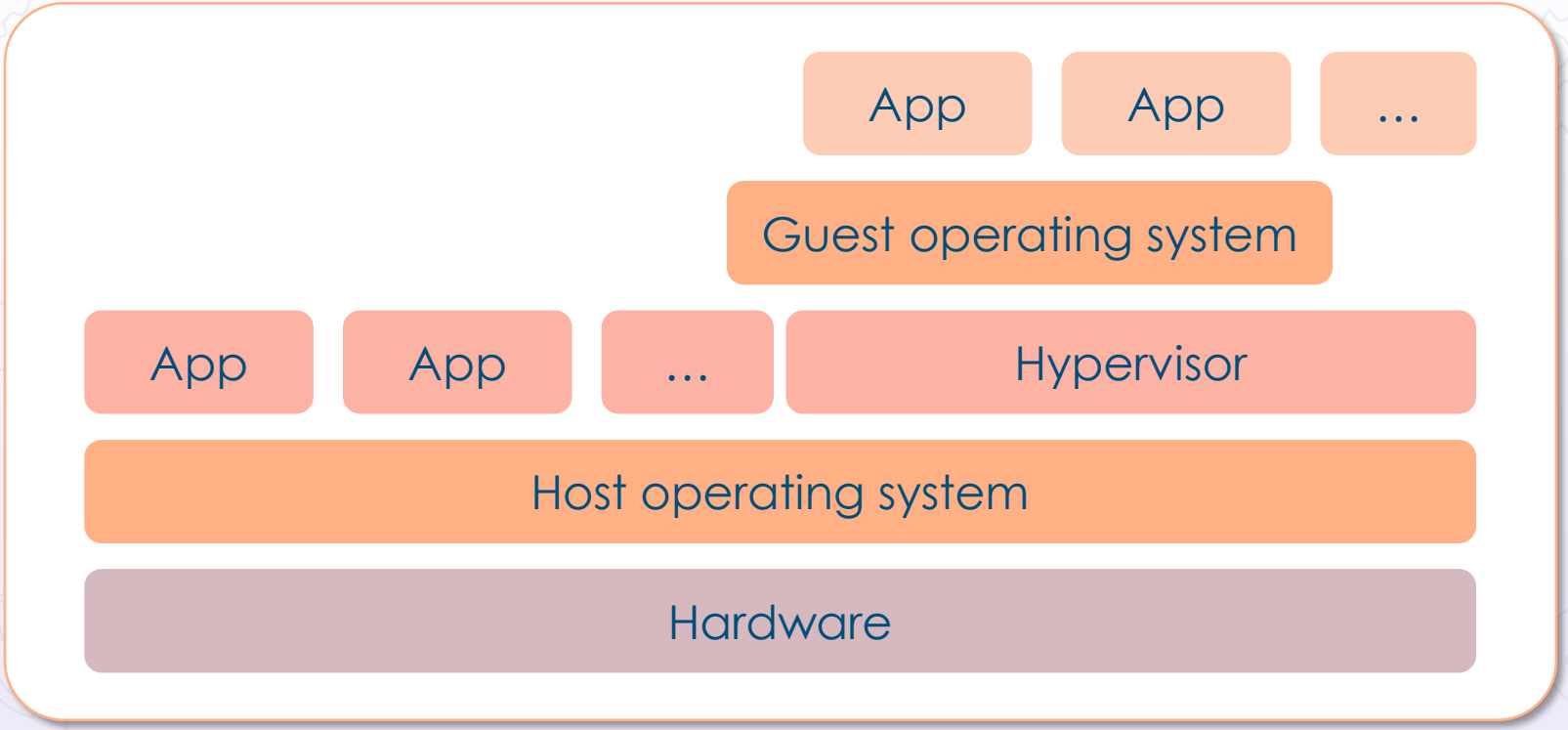
SCADA Security Concerns

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

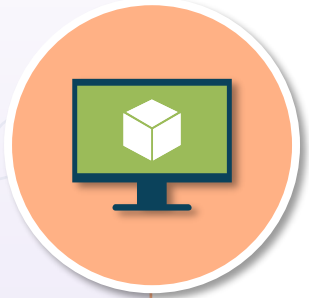
Type 1 Hypervisors



Type 2 Hypervisors



Virtualization Issues

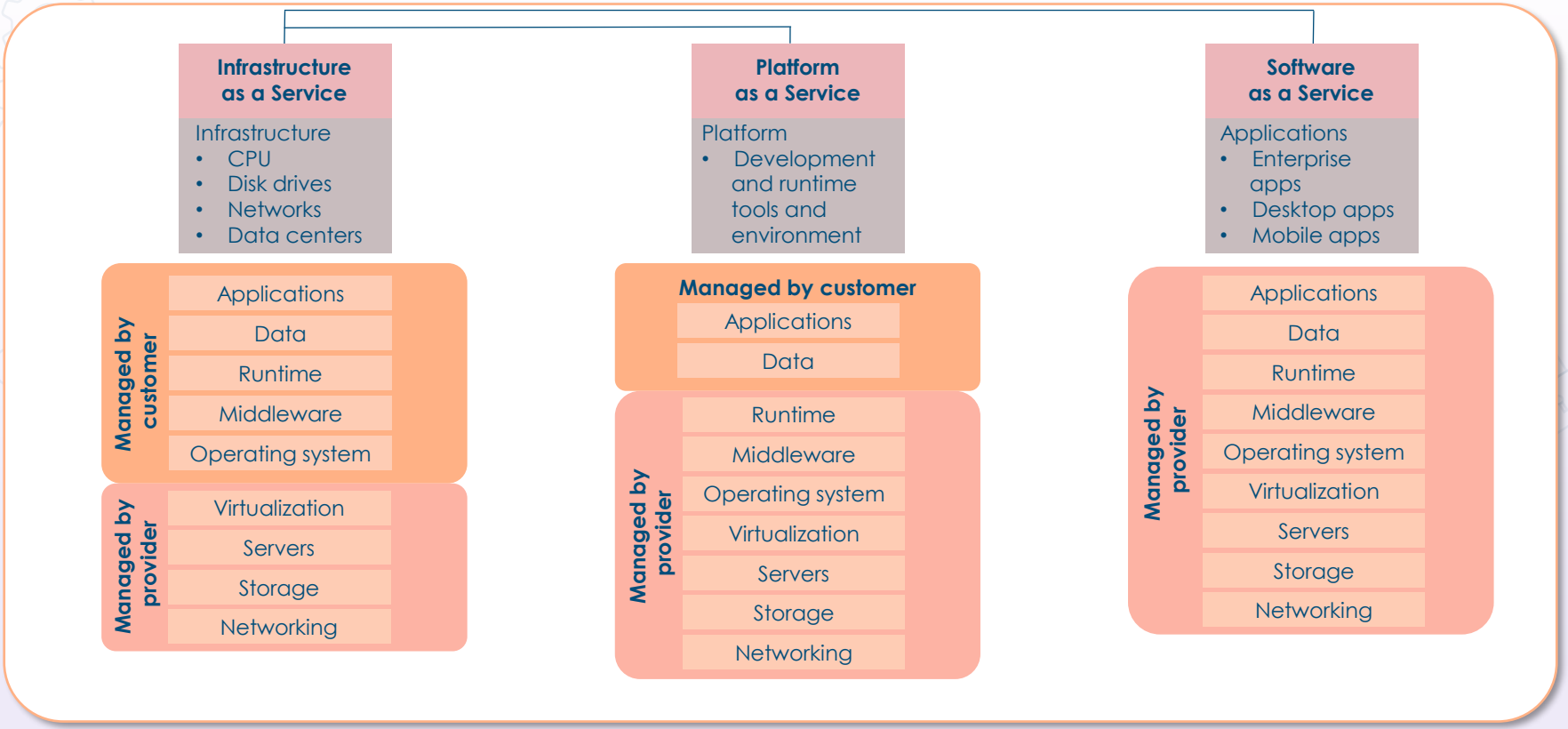


- VM sprawl
  - When the number of VMs overtakes the administrator's ability to manage them and the available resources
- VM sprawl avoidance
  - Enforce a strict process for deploying VMs
  - Have a library of standard VM images
  - Archive or recycle under-utilized VMs
  - Use a virtual machine lifecycle management tool or a cloud service provider-managed service

Virtualization Issues

- VM escape
  - A serious threat where a process running in the guest VM interacts directly with the host OS
- 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
  - Strong access controls and passwords

