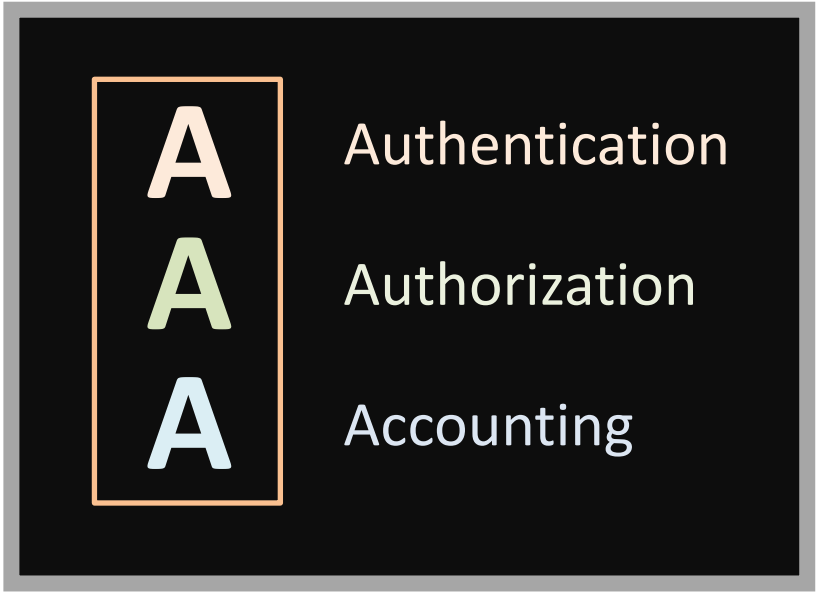
Security+ Session 4

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

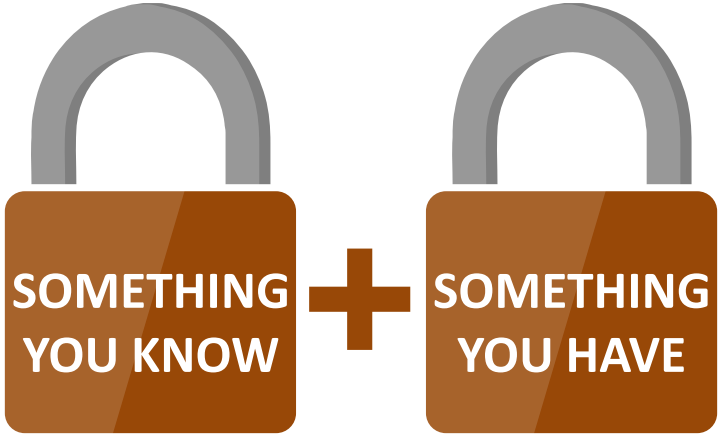
Identity and Access Management (IAM)

- Authentication vs. identification
- AAA Services
  - Authentication
  - Authorization
  - Accounting
- Local or centralized



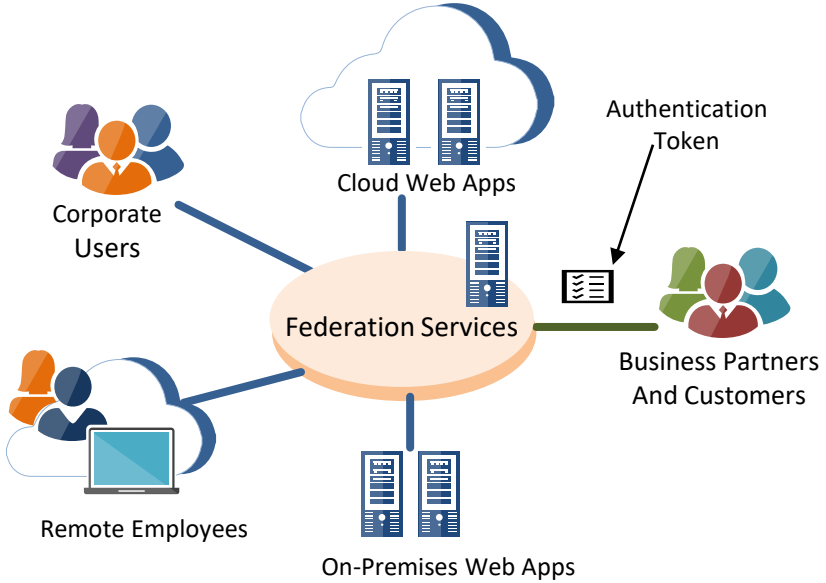
Identity and Access Management (IAM)

- Multi-factor authentication (MFA)
  - Something you know
  - Something you have
  - Something you are
  - Somewhere you are
  - Something you do



Identity and Access Management

- Federation Services
  - Directory Service provide authentication and authorization so that users can cross domains to access resources using a variety of AAA common standards and protocols
  - Maps identities and access attributes between Identity Providers (IdP) and multiple Service Providers (SP)
- Transitive trust
  - Two-way agreement between two entities to allow for resource sharing and secure access
- Single sign-on
  - A characteristic of authentication mechanisms that allow a principal's identity to be granted access across multiple Service Providers after providing credentials once at login

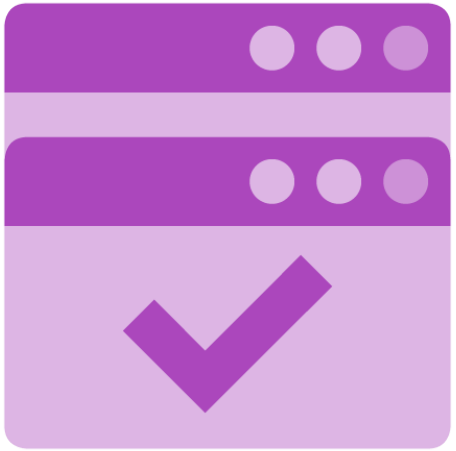


Single Sign-on (SSO)

- SSO is a method of access control of multiple associated, yet independent, systems
- A user logs in with a single ID and password (or other credential factors) and gains access to any of several related systems and services with these benefits:
  - Mitigate risk for access to 3rd-party sites
  - Reduce password fatigue from different credential combinations
  - Avoid having to re-enter passwords for the same identity
  - Reduce IT costs due to lower number of IT help desk calls

Lightweight Directory Access Protocol (LDAP)

- Provides access for management apps and browsers that need interactive read/write access to an X.500 or Active Directory service
- AAA systems can leverage existing user repositories for authentication
- For example, if a company uses LDAP, those systems can offer robust user repositories with sophisticated password management features to the AAA front-end