Cloud Computing Service Types



IaaS According to NIST

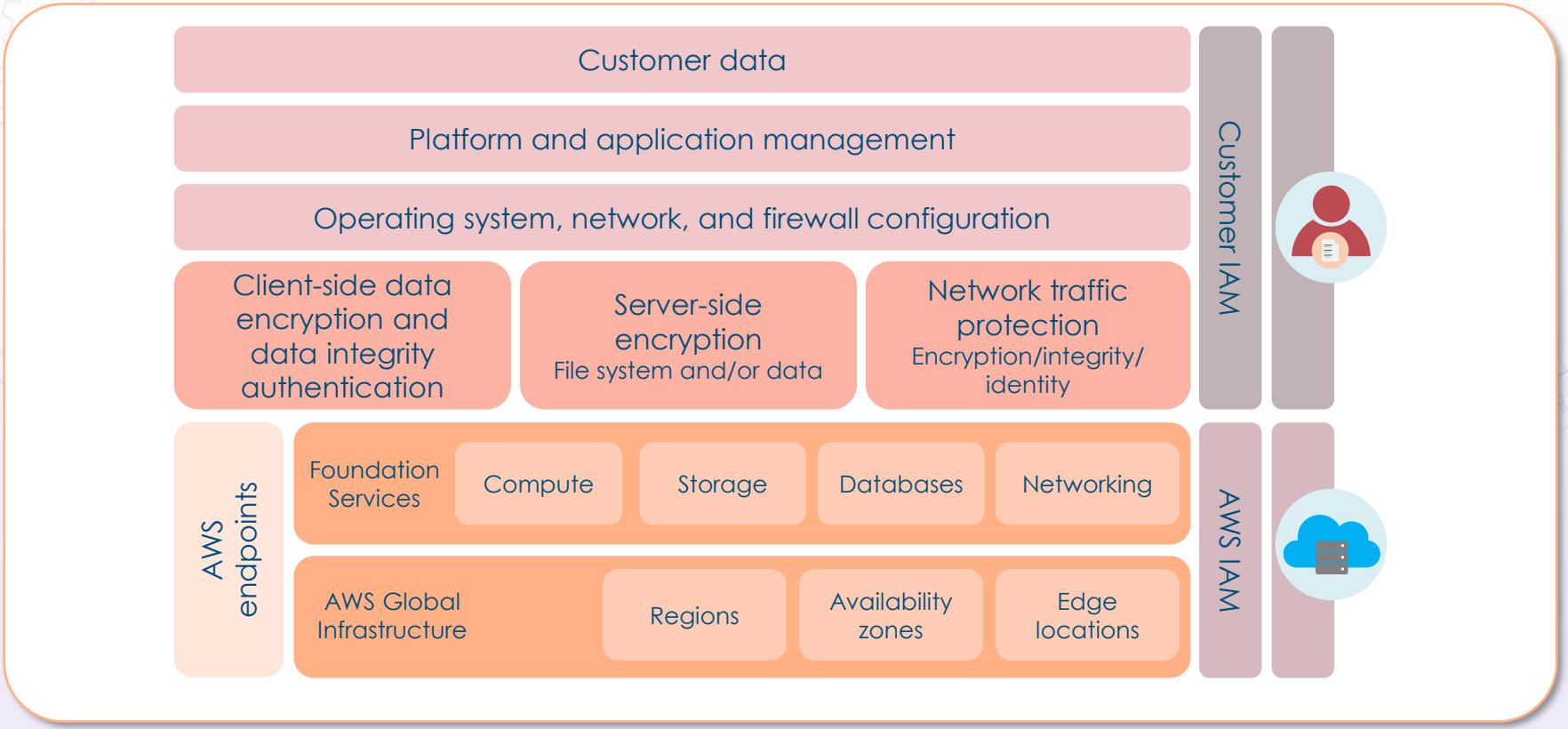
"The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls)."

CSRC Content Editor, "Infrastructure as a Service (IaaS) - Glossary," CSRC, accessed May 5, 2021, https://csrc.nist.gov/glossary/term/Infrastructure_as_a_Service.

Cloud Providers Global Infrastructure

Cloud Providers Global Infrastructure



PaaS According to NIST

"The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider.

The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations"

CSRC Content Editor, "Infrastructure as a Service (IaaS) - Glossary," CSRC, accessed May 5, 2021, https://csrc.nist.gov/glossary/term/Platform_as_a_Service.

Common PaaS Offerings

Development and SDK platforms for Java, PHP, Python, etc.

Container services for Docker and Kubernetes

Managed and fully managed relational and document databases

Managed security and threat modeling services

SSO, machine learning, AI, IoT, blockchain, media services

SaaS According to NIST

"The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser.

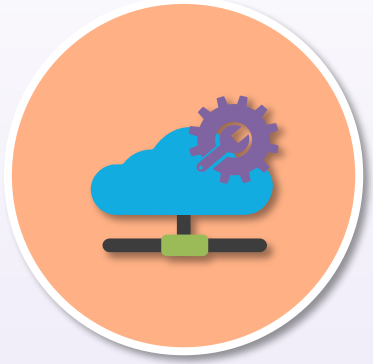
The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings."

CSRC Content Editor, "Software as a Service (IaaS) - Glossary," CSRC, accessed May 5, 2021, https://csrc.nist.gov/glossary/term/Software_as_a_Service.

Common SaaS Offerings

- Customer relationship management (CRM)
- Human resources and workplace tools
- Finance, sales, and marketing
- E-mail, collaboration, and storage
- Help & service desk and virtual call center

Cloud Models



Private – deployed in sandbox within an organization

Public – deployed by a provider for customer consumption

Community – deployed by a consortium in a certain sector

Hybrid – combination of private, public, or community

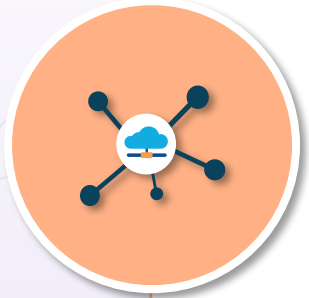
Managed Security Service Providers (MSSPs)

- A managed security service provider (MSSP) offers outsourced security monitoring and management for security systems and devices
- Common MSSP services:
  - Managed layer 3-7 firewalls
  - Intrusion detection and prevention (IDS/IPS)
  - Endpoint response and detection
  - Virtual private networking support
  - Vulnerability scanning and anti-viral services

Managed Security Service Providers (MSSP)

- MSSPs use high-availability security operation centers (either from their own facilities or from other data center/cloud providers)
- They offer 24/7 services with the goal of reducing the on-premises operational security staff the enterprise needs to hire, train, and retain to preserve a mature security posture

Cloud Access Security Brokers (CASB)

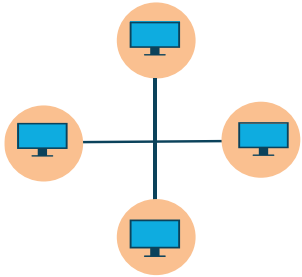


- Software service implemented between cloud customer and Software as a Service provider
- Could be on-premises or in-service provider cloud
- Acts as a gatekeeper to help enforce enterprise security policies while cloud resources are being accessed
- Extend organization's policies beyond local infrastructure
- Provides visibility, compliance, data security, and threat protection
- Can assist with implementation and enforcement of identity and access management, as well as single sign-on
  - Federated access with web service sign-on
  - Implement SAML 2.0, OAUTH, OIDC, Active Directory integration

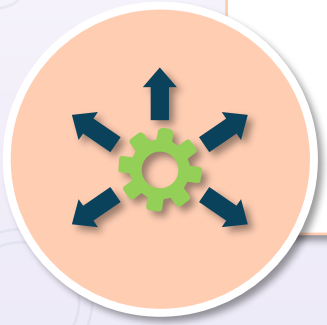
Distributed System Attributes

Securing Distributed Systems

- A distributed system needs more security measures than centralized systems, as there are many users, differentiated data, multiple sites, and distributed control
- Security engineers must consider many permutations of failures and errors that can happen at any time, independently or in combination with other error conditions
- In distributed communication systems, there are several types of exploits:
  - Passive eavesdroppers that monitor messages and collect private information – information leakage
  - Active attackers that not only eavesdrop but further corrupt messages by inserting new data or modifying existing data
  - Distributed Denial of Service (DDoS) and botnets
  - Unauthorized access through poor access controls



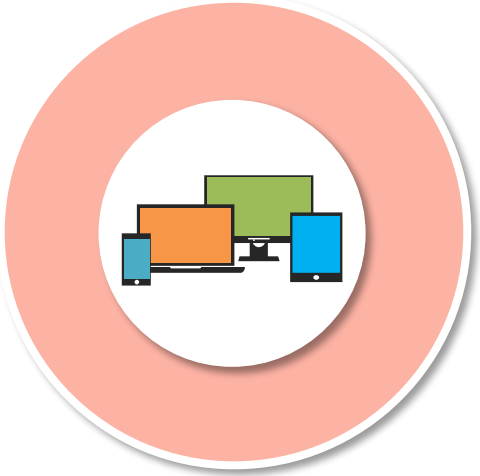
Securing Distributed Systems



- Communications can be secured with IPsec or TLS
- Data at rest can be authenticated, authorized, validated, and encrypted with strong algorithms and modes (AES-GCM-256)
- Layer 2 can be secured (i.e., SANs) with 802.11AE MACsec

Mobile Deployment Models

BYOD



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

Mobile Deployment Models

CYOD

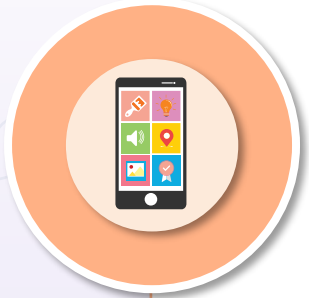
- **Choose Your Own Device**
- Much like BYOD in that it lets employees work from anywhere using a mobile device
- CYOD devices must be approved by the organization, unlike BYOD
- Users often select from a list of approved devices, which are usually smartphones
- These networks offer more stability,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

Mobile Deployment Models

COPE

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

Enterprise Mobility Management (EMM)



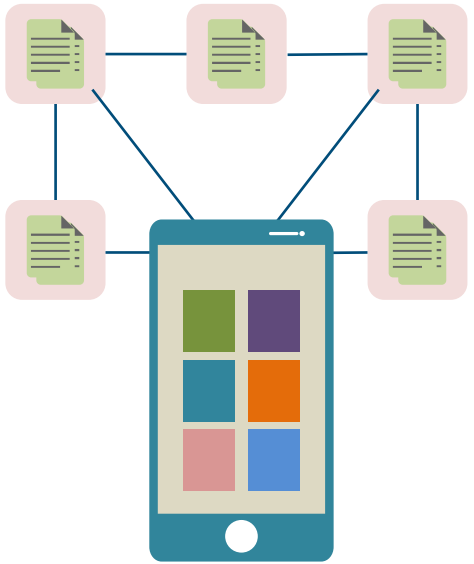
- Organizations must securely configure and implement each layer of the technology stack, including mobile hardware, firmware, O/S, management agent, and the apps used for business
- Solution should reduce risk, so employees are able to access the necessary data from nearly any location, over any network,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

Enterprise Mobility Management (EMM)

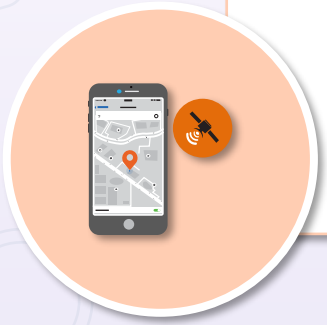
- There are three basic core competencies that all organizations need from an EMM solution:
  - **Visibility**: understanding what's running on mobile devices is the key to discovering potential risks and adhering to compliance policies
  - **Secure access**: providing the ability for mobile users to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

Mobile Device Management (MDM)

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

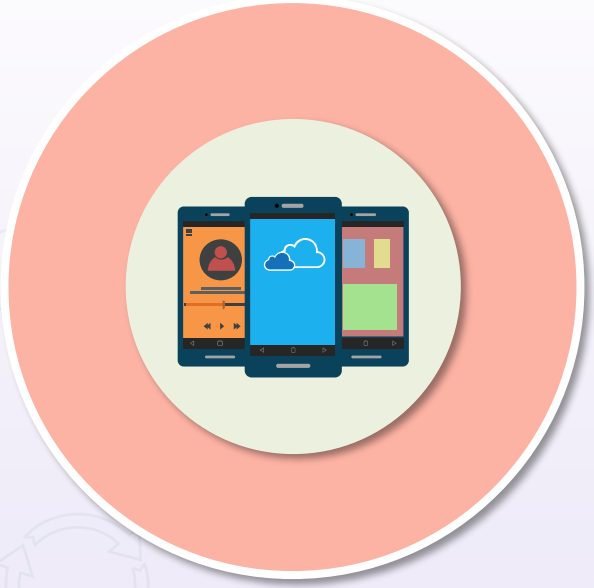


Mobile Device Management (MDM)



- Know your policy for enabling geolocation, as this is a vulnerability for certain sectors
- There is a risk of social surveillance by GPS with geotagging
- Geofencing can be used to put restrictions on where a mobile device can be actively used based on GPS
  - It could be based on RFID tagging

Mobile Application Management (MAM)



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

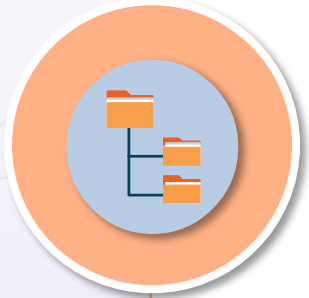
MAM Data Privacy Concerns

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

Jailbreaking

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

Rooting

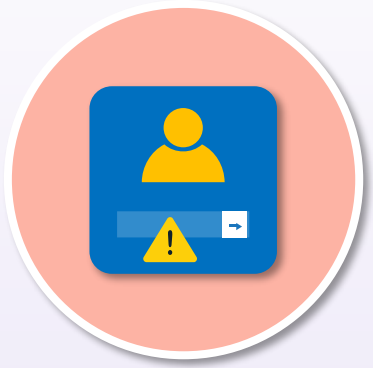


- Rooting grants full access to a device on a level much higher than jailbreaking, giving access to the Android system and beyond
- Every line of code in the Linux-based device becomes editable, with options only restricted by coding skills
- Since Android is open source, you can go into recovery mode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

Sideloading

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

EMM Challenges



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

Containerization and Sandboxing

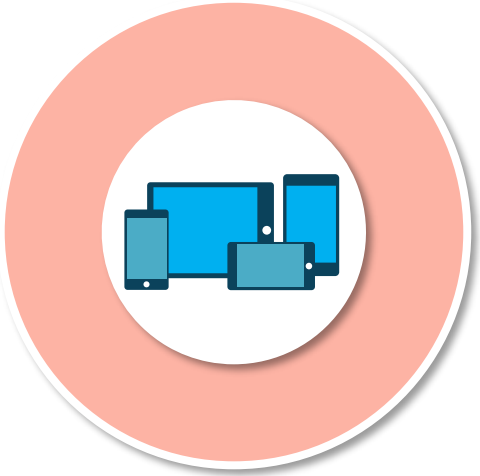
- Containerization is technically a technique that limits the environments in which certain code or apps can run
- Provides protection, isolation, and integrity functionality to get better levels of overall data isolation
- Users can continue to chat, text, and tweet without affecting business functions since sensitive apps and data remain protected within sandboxed containers with separate controls and higher security levels
- Apple iOS uses secure enclaves to prevent the main processor from gaining direct access to sensitive data
  - SEPOS includes its own kernel, drivers, services, and applications
  - Has its own set of peripherals accessible by memory-mapped dedicated I/O lines
  - Uses inline AES to encrypt external RAM

Application Wrapping

- Involves adding an additional management layer
- Allows MAM administrator to set specific policy elements that can be applied to an application or group of applications
  - Whether or not user authentication is needed for a certain app
  - Whether or not app data can be stored on the device at all
  - Whether or not specific APIs (e.g., file sharing) will be permitted

Modern EMM Attributes

MobileIron, AirWatch, and XenMobile



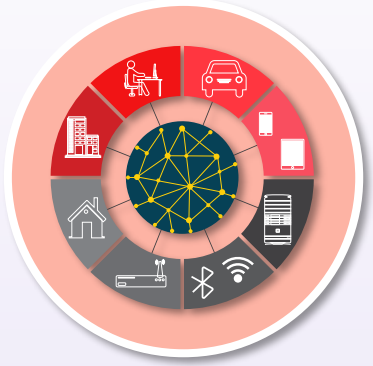
- Offer BYOD and MAM security capabilities
- Provide flexible bundles for different use cases
- Unified endpoint management
- End-to-end security and identity management (IdM)
- Enterprise integration
- Productivity applications
    - Create mobile business apps without writing code
- Introduce User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

Internet of Things

IoT

- The explosion of Internet of Things (IoT) and Internet of Everything (IoE) presents a challenge for embedding computing vulnerability discovery
- Systems are often powered by specialized chips or system-on-a-chip as well as some older unpatched version of Linux or Microsoft Windows

Example IoT Devices



- Sensors and smart devices
- Facility automation
- Commercial appliances and medical devices
- Vehicles and aircraft (manned/unmanned)
- Smart meters and sensors

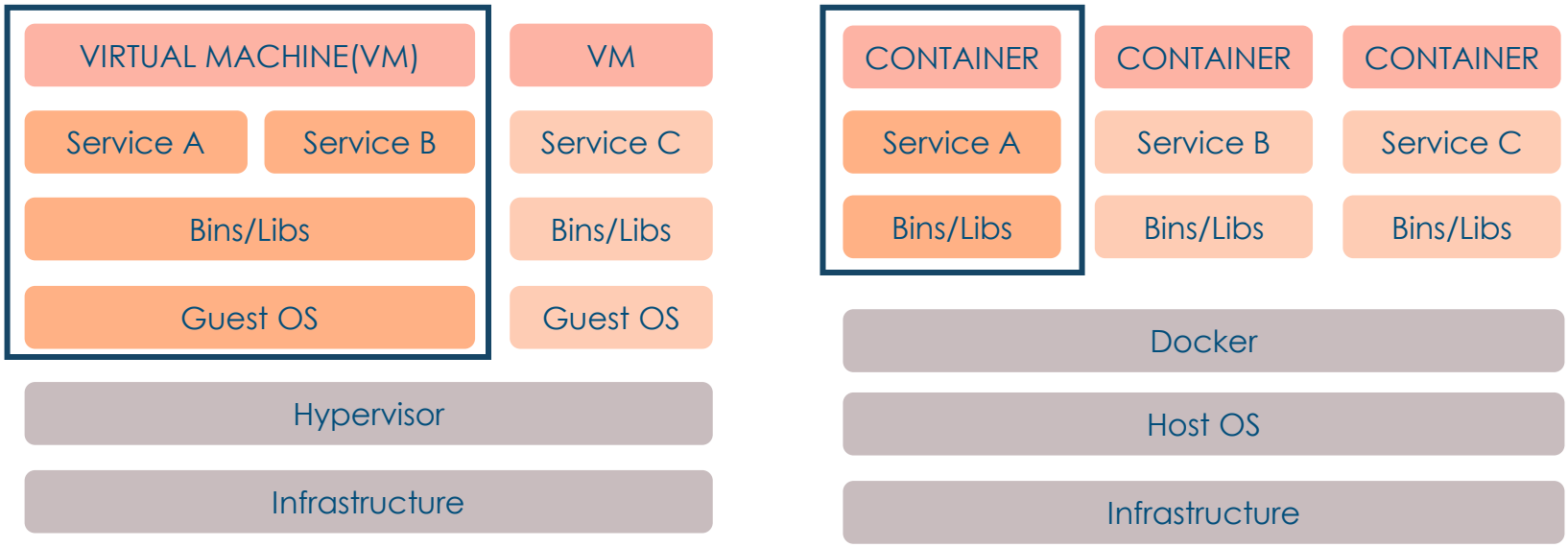
OWASP IoT Top Ten Vulnerabilities

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

Containers

- Isolated abstracted applications with all components included in a modular form (code, bins, libraries, dependencies)
- Portable modules across platforms and cloud providers allow for ease and consistency
- Can be server-based on serverless in the cloud
- Container isolation is done on the kernel level without the need for a guest operating system
- Self-contained environments allow for rapid deployments, closer parity between development environments, and unlimited scalability