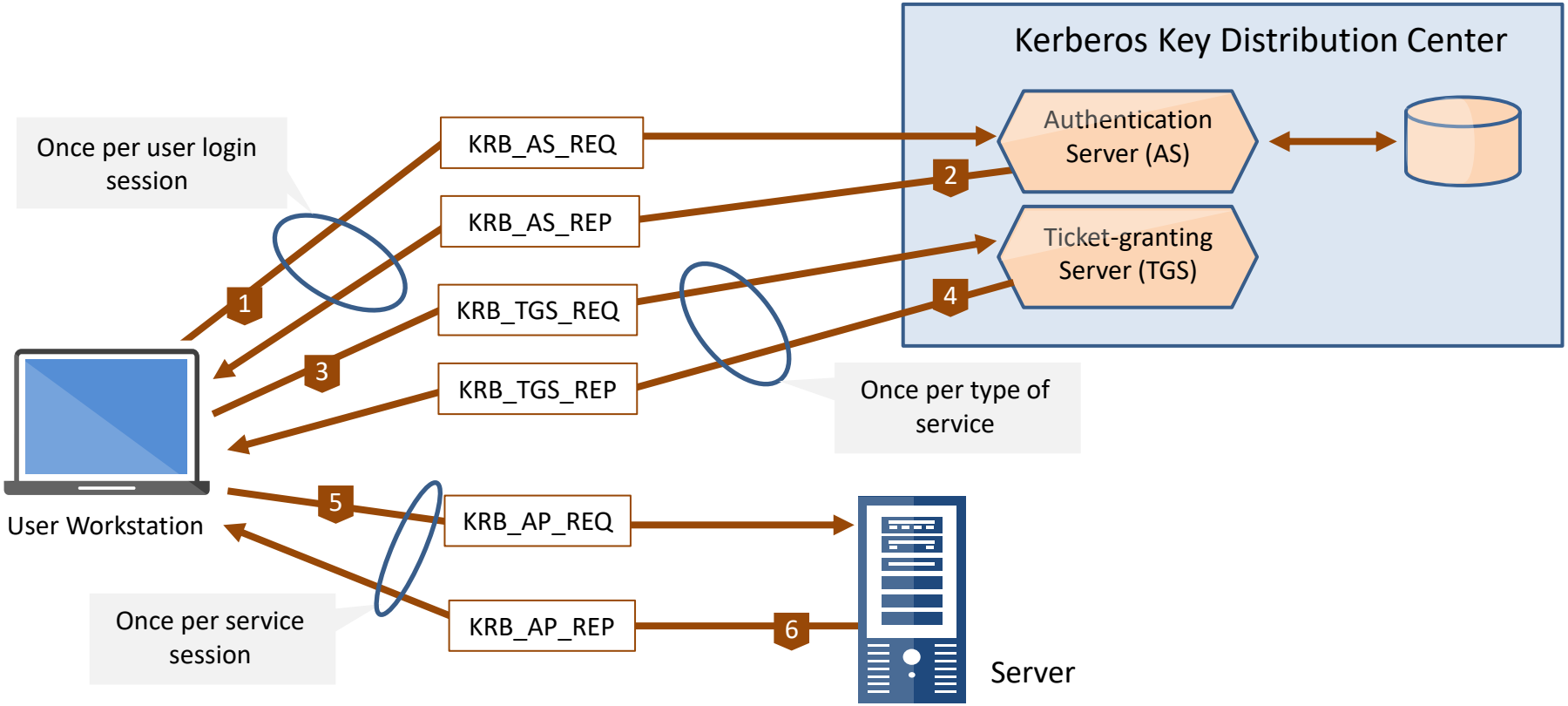
Lightweight Directory Access Protocol (LDAP)

- Many directory services and infrastructure devices use LDAP, or preferably LDAP over SSL (LDAPS)
- It is a simpler iteration of the X.500 parent protocol used for locating information in a directory database
- LDAP typically uses a tree structure, or hierarchy, for data entries and includes
  - A root directory representing the source of the tree
  - Items representing countries
  - Items representing organizations
  - Organizational units
  - Individual entries representing people, files, and shared resources

Kerberos

- Kerberos is a single sign-on (SSO) authentication protocol that uses a secret-key cryptosystem for network-wide authentication
- It performs mutual authentication, where a client proves its identity to a server and a server proves its identity to the client
- After they have proven their identities, they can also encrypt all communications going forward
- To guarantee privacy and data integrity Kerberos depends on a trusted third party called the Key Distribution Center (KDC), which is cognizant of all systems and is trusted by all in the realm

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
Once per type of service
User Workstation
KRB_AP_REQ
KRB_AP_REP
Once per service session
Server
1
2
3
4
5
6

TACACS+

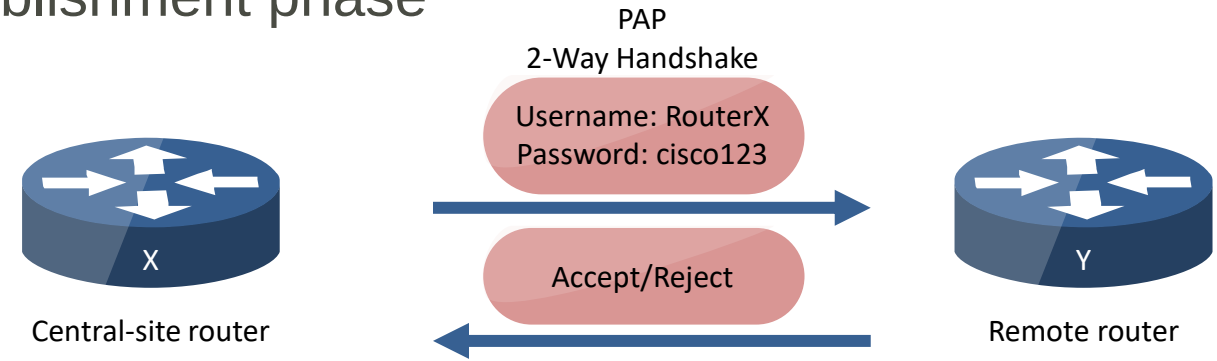
- Terminal Access Controller Access-Control System Plus (TACACS+) was developed by Cisco
- Now a standard client and server protocol for AAA services
- Dynamic authorization is on a per-user or per-group basis
- Offers separate and independent modular authentication, authorization, and accounting abilities
- 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+

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

Password Authentication Protocol (PAP)

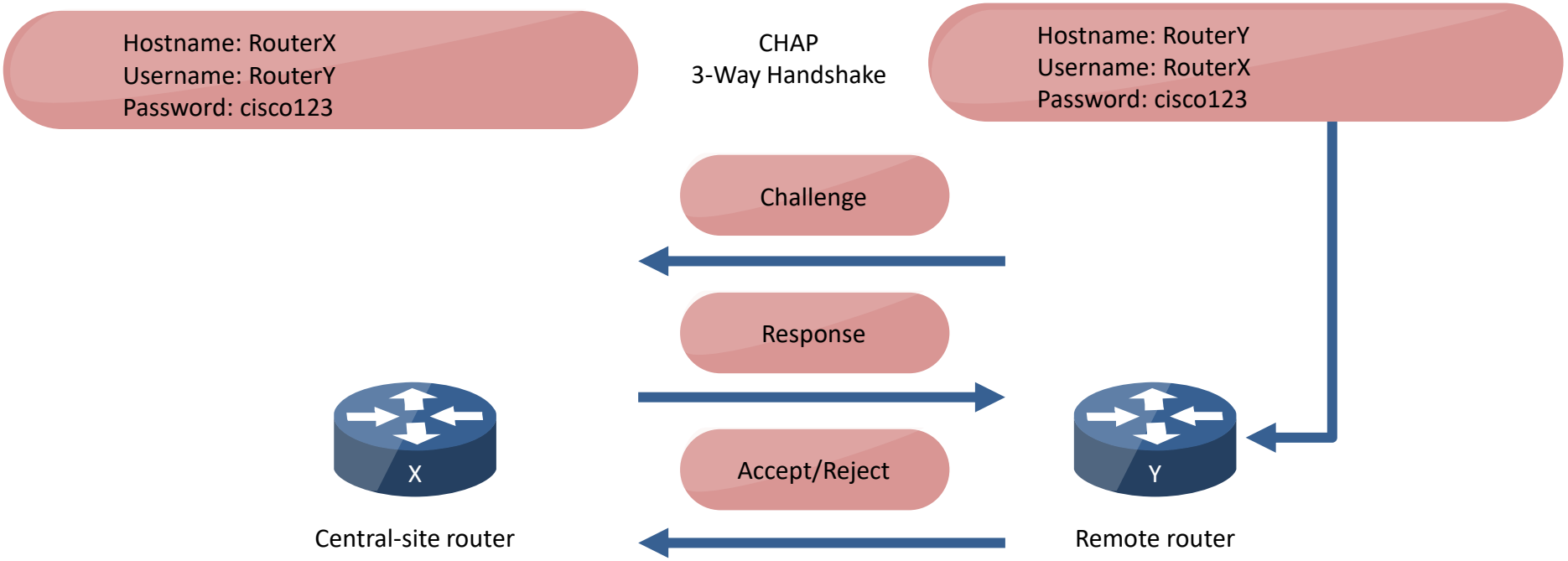
- PAP provides an optional authentication phase before proceeding to the PPP Network Layer protocol phase
- Each end of the PPP link must first send LCP packets to set up the data link during the MAC Link Establishment phase
- By default, authentication is not mandatory
- If authentication is desired, the PAP deployment must require the Authentication-Protocol configuration option during Link Establishment phase