Virtual Machines vs. Containers



Docker vs. Kubernetes

Automation vs. orchestration

- Docker is a containerization platform
- The Docker Engine is the runtime that allows you to build and run containers
- Docker is currently the most popular container platform, and over 30% of enterprises currently use Docker in their AWS environment

- Kubernetes is an orchestrator for container platforms
- It is a comprehensive system for automating deployment, scheduling, and scaling of containerized applications
- It is the industry leader and supports many container tools, such as Docker

Docker vs. Kubernetes

Life of an application

How do you package and distribute an application?

Docker

First week

How do you scale, run, and monitor an application

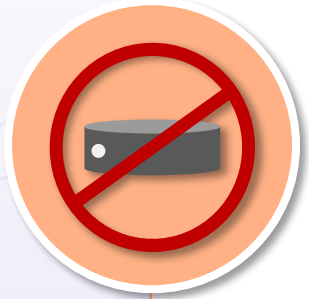
Kubernetes

Next 8 years

Serverless Architectures

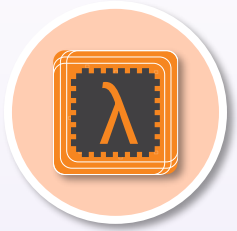
- Serverless cloud architecture lets the customer move more responsibility to the provider, while enhancing agility and innovation of applications
- Serverless is also known as Functions as a Service when running serverless code in a wide variety of use cases
- It also enables the customer to run container applications and services without having to consider underlying servers
- Serverless architectures eliminate infrastructure duties, such as provisioning, patching, maintenance, and capacity management

Serverless Architectures



- This solution can be used for nearly every type of application or back-end service, and everything needed to run and scale an application with high availability is controlled for you by the CSP
- When building serverless applications, developers can focus on the core product or service as opposed to managing and operating servers or runtimes, either in the cloud or on-premises
- The reduced overhead empowers developers to get back time and energy that can be used on further delivery of reliable and scalable products and services in the cloud

Serverless Architectures



AWS Lambda and Azure Functions

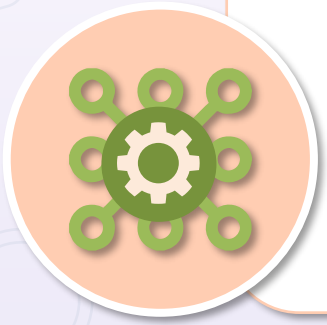
Serverless code

- Solutions let you run small pieces of code called functions that you only pay for when running
- You do not need to deploy a server or application infrastructure
- Run code based on HTTP requests, predefined schedule, API call trigger, security event, manually, and much more

Serverless containers

- AWS Fargate is a serverless compute engine for containers that works with both Elastic Container Services and Kubernetes
- It eliminates the need to provision and manage servers, lets you stipulate and pay for resources per application, and enhances security through application isolation by design

Microservices



- Microservices are specific service-oriented application components
- An architectural approach to software development where the results are made up of small independent services that communicate over well-defined APIs
- These services are typically maintained by small, self-contained teams of developers
- Microservices architectures make applications faster to develop and easier to scale
- They enable innovation and fast-tracked delivery of new application features

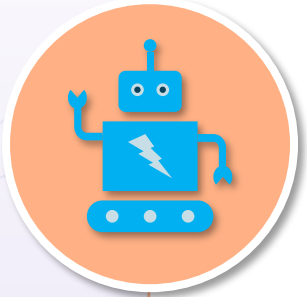
Microservices

- Tightly scoped but loosely coupled
- Thoroughly modular and encapsulated
- Independently deployable
- Freely scalable
- Communicate using notification and queueing services

Embedded System Security and Constraints

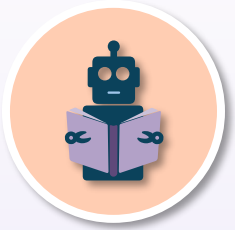
- Complete embedded source code is often not available
- Many of the device drivers and other components are simply binary sites with no source code at all
- Even if a patch is available, it is rarely applied in a consistent manner
- Hundreds of millions of devices are sitting on the Internet, unpatched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

Raspberry Pi



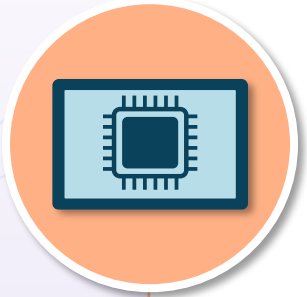
- Sequence of small, single-board computers developed by the UK Raspberry Pi Foundation
- Originally designed to teach computer science in schools and developing countries
- System exploded in popularity, especially for robotics
- No peripherals or cases included, although some accessories are included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

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 Systems

RTOS

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

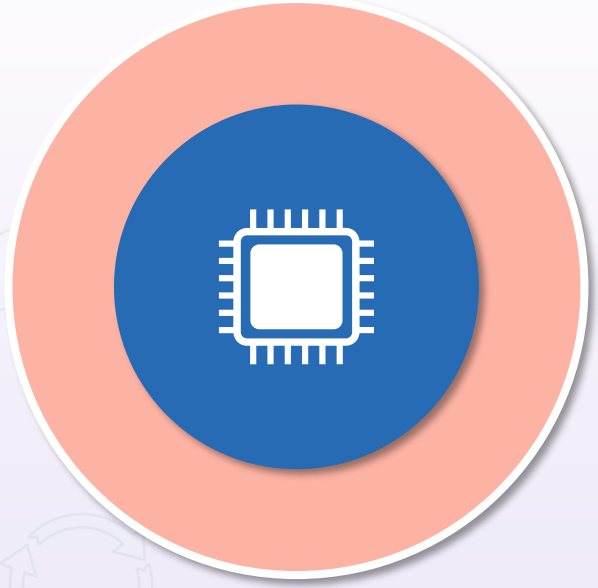
Securing Embedded Devices

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

Other Specialty Systems

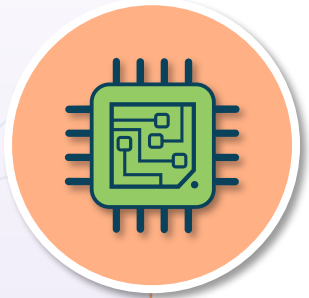
- Multifunction printers (MFP) – a combination of email, fax, photocopier, printer, and scanner
- Adaptive voltage scaling (AVS) – a closed-loop dynamic power minimization method that adjusts the voltage sent to a computer chip to match the chip's needs during operation
- Unmanned aerial vehicle (UAV)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

Boot Integrity with UEFI



- Unified Extensible Firmware Interface replaces legacy BIOS
  - Low-level software for booting the device
  - Tests the hardware components (POST)
  - Gets the OS up and running
  - Offers the ability to protect the device at a lower level with passwords

Hardware Root of Trust



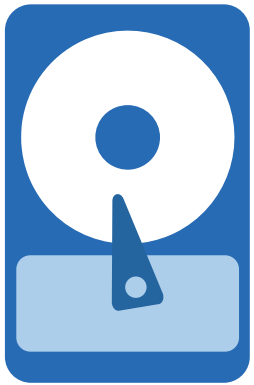
- Hardware root of trust
  - Anchoring the trustworthiness of a system to hardware not software
  - Hardware solutions are more secure than software solutions
  - Less susceptible to attacks since security solutions are on-chip
- Foundations of a Trusted Execution Environments (TEE) or Trusted Computing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

Trusted Platform Module (TPM)

- Computer chip (microcontroller) installed on the device or built into PCs, tablets, and phones
  - Tamper-resistant security chip
  - Stores info needed to authenticate the platform
  - Passwords, certificates, and 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)

Self-encrypting Drives (SEDs)

- Implements full disk encryption (FDE)
- Hardware-based data encryption
  - All contents on the drive are encrypted, including keys always
  - Encrypts data as written and 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, and device authentication
  - Encryption, key management, network access control, and policy compliance