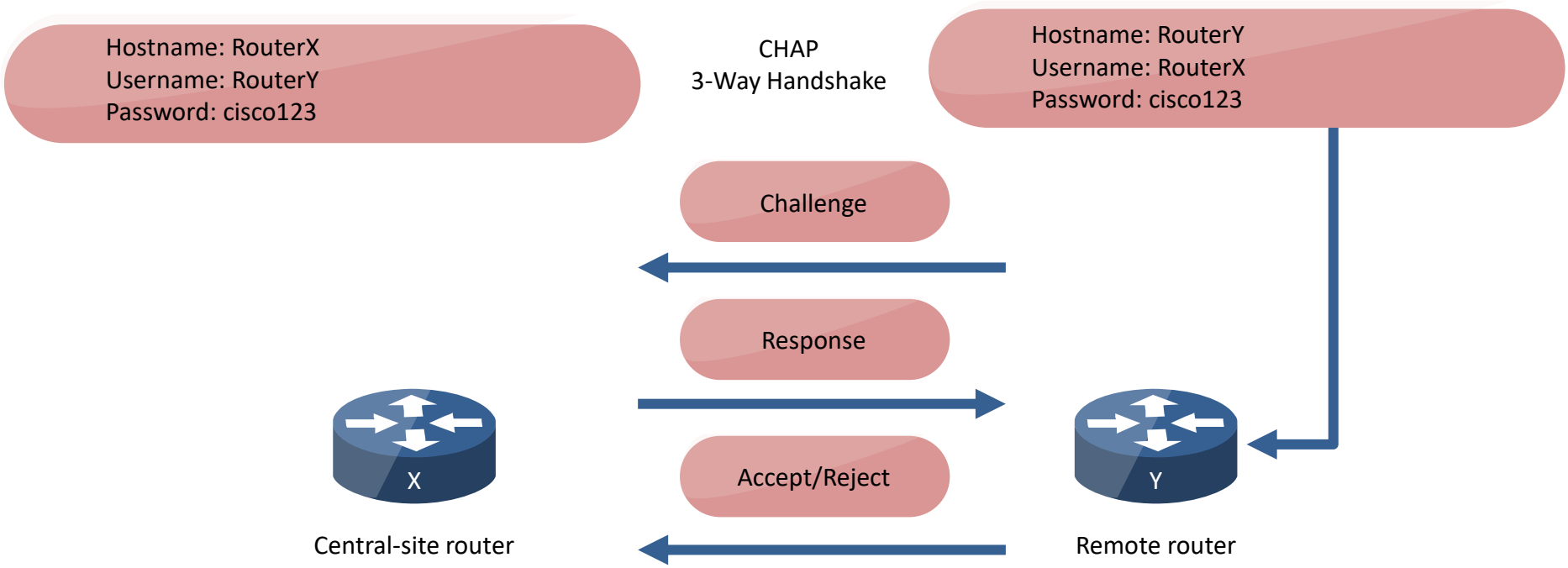
Challenge-Handshake Authentication Protocol (CHAP)

- CHAP is based on earlier PPP authentication
- Challenge/response is a technique that validates the identity of a person (or a process) while keeping the shared secret password a secret between the participating parties
- The CHAP client must prove it knows a shared secret to the server
- Authenticator sends a new challenge at random intervals
- These schemes are often called proof of possession protocols

Challenge-Handshake Authentication Protocol

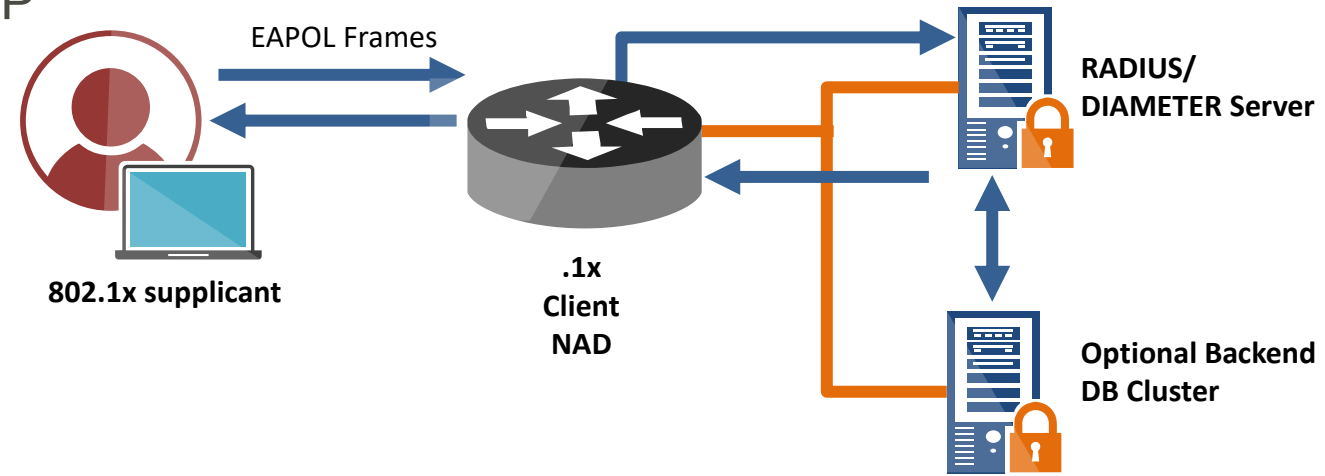


MS-CHAP


Hostname: RouterX
Username: RouterY
Password: cisco123
CHAP
3-Way Handshake
Hostname: RouterY
Username: RouterX
Password: cisco123
Challenge
Response
Accept/Reject
X
Y
Central-site router
Remote router

802.1X and RADIUS Authentication protocols

- An ongoing extension of the original PPP protocols
- Commonly used by AAA and identity services in wired and wireless network environments
  - Extensible Authentication Protocol (EAP)
  - Protected EAP
  - EAP-FAST
  - EAP-TLS
  - EAP-TTLS

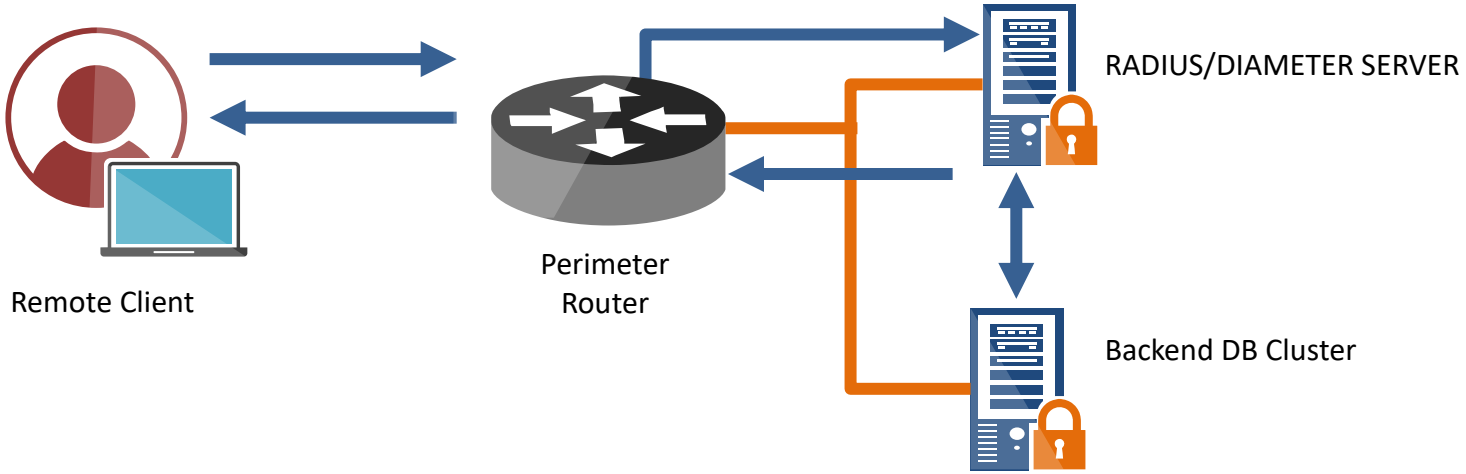


802.1x EAP Comparisons

802.1x EAP Types Feature / Benefit	MD5 --- Message Digest 5	TLS --- Transport Level Security	TTLS --- Tunneled Transport Level Security	PEAP --- Protected Transport Level Security	FAST --- Flexible Authentication via Secure Tunneling
Client side certificate required	no	yes	no	no	no (PAC)
Server side certificate required	no	yes	no	yes	no (PAC)
WEP key management	no	yes	yes	yes	yes
Rogue AP detection	no	no	no	no	yes
Provider	MS	MS	Funk	MS	Cisco
Authentication Attributes	One way	Mutual	Mutual	Mutual	Mutual
Deployment Difficulty	Easy	Difficult (because of client certificate deployment)	Moderate	Moderate	Moderate
Wi-Fi Security	Poor	Very High	High	High	High

RADIUS

- RADIUS (Remote Authentication Dial-In User Service)
- A client-server protocol and software that enables RAS (remote access server) to communicate with a central server to authenticate dial-in users and authorize their access to systems



RADIUS

- Features of RADIUS:
  - Uses a client-server model
  - Transactions use a shared secret between the client and the RADIUS server for authentication
  - Shared secrets are never sent over the network and only the password is encrypted
  - 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

Secure Token

- Secure tokens are also called authentication tokens and assertions
- Microsoft Azure calls these Secure Access Signatures (SAS)
- In Federated services and SSO it is an assertion made about an entity for authentication and authorization purposes
- The tokens are passed between Identity Providers and Service Providers instead of the original credentials
- Assertion has more than authentication credentials
- Can include elaborate authorization attributes

Security Assertion Markup Language (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
- 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)

- There are two components in the SAML scenario:
  - Identity provider and service provider
  - The identity provider declares the identity of the user
  - The service provider takes the assertion and passes the identity data to an application or service

Open Authorization (OAuth)

- OAuth 2.0 is an open authorization framework that allows a third-party application to get limited access to an HTTP service
- Consumer 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 access to their data while protecting account credentials
- Google Docs OAuth has recently been vulnerable to a well-known phishing scam

OpenID Connect

- OpenID Connect 1.0 is a basic identity layer on top of the OAuth 2.0 protocol
- Verify the end-user identity
- Can get basic profile information about the user with an interoperable method
- Supports web-based, mobile, and JavaScript clients
- OpenID Connect is extensible so functionality can be added

Shibboleth

- Shibboleth provides federated identity
- Connects users to both inter/intra-organization applications and services
- The Shibboleth system is free and open source and is popular with universities and public service organizations
- Empowers sites to make well-informed authorization choices for discrete access to protected online resources while maintaining user privacy

NT LAN Manager (NTLM)

- Windows Challenge/Response (NTLM)
- Authentication protocol used on Windows OS networks
- NTLM must be used for logon authentication on stand-alone systems
- NTLM credentials are based on data obtained during the interactive logon process and consist of
  - Domain name
  - Username
  - One-way hash of user password

Mandatory Access Control (MAC)

- MAC is non-discretionary and secures data by assigning sensitivity labels, then compares label to the level of user sensitivity
- Appropriate for extremely secure systems such as multilevel secure military applications
- Main advantage is that access based on "need to know" is strictly adhered to and scope creep is minimized
- Bell-LaPadula model uses mandatory access control (MAC)

Discretionary Access Control (DAC)

- Discretionary access control (DAC) restricts access to data and systems based on the identity of users and/or their group membership
- Access results are usually based on authorization granted to a user based on the various forms of credentials he/she presented at the time of authentication
- In most DAC implementations, the owner of the resource can change its permissions at their discretion
- A DAC framework can deliver the capability for granular access control

Discretionary Access Control (DAC)

- The advantages of using this model:
  - Easy to implement and operate
  - Aligns with the least privilege security principle
  - Object owner has control over granted access

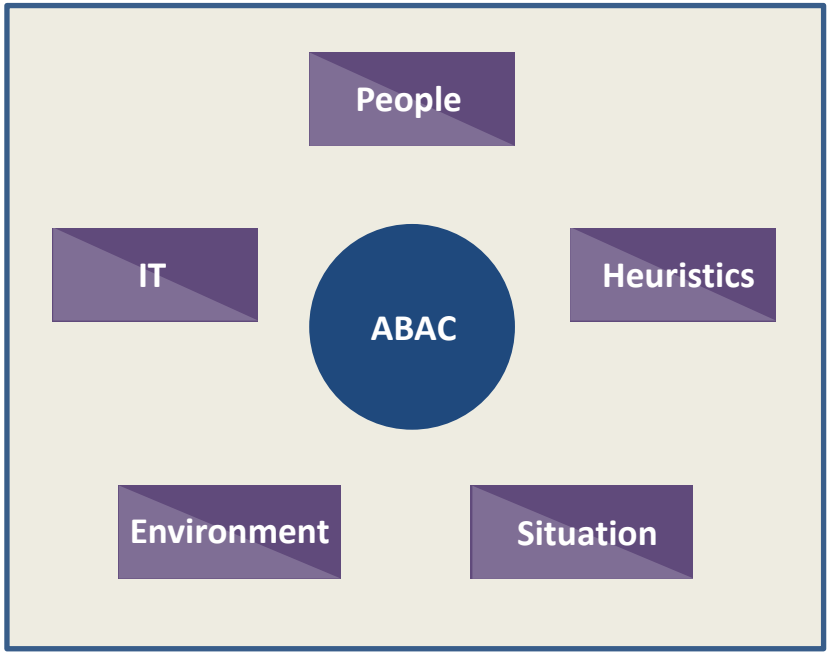
- Issues that can be faced while using DAC:
  - Documentation of the access has to be strictly maintained
  - There is a propensity for scope creep to occur

Attribute-Based Access Control (ABAC)

- Controls access to entities by weighing rules against the attributes of the subject's actions and the request environment
- ABAC relies upon the evaluation of the following:
  - Attributes of the subject
  - Attributes of the object
  - Environment conditions
  - A formal relationship or ACL

Attribute-Based Access Control (ABAC)