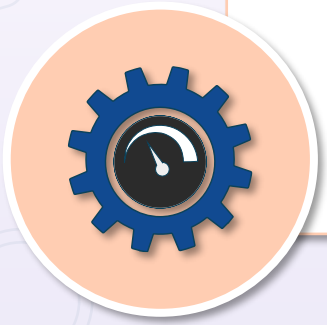
OPAL

- The TCG Opal Security Subsystem Class (SSC) is a group of specifications for SEDs created by the Trusted Computing Group (TCG)
- The Opal SSC defines a hierarchy of security management standards to secure data from theft and tampering by unauthorized persons who can access a storage device or host system where the storage device resides

HPC and Edge Computing Systems

- High Performance Computing (HPC) facilities are connected to 10/100 Gigabit networks just like other compute systems and often run the same Linux-based OSs
- They have always been victimized by many of the same vulnerabilities, be they compromised access credentials, system misconfigurations, or software bugs
- Some HPC systems run very unusual hardware and software stacks and may have quite different and specific purposes (high-end math functions) and modes of operation than most general-purpose computing systems

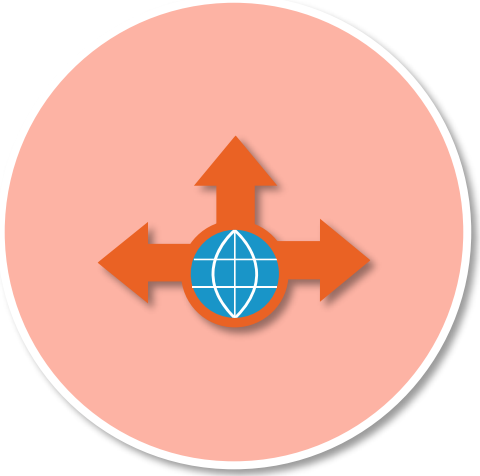
HPC and Edge Computing Systems



- What sets HPC systems apart is often not the hardware and software but rather the types of sensitive data being processed and analyzed
- Because of the speed of these systems, distributed attacks and polymorphic malware outbreaks will spread faster
- These are also prime targets of privileged insiders

Edge Computing Systems

Content delivery networking (CDN)



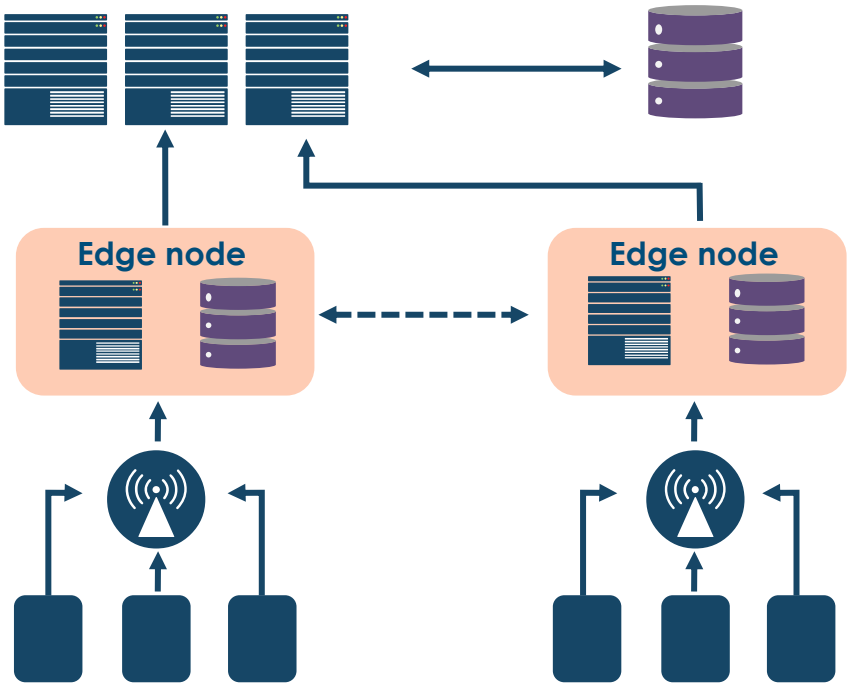
- Edge computing is a distributed computing standard that brings compute services and data storage close to the site where it is needed to speed up response times and preserve bandwidth
- CDN solutions place cached versions of content (often in elastic Redis in-memory storage clusters) at metro area edge locations
- Security is a shared responsibility model between customers, ISPs, and CDN providers

Edge Computing

CLOUD

EDGE

- Service delivery
- Computing offload
- IoT management
- Storage & caching



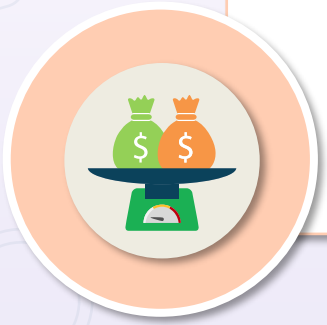
Securing AWS CloudFront CDN

- Deploy web application firewall (WAF) on the distribution node in the cloud
- Cloud-based DDoS protection and threat services (Shield Advanced and GuardDuty)
- All control API calls must be digitally signed and use TLS-enabled endpoints
- Private Content feature controls who can download content from CloudFront
- Origin access identities control access to original copies of objects (usually in S3)

Operational Physical Security

- Physical security aims to ensure the safety and CIA of all resources in the organization from
  - environmental threats
  - natural disasters
  - man-made attacks
  - supply system threats, and
  - socio-political threats

Primary and Secondary Loss

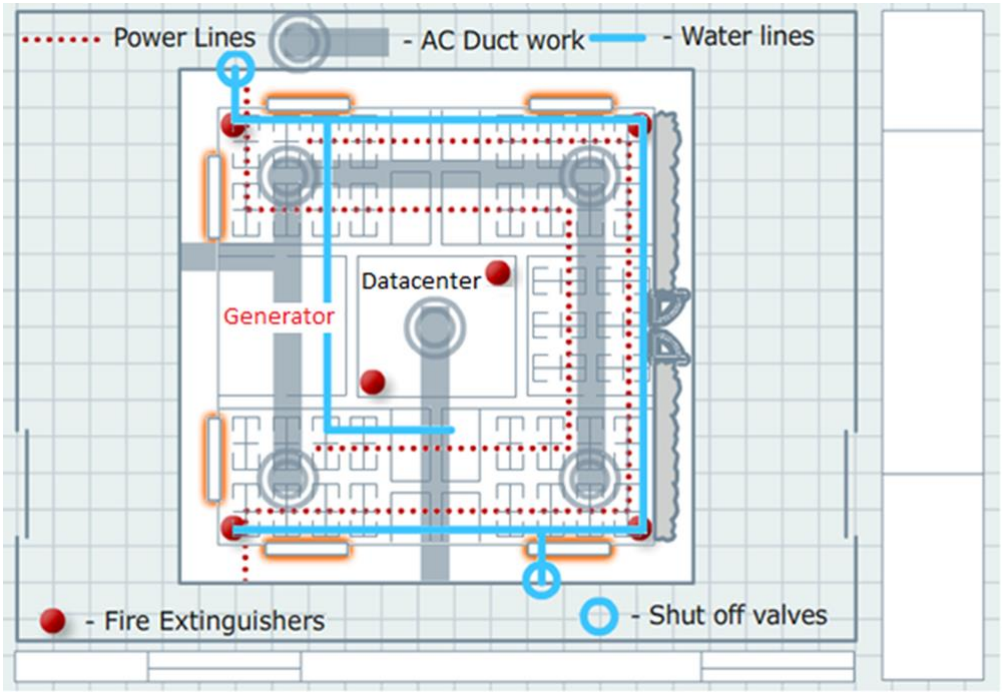


- Loss of life
- Interruption to operations
- Productivity loss
- Response
- Loss of revenue
- Compromised CIA of assets
- Replacement costs
- Damaged public image and reputation
- Loss of customers or competitive advantage
- Fines and judgments

Physical Defense-in-Depth

- When designing physical security controls, use a defense-in-depth approach
  - Begin at the property or facility edge and work back to the most valuable assets
  - Begin at "the keep" of valuables and work your way out to the physical edge
- This course will take an "outward-in" approach
- Different sites will have varying demarcation points of physical and logical entry

Know ALL ingress and egress points



Perimeter Barriers

- Landscaping
- Fences
- Tire shredders
- Bollards
- Moats or ponds
- Gates

Gates Are Separated into Classes

- Class I: Residential gate operation
- Class II: Commercial, like 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.)