- ABAC systems are capable of enforcing both Discretionary Access Control (DAC) and Mandatory Access Control (MAC) models
- Also, Risk-Adaptable Access Control (RAdAC) solutions use risk values expressed as variable factors:
  - People's characteristics
  - Attributes of IT components
  - Heuristics
  - Environmental factors
  - Situational variables



Role-Based Access Control

- Access decisions rely on org chart, roles, responsibilities, or location in a user base
- Role is typically set based on evaluating the essential objectives and architecture of the enterprise
- For example, in a medical center, the different roles of users may include those such as doctor, RN, PA, specialist, technician, attendant, receptionist, etc.
- RBAC framework is determined by security administrators and officers and not at the discretion of the user

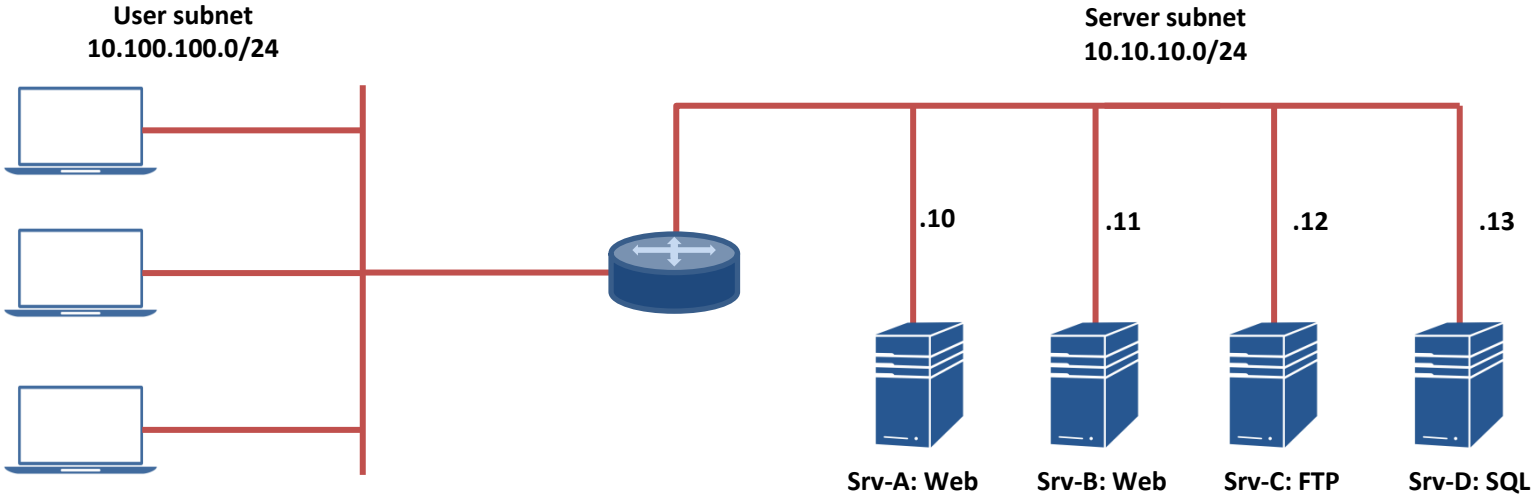
Role-Based Access Control

- Pros:
  - Easy to implement and control
  - Roles are assigned using written security policy
  - Built into many security frameworks
  - Aligns accepted security principles
- Cons:
  - Scope creep can take place over time
  - Roles and access must be audited rigorously
  - Multi-tenancy capabilities need things like AD OUs

Rule-Based Access Control

- Rule-based access control uses the acronyms RBAC or RB-RBAC
- Rule-based access control can dynamically assign roles to users based on criteria defined by the custodian or system administrator
- Example: if a user is only allowed access to a folder from 6 a.m. to 6 p.m. Monday through Friday, then rule-based access control would be implemented using a time-based ACL
- It is common for infrastructure devices like routers, switches, and firewalls to use access control rules (ACLs)

Rule-Based Access Control




```
access-list 100 permit tcp any 10.10.10.10 eq www
access-list 100 permit tcp any 10.10.10.10 eq 443
access-list 100 permit tcp any 10.10.10.11 eq www
access-list 100 permit tcp any 10.10.10.11 eq 443
access-list 100 permit tcp any 10.10.10.12 eq ftp
access-list 100 permit tcp any 10.10.10.12 eq ftp-data
access-list 100 deny ip any any log
```

Fingerprint Scanner

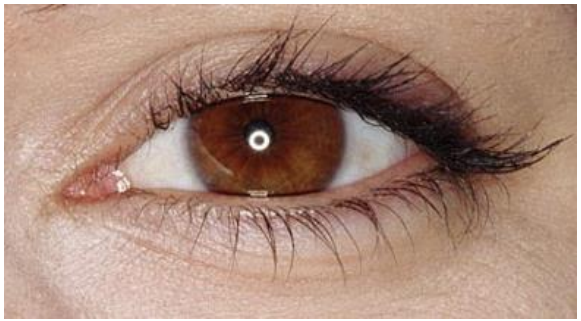
- One of the most common biometrics since they vary from person to person and do not change over time
- Integrated into mobile devices and laptop computers using hardware and/or software
- A fingerprint scanner system has two functions:
  - Get an image of the finger
  - Determines whether the outline of ridges and valleys in the image matches the patterns in pre-scanned images

Retinal Scanner

- Referred to as "ocular-based" identity technologies
- The retina is a thin tissue composed of neural cells located in the back portion of the eye
- Due to the complex make-up of the capillaries, every person’s retina is distinctive
- Scanner sends a beam of low-energy infrared light into an eye when user looks through the scanner’s eyepiece
- Beam of light traces a standardized path on the retina and the pattern of variations are converted to code and stored in a database

Iris Scanner

- The iris is the thin, circular structure "color" part of the eye and controls the diameter and size of the pupils and therefore the amount of light reaching the retina
- Muscles attached to the iris expand or contract the pupil so the larger the pupil the more light can enter
- Unlike retina scanning, iris scanners use camera technology to get images of the intricate and detailed structures of the iris using delicate infrared illumination



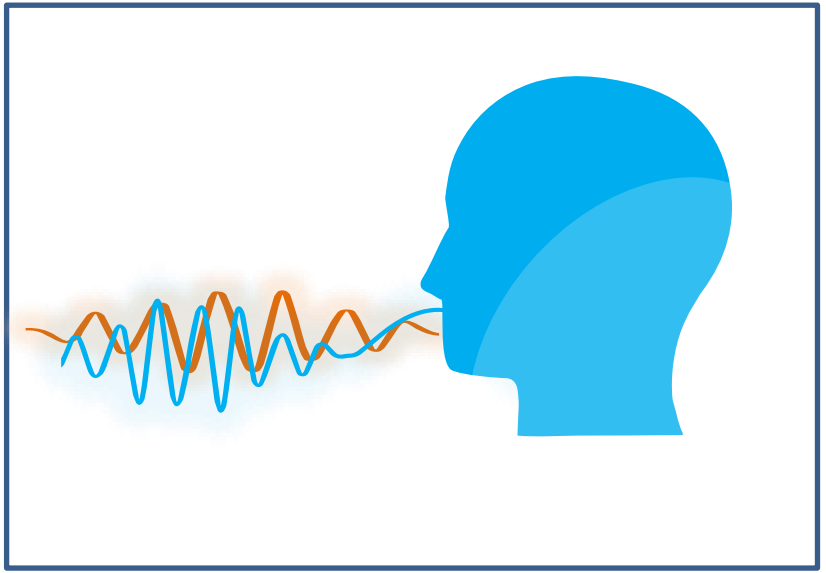
Retinal vs. Iris Scanning

- Similarities:
  - Low rate of false positives and extremely low rate of false negatives
  - Reliability is due to the fact that no two people have the same eye patterns
  - Identity of the subject can rapidly be confirmed
  - Capillaries decompose too fast to use a removed eye for access

- Differences:
  - Retinal scan accuracy can be affected by disease whereas the fine surface of the iris stays constant
  - Retinal scanning is categorized as invasive since the eye must be very close to the eyepiece
  - Iris scans are non-invasive and can be performed at a distance
  - Iris scans are more widely accepted as a commercial modality

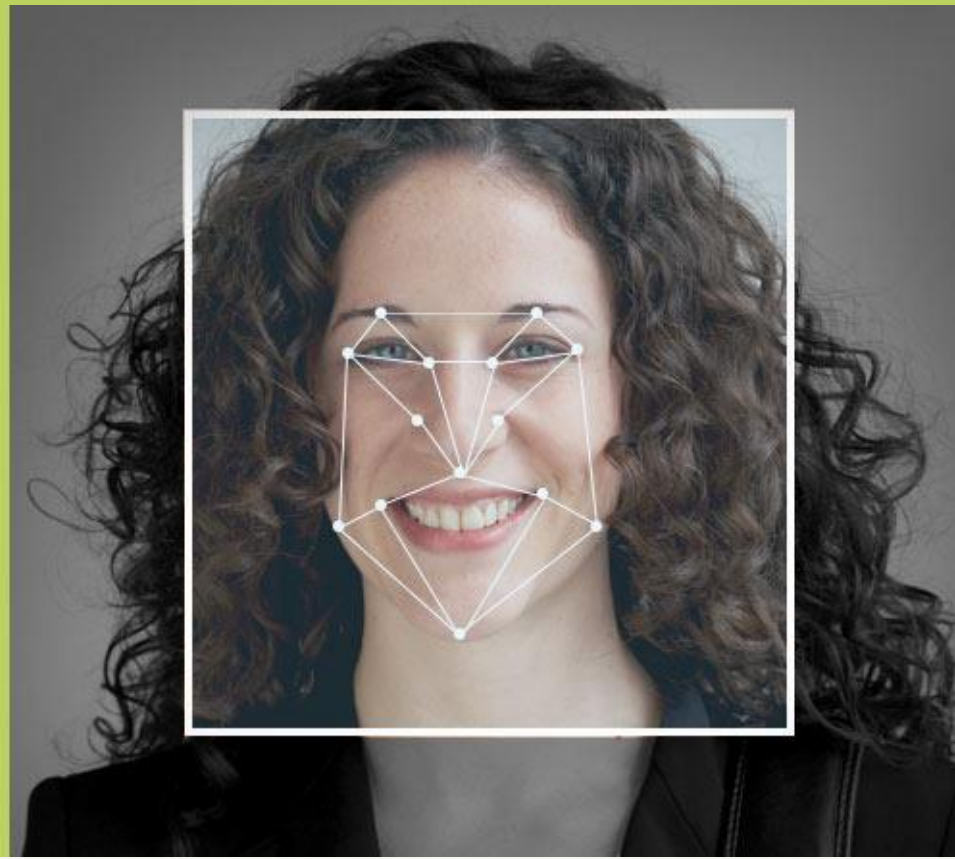
Voice Recognition

- There is a difference between speaker recognition and speech recognition
- "Voice recognition" can be used for both terms
- Speaker recognition leverages the aural aspects of speech that diverge among people
- Traits include human physical structure learned social communication patterns
- Voice recognition is classified as a "behavioral biometric"



Facial Recognition

- One of the fastest growing mechanisms
- Commonly used to identify or verify an individual in still or video images
- The main applications of face recognition are in areas of security biometrics and human-to-computer interaction (including robotics)
- Main method for modeling facial images is PCA



False Acceptance Rate and False Rejection Rate

- **FAR** – measures the probability that the biometric system will incorrectly accept an access effort by an unauthorized user
  - A system's FAR is often specified as the ratio of the number of false acceptances divided by the amount of authentication attempts
- **FRR** – measures the probability that the biometric system will erroneously reject an access attempt by an authorized user
  - A system’s FRR is usually stated as the ratio of the number of false recognitions divided by the amount of authentication attempts
- **CER** – crossover error rate is the value of FAR and FRR when the sensitivity is setup so that FAR and FRR are the same
  - An excellent metric for quantitative comparison of differing biometrics

Security Controls

- Any mechanism that protects business assets
  - Administrative
    - Defines policies, procedures, and guidelines
      - Password policy, hiring policy, screening policy, mandatory vacations, training
  - Technical
    - Controls access to a resource
      - Firewalls, encryption, passwords, IDS/IPS, smartcards, biometrics, RADIUS
  - Physical
    - Controls access to facility
      - Locks, guards, fences, video cameras, gates, bollards

Security Controls

Administrative	Technical	Physical
Effective hiring practices	Controlled user interfaces	Guards
Effective termination practices	Password, tokens, OTPs	Fences
Classification of data based on levels of sensitivity	Firewalls	Motion detectors
Supervision of employees	Routers that filter traffic	Locks
Tracking employee activity	Anti-virus software	Cable conduits
Separation of duties	Access control lists	Swipe cards
Rotation of duties	Intrusion detection/prevention systems	Badges
	Smart cards	Dogs
	Biometrics	Cameras
		Alarms

Note: Some controls fit into multiple categories based on the context

Security Controls

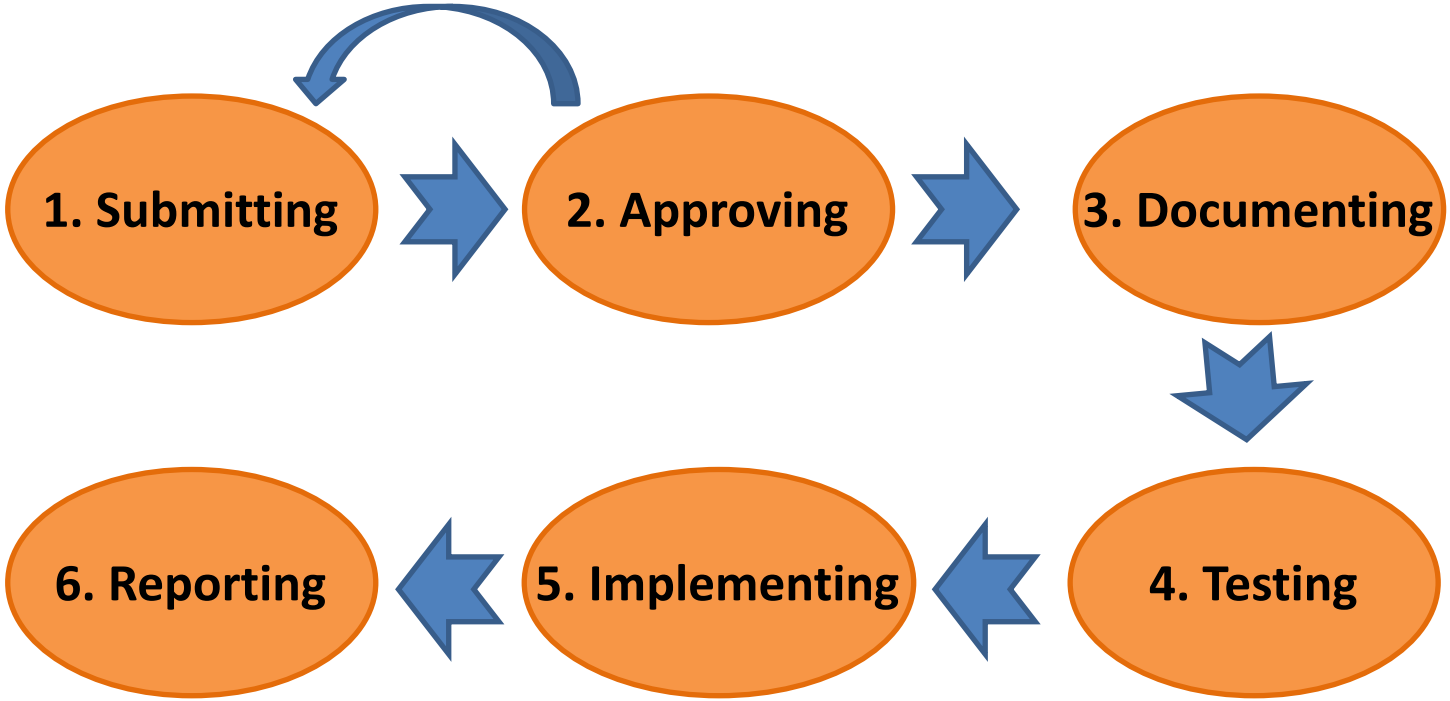
- Deterrent
  - Discourages you from performing attack
- Preventive
  - Stops you from performing attack
- Detective
  - Identifies an attack that is happening
- Corrective
  - Restores a system to state before attack
- Compensating
  - Aids controls that are already in place