Fence Barriers

- Most organizations will have protective fence barriers around the perimeter to deter or prevent individuals from unauthorized entry and exit
- Fences may only be used in certain zones or areas to protect junction boxes, generators, dumpsters, and shredding service pickup points
- High security areas will use barbed wire and/or electric fences combined with warning signs every 6-8 feet
- Fences are combined with entry/exit gates of varying strength
  - Barricade gates
  - Tire shredders

Bollards

Vertical posts

- Bollards are strategically placed pylons meant to prohibit vehicles from entering certain areas
- Placed in front of buildings, in parking lots, or along sidewalks to guide pedestrian traffic
- Typically concrete or strong metal
- High-tech bollards can be mechanical and include cameras and sensors
- Can be vertical or horizontal

Signage

- Signs are a deterrent control
- Signs and window stickers are designed to deter individuals from doing something unauthorized
- May also be combined with harmful fences
- A logical system banner is also a form of signage

Signage


Authorized Personnel Only
Do Not Enter
No Trespassing
KEEP OUT
Authorized
Personnel Only
Beware of Dog
Caution Electric Fence
Armed Guard on Duty

CCTV and Security Cameras

- Provide a way to monitor and record the property perimeter and other facility areas for intruders and potential attackers
- Considered a detective control primarily although their very presence can be a deterrent
- Commonly, are recording devices sent to monitoring stations with security guards or technicians
- Backup recorded media should be securely stored
- Should trigger alerts when a camera is disabled
- Should be combined with adequate lighting and all "dead spots" should be covered

Lighting

Visibility

- Internal and external systems
- Low lights for posts and patrolling
- Glaring lights for intruders
- Common types of protective lighting systems include the following:
  - Continuous lighting – the most common type of lighting
  - Trip lighting – lighting activated by some trigger or sensor
  - Standby lighting – lighting activated when suspicious activity is suspected
  - Emergency lighting – lighting used for limited times when power fails

Lighting

Mercury vapor

- Least temperature sensitive
- Preferred outdoor security lighting
- Long life, strong illumination, turns on slow

Quartz

- Bright white light (high visibility)
- Turns on immediately
- Ideal for perimeters and problem areas (1,500 to 2,000 watts)

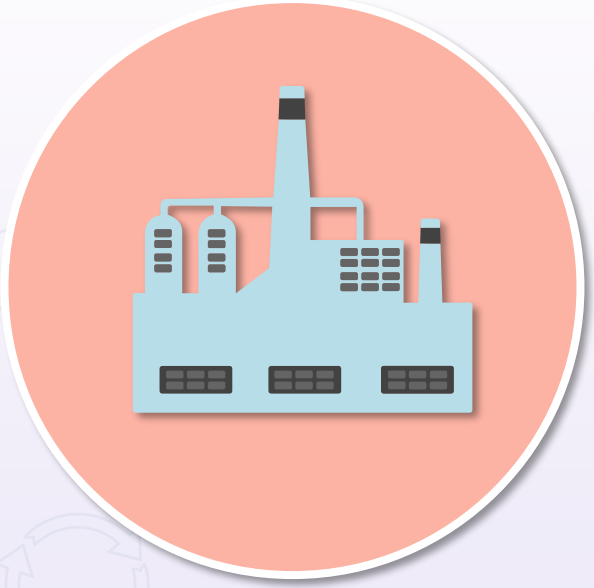
Sodium vapor

- Soft yellow light
- More effective than mercury
- Great in fog

LED

- Cost-effective
- Inexpensive and available

Industrial Camouflage



- Cameras and surveillance devices are often camouflaged in landscaping elements, statues, and tall trees
- For example, towers carrying cell phone and other equipment are covered by fake trees
- Certain high-security rooms can be underground and set at distance from main buildings

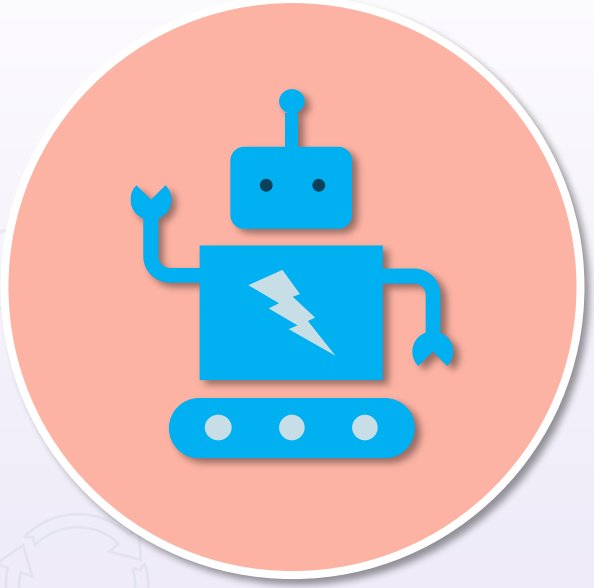
Security Guards

- Guards are typically 24x7 but could be just on-site during business hours or off-hours
- They are a security control of multiple types: detective, preventative, and deterrent
- They can provide rapid security response if an intrusion or incident occurs
- Should also interface with other law enforcement

Security Guard Considerations

- Do you hire or contract, freelance, or certified/licensed?
- Will they be armed or unarmed?
- What is the impact on insurance policies?
- Are you involved with screening and background checks?
- Who provides the ongoing training?

Robotic Sentries



- Robot sentries can be used in home or commercial environments as security guards with cameras, sensors, and more
- The Samsung SGR-A1 is a type of sentry gun that was developed jointly with Korea University to support South Korean troops in the Korean Demilitarized Zone

Motion Detection Sensors

- Photoelectric – break in a light beam
- Passive infrared – infrared light
- Vibration – change in the level of vibration
- Acoustic – change in sound waves
- Microwave – change in radio waves
- Electromechanical – break in an electrical circuit
- Electrostatic – change in an electrostatic field
- Moisture and temperature detection – for server rooms and data center environmental controls

Sensors Trigger Alarms

- Static or flashing light on display panel
- Bell rings or horn blares (>130 decibels)
- SMS or text message sent
- Telephone call or software alerts to security desk or law enforcement
- Silent alarms

Locks

- Locks are the most common physical security mechanism
- They are considered a preventative control although they technically only delay entry – not prevent it in the long run
- Locks keep honest people out but cannot deter resolute intruders, since most locks are easily bypassed, and most keys are readily duplicated
- They can be physical, electronic, and/or biometric

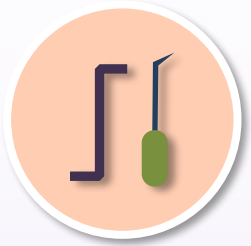
Types of Locks

- Key lock – a lock that requires a key to open
- Warded – wards are obstructions to the keyhole that prevent all but the properly cut key from entering
- Wafer/tumbler – wafers under spring tension are in the core or plug of the lock and protrude outside the diameter of the plug into a shell formed by the lock body
- Deadbolt – a bolt inserted into the frame of the door for additional security when combined with other locks

Types of Locks

- Interchangeable core – a lock with a core that can be removed and replaced using a special-change key
- Combination – a sequence of numbers in proper order
- Electronic combination – digital readouts obtain power from the energy created when the dials are turned – better security than combination locks, but more expensive
- Keyless – has buttons that are pushed in sequence to open the door – sometimes called a cipher lock
- Smart lock – inexpensive plastic card that is pre-authenticated to open a door – used in most hotels

Breaking Physical Locks



Picking

Uses a tension wrench to rotate the key plug of the lock to find the lock tumblers

At the same time, the pick is used to move the binding tumblers, one at a time, to the shear line

When all the tumblers are aligned properly with the shear line, the lock opens

Raking

Uses a pick that has a wider tip inserted all the way to the back of the plug

The pick is then pulled out quickly so that all the pins are bounced up, and as the rake exits, a tension wrench turns the plug

Upper pins will fall on the ledge created by the turning pins, so remaining pins can be picked

Brute force

Brute force techniques will always be successful given enough time and effort

This involves using hammers, tire irons, firearms, explosives, and more

This contributes to locks being a "delay" control, in practicality

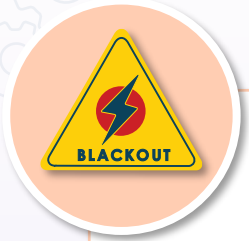
Personnel Controls

- Many organizations will have all guests register at a reception area security desk
  - Collect and input identification information in visitor log
  - Camera station with picture for temporary badge
  - Distribute temporary access cards or badges
- Guests and contractors may go through rapid background checks and identity validation procedures
- Guests may need to always be escorted by another employee or security officer to provide two-person integrity and control
- No piggybacking and tailgating policies

Power Controls

- Power system security involves practices to keep the system operating when subcomponents fail
- Most power systems are operated so that any single initial failure event will not leave other components heavily overloaded
- Enterprises should deploy redundant providers, surge protectors, Uninterruptible Power supplies, and various backup generators
- Junctions should be secured and have adequate lighting and cameras

Blackouts vs. Brownouts

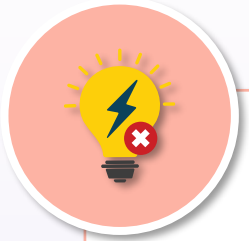


Blackouts

The complete stopping of electrical power in an area for longer periods of time

Can last from hours to days and can extend into weeks in case of a serious emergency or a natural disaster like thunderstorms, floods, or earthquakes

Can also occur due to a technical problem at grid stations, the electricity production site, or some issues with transmission lines



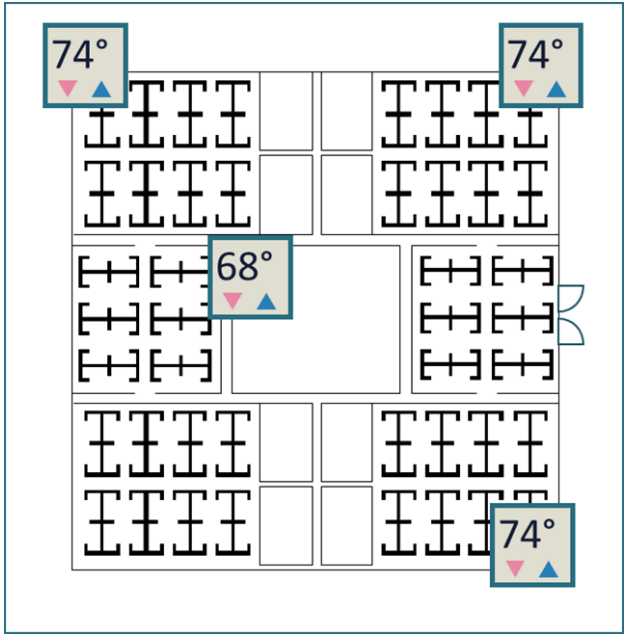
Brownouts

Intentional or unintentional sags, slumps, or drops in electrical voltage

Are not insignificant as they can be very damaging to electrical devices and can cause them to function poorly and eventually go bad

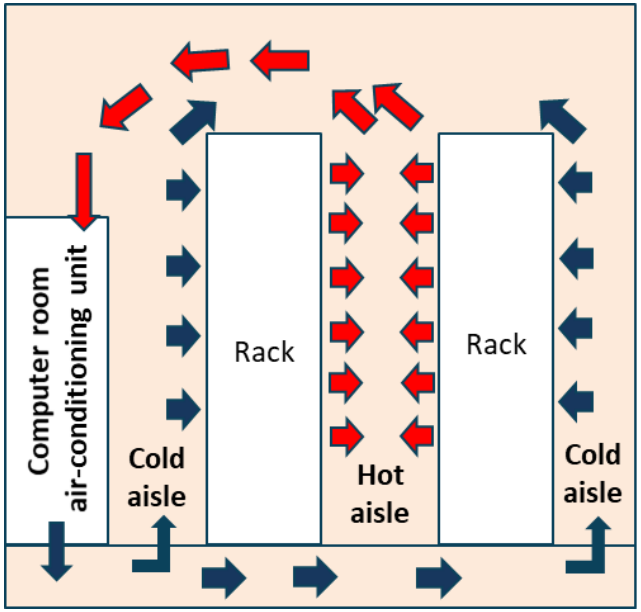
Brownouts can occur due to a thunderstorm, rain, or any other natural disaster

Environmental Controls



- Poor heating, ventilation, and air conditioning (HVAC) lead to extreme heat, extreme cold, extreme humidity, and/or extreme dryness
- Needs proper monitoring and ongoing maintenance (e.g., pressurization and temperature)
- Physical security of all components and controllers is a concern
- Location options may be limited by the facility
- Environmental control can also include the possibility of chemical and biological leaks or attacks

Hot and Cold Aisles

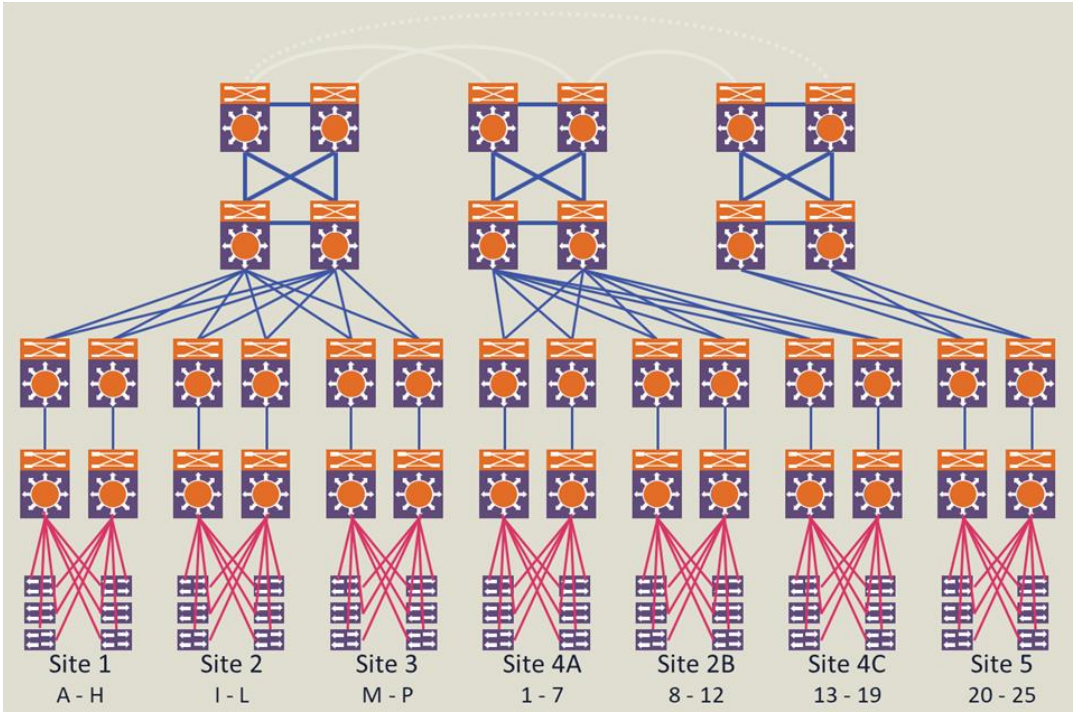


- Heating, ventilation, and air-conditioning (HVAC) are vital environmental issues
  - Poor HVAC leads to extreme heat, cold, humidity, or dryness
  - Recommended temp: 72 to 76 degrees
  - Recommended humidity: 40-60%
- Maintain hot and cold aisles in the server rooms and data center to move hot air from devices into a hot aisle and redirect to an air conditioning unit or room
- Should have separate air-conditioning controls for data center or server room

Distribution Frames and Wiring Closets

- Gain visibility into all ethernet and fiber cable runs as well as the security of distribution frame (MDF rooms) rooms and closets
    - Under the floor
    - Above ceiling panels
    - In the walls
- Lock all doors to server rooms and frame rooms
- Cameras can be used along with other types of sensors and access alarms
- No window access or use security windows with wire mesh
- Use hardened management stations and environmental controls for temperature, fire, gas, and humidity

Distribution Frames and Wiring Closets



Router Man backbone
Connected by dark fiber

Site backbone
One per MAN region
Three on main campus

Core

Desktop cluster
One per site
Seven on main campus

BDF
Building Distribution Frame
One per building
41 in main campus

Distribution

IDF
Intermediate Distribution Frame
Two per floor

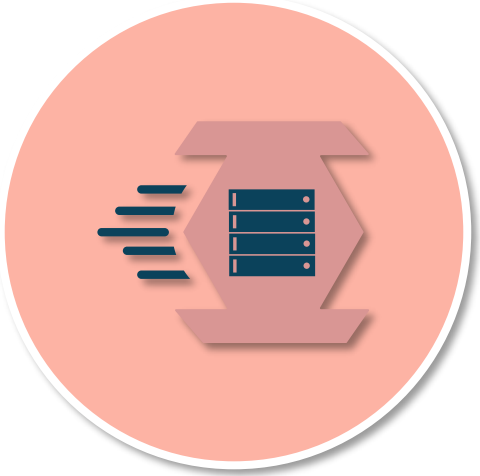
Access

Server Rooms and Data Centers

- Know all ingress and egress points
- Implement protective barriers
- Have redundant and monitored support systems
- Get visibility into all power conduits and water lines
- Have visibility into high-security compartmentalized areas
- Work with facilities management to integrate blueprints and topological diagrams into IT services

Server Rooms and Data Centers

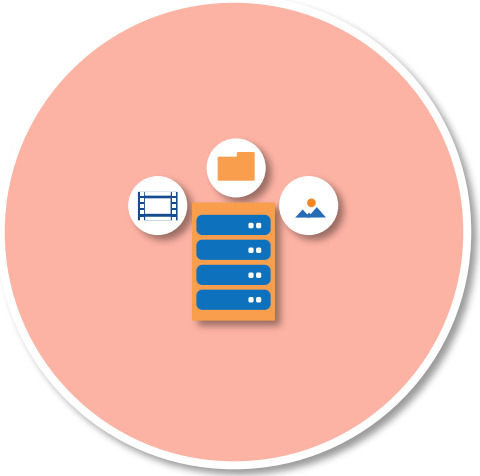
Control physical access



- Access control both at the perimeter and at room ingress points – by professional security staff using video surveillance, intrusion detection systems, and other electronic methods
- Authorized staff should pass two-factor authentication a minimum of two times to access data center floors
- Biometric multifactor authentication (MFA) is highly recommended
- All visitors and contractors should show identification and be signed in and continually escorted by authorized staff

Server Rooms and Data Centers

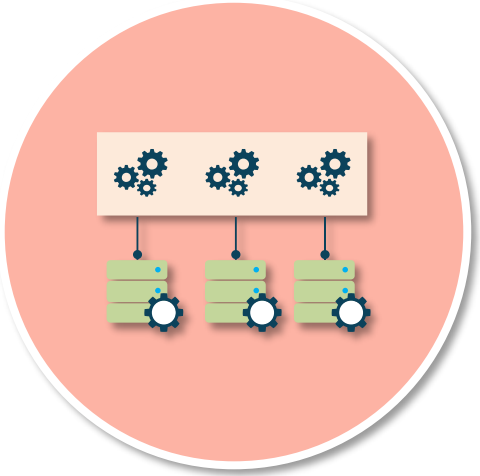
Control physical access



- When an employee no longer has a business need for data center privileges, access must be immediately revoked, even if they continue to be an employee
- Automatic fire detection and suppression equipment
- The electrical power systems should be fully redundant and maintainable without impact to operations 24/7
- Uninterruptible power supply (UPS) units can provide back-up power for critical and essential loads in the facility in the event of an electrical failure
- Data centers often use generators to provide back-up power for the entire facility