Security Controls

	Preventive	Detective	Corrective	Deterrent	Recovery
Physical					
Fence					
Lock					
Motion Detector					
Administrative					
Separation of Duties					
Job Rotation					
Technical					
ACLs					
IDS					
Data Backup					

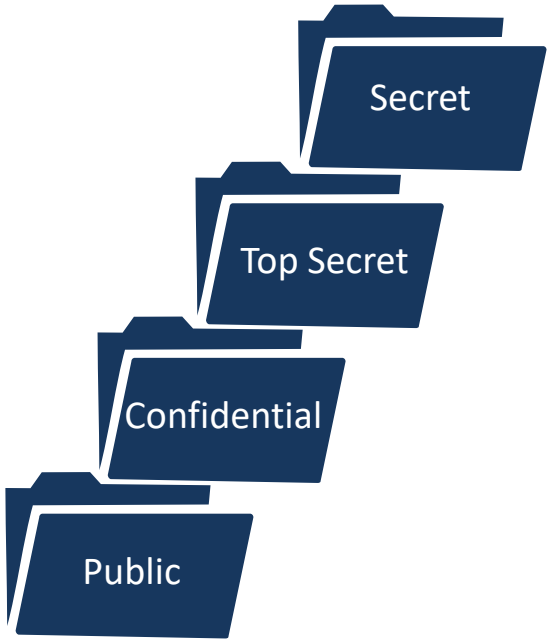
Change Management

- Defined procedures for implementing change



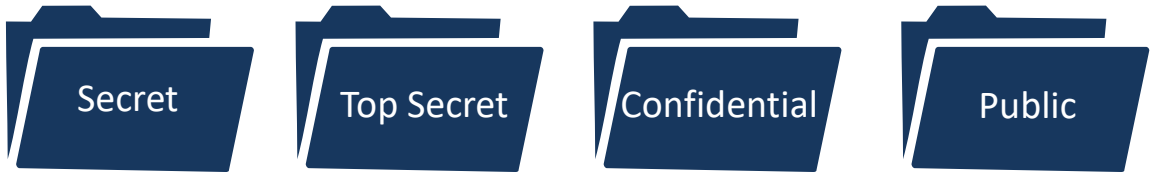
Labeling and Handling

- Labeling
  - Also called “sensitivity levels”
  - Can involve physical and logical tagging
  - Classification of information
    - Used to determine level of protection
      - Determines how it should be handled
- Handling
  - Controls who has access to information
  - Based on labeling
    - How it has been classified



Data and System Classification

- Military classification scheme
  - Top secret
  - Secret
  - Secret But Unclassified (SBU)
  - Confidential
  - Unclassified
- Commercial classification
  - Corporate confidential
  - Personal confidential
  - Trade secret/proprietary
  - Private
  - Public



Data Sensitivity

- PII – Personally identifiable information
  - Individual identifiable information
    - Consists of first name or initial with last name and one or more pieces of info
      - SSN, Driver's License Number, ID Card, Financial Account Number, Medical/Health

- PHI – Protected health information
  - Individual identifiable health information
    - Contains at least one piece of info
      - Name, Address, Birth Date, Phone Number, Mail or Email Address, SSN, URLs, IPs

Data Roles

- Owner
  - Owner of the information
  - Determines classification level
- Steward
  - Manager of the data and metadata
  - Ensures compliance (standards/controls) and data quality
- Custodian
  - Keeper of the information
  - Ensures C.I.A. is maintained
- Chief privacy officer
  - Ensures privacy of all data in the entire organization

Data Retention

- Keeping data until it is no longer needed
  - What does "no longer needed" mean?
- Data retention policy
  - Identifies how, where, and why data will be retained for the following:
    - Operational use
      - Current and future use
    - Adherence to
      - Legal and regulatory requirements and compliance
    - Periodic audits

Destruction and Sanitization

- Destruction
  - Burning
  - Shredding
  - Pulverizing
  - Pulping
- Sanitization
  - Degaussing – removing the magnetic field of drive
  - Purging – clearing everything off the media
  - Wiping – overwrite every sector of drive with 1s and 0s
  - Encryption – encrypt all files before deleting or disposal of media

File System Security

- Good planning before bringing systems online is critical
- Must understand the file and directory permissions and ownership model of your system (Unix, Linux, Windows, Mac, etc.)
- Centralized file security, change and configuration management is a must for SMB to large enterprise
- Least privilege principle should be in place
- Remember system and other special accounts

Database Security

- Database security should offer authorized and safe access for users and administrators while preserving the integrity of the data
- Three key areas of consideration:
  - Shielding data from unauthorized access
  - Averting unauthorized disclosure
  - Recovering from software or hardware problems

Database Security

- Also involved with database security:
  - Zero Trust
  - Access controls
  - Application access (Views Only)
  - Vulnerability management
  - Continuous monitoring and auditing
  - Backup and recovery

Database Security

- Database threats:
  - Excessive and unused privileges
  - Privilege abuse
  - SQL injection
  - Malware
  - Denial of service
  - Storage media exposure
  - Poor auditing

User Accounts

- Must be unique per person and not shared
- Often use DAC security model
- Admins should have a separate non-privileged account for normal daily activities
- Best when they are centrally managed
- Least privilege security principles
- MFA is preferable to simple password credentials
- Employ lockout for 3-5 failed attempts
- SSO should be an enterprise goal

Shared, Guest, and Generic Accounts

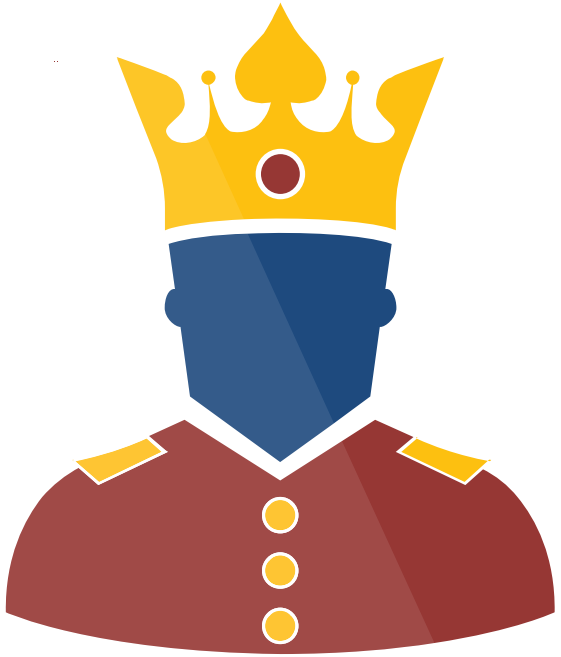
- Four main types of shared accounts:
  - Anonymous or guest accounts
  - Temporary employee accounts
  - Shared administrative accounts
  - Accounts used for running scripts or batch processing