Server Rooms and Data Centers

Control physical access



- Airgap is the physical separation of the control network and other networks
- Separate the highly secure networks from the unsecured networks with physical or logical compartmentalization
- Log and audit all devices and objects entering and exiting facility
- Stop malicious and privileged users from having individual access
- Use private clouds, sandboxes, and detonation chambers

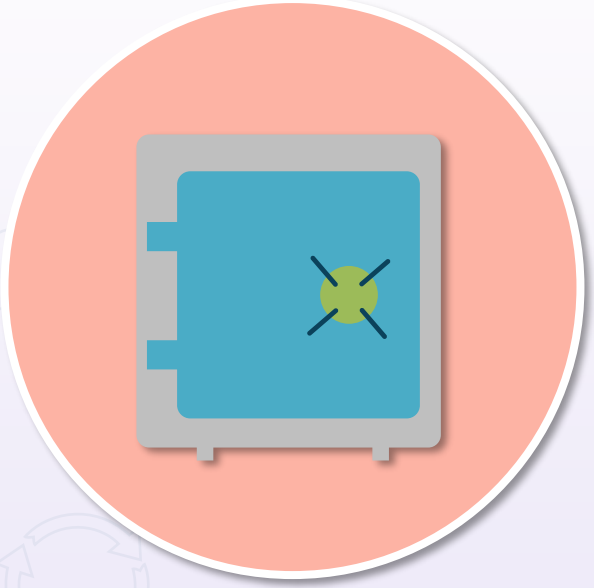
Secure Enclosures

- The corporate safe may be the highest value asset in the organization based on the contents
- Safes are used to protect valuable items, such as currency, deeds, securities, policies, precious metals, cybercurrency cold storage devices, and failsafe passwords
- Employees may need a special area to store and protect valuables, such as lockers or locked cabinets
- A reinforced filing cabinet is a type of secured container designed to withstand burglary attempts
- The U.S. government provides container classifications for these reinforced containers, based on the time taken to break into them, either covertly or surreptitiously with no forced entry

Safes

- The Underwriters Laboratory (UL) provides safe classifications that specify the degree to which safes can withstand attack
  - For example, a safe that takes 30 minutes to break into using various tools and torches is classified as a Tool Resistant safe class - TL30

Safes

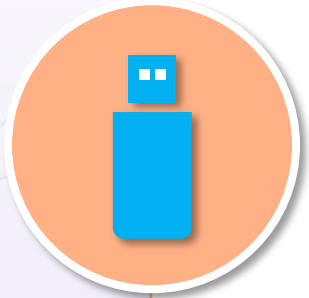


- Factors considered in classifying the safe:
  - Lock mechanism factors to open the safe
  - Material used to construct the safe
  - The weight and whether it's securely anchored or embedded in concrete
  - The tensile strength of the steel
  - Whether the safe has a relocking device

Media Storage Facilities

- Often stores data backups and redundant spares
- May include hard copies of document and microfiches, etc.
- Facilities and media storage should be part of COO plan and business continuity planning
- Same access policies that apply to data center and other sensitive areas of organization
- AWS, GCP, and Azure all offer long-term data archiving and hardware security modules (HSMs) with AES encryption

Media Storage Facilities



- Media storage should be covered with a disposition and destruction policy
- When a storage device has reached the end of its useful life, procedures should include a decommissioning process that prevents data from being exposed
- NIST 800-88 ("Guidelines for Media Sanitization") may be part of the decommissioning process

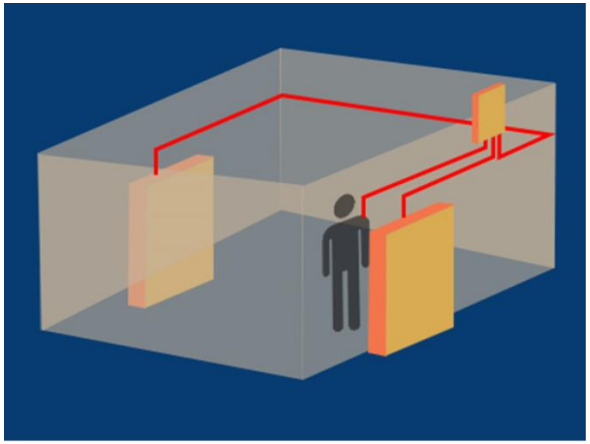
Evidence Storage

- Evidence room facilities are only as secure as the honesty of the staff
- Separation of duties and dual operator (two-person rules) are helpful policies
- Same stringent security as data center
- Chain of custody must be maintained for incident response, forensics, and law enforcement – contents of evidence room may have higher street value

Evidence Storage

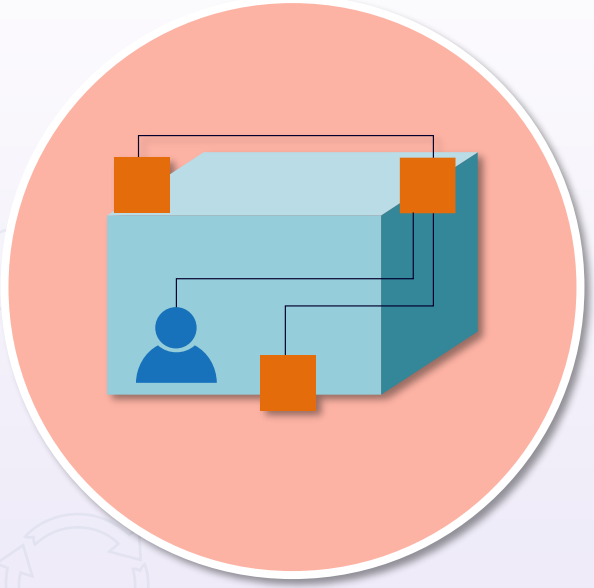
- Walls should be made of materials like cinder blocks or concrete instead of drywall, and all walls should extend from ceiling to floor, with no ability to access over the walls or through a false ceiling
- Doors must be solid, preferably steel, with no glass – preferably, there should be no doors leading directly to the exterior of the building from the evidence room
- Modern digital evidence management software should be used

Mantraps



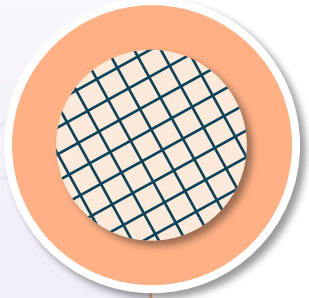
- A system that routes personnel through two interlock-controlled doors into an area
- The design specifies that the inner door will not unlock if the outer door is open, or vice versa
- In most cases, a person must produce some type of authentication to enter the second door
- Can also prevent "piggybacking" and "tailgating"

Mantraps



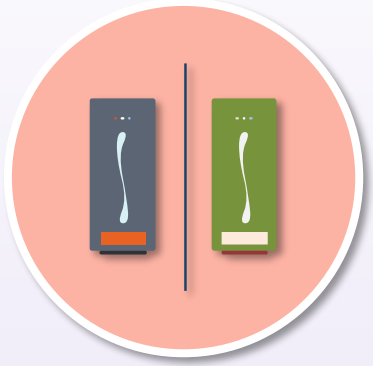
- The person can be identified and authenticated
  - Provide credentials and license or passport
  - Can include biometric readers
  - CCTV and intercom systems are often used
  - Security guard behind bullet-proof glass
  - The person is eventually allowed in through strong door with electronic locks

Faraday Cages and Bags



- Faraday cages are rooms, enclosures, or bags that block electromagnetic fields emanating from Electric Magnetic Interference (EMI), Carrington events, solar flares, and Electro-magnetic Pulses (EMP)
- The shield may be fashioned from a continuous covering of conductive material, or in the case of a Faraday cage, a mesh of similar materials
- These can often be found in data centers or other enterprise safe rooms
- Military grade faraday bags can also be used for removable drives, cold storage cybercurrency wallets, and other critical components

Air Gap



- Secure system has no access to Internet
- May be disconnected from any network
- Can be physical or logical (PVLAN)
- Still vulnerable to rogue insider
- Stuxnet was introduced to air-gapped area

Air Gap

- Military and governmental agency networks and systems
- Financial systems, such as stock and cybercurrency exchanges
- Industrial control systems, like SCADA, in water processing facilities
- Life-critical systems, such as nuclear power plants, computers used in aviation, and computerized medical equipment

Fire Controls

Prevention is key

- 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

Fire Suppression

Create barriers

- Firewalls to prevent the spread of fire

Use portable fire extinguishers

- Locate in strategic places throughout building

Use automatic water sprinkler systems

- Common, but can cause water damage and worsen electrical fires

Use halon substitutes or carbon dioxide discharge systems

- Commonly used around computers and networking equipment

Types of Extinguishers

- Type A - common combustibles, such as wood products, paper, and laminates
  - Suppressed with dry chemical, clean agent, wet chemical, water and foam
- Type B - combustible liquids, such as petroleum products and coolants
  - Suppressed using halon substitutes, dry chemical, clean agent, foam and carbon dioxide
- Type C - electrical equipment and wires
  - Extinguished using dry chemical, clean agent, water mist and carbon dioxide
- Type D - combustible metals
  - Can be suppressed only with dry powder
- Type K - flammable liquids unique to cooking
  - Extinguished using dry powder