Privileged Accounts

- Privileged accounts get elevated access to systems with special credentials
- Typically give non-restricted or at least elevated access to the system, service, or applications
- Designed for systems administrators to deploy and manage IT infrastructure devices, operating systems, databases, applications, and more
- They are the "keys to the kingdom" and the prime target of malicious external attackers and insiders

Privileged Accounts

- Most common privileged accounts:
  - Root user
  - Local administrative accounts
  - Privileged user accounts (exec user)
  - Forest and domain administrative accounts
  - Emergency accounts
  - Application accounts



Service Accounts

- Service accounts can be privileged local or domain accounts used by an application or service to function with the network operating system
- Some service accounts have domain administrative privileges contingent on the application needs such as corporate mail or database services
- Local service accounts can operate with several different system components, which renders coordinating of password changes challenging
- Service account passwords are rarely changed and this can become a significant vulnerability for an enterprise

Least Privilege Principle

- Applies a need-to-know scheme to trust relationships between users and security domains
- Policy originated in military and intelligence operations
- When fewer people know about certain systems and data the risk of unauthorized access is reduced
- This should lead to restrictive policies in network security
- Weakest link is related and means that a security system is only as effective as its weakest link
- Human access policies are often considered to be the weakest link in information security architectures

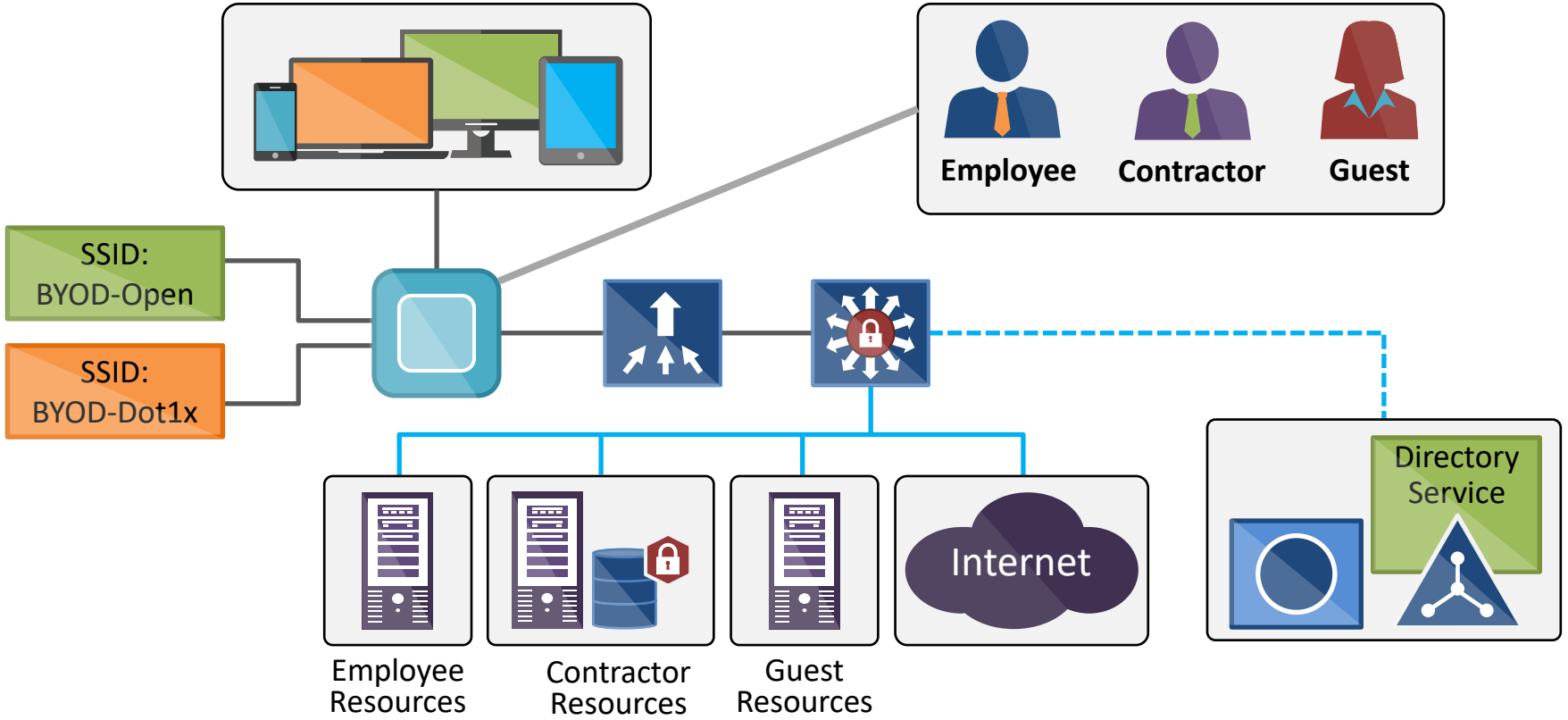
Time-of-Day Restrictions

- Time-of-day restrictions should control access after working hours, weekends, holidays and during special events
- Restrictions can also be object-oriented as opposed to subject-oriented
- Time-based ACLs and other enterprise IAM solutions (Cisco ISE)

Onboarding and Offboarding

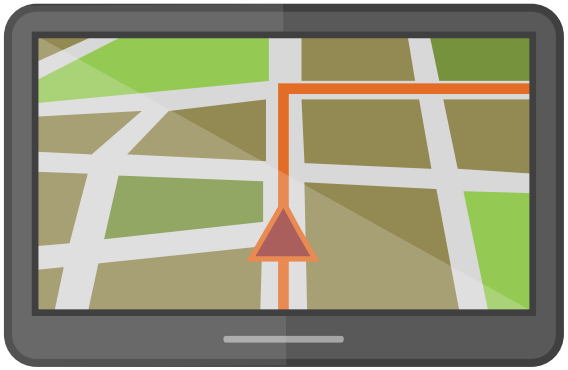
- Enterprises deploy systems that involve self-service onboarding of personal devices
- Employee registers a new device, and the native supplicant is automatically provisioned for that user and device and installed using a supplicant profile that is preconfigured to connect the device to the corporate network
- Offboarding is the reverse process performed in adherence to corporate policies

Onboarding and Offboarding



Location-Based Policies

- Location-based policies are part of context-based identity service methodologies
  - Wired, wireless, or VPN
  - Geographical location
  - Device profile and posture
  - Date and timestamp
  - Role-based authorization
- Involves dynamic Change of Authorization (CoA)
- Capabilities also include device tracking tools (RFID, NFC, GPS, etc.)



Recertification

- The process of issuing new certificates to end users and systems that have expired digital certificates
- Can also involve recertification of software and code that is digitally signed
- Any system that goes through a certification process must have a secure scheme for recertification that cannot be compromised by a rogue actor or a MITM attack

Account Maintenance

- Operating system account maintenance must be secured as part of a configuration management and change management initiative
- Handled through the service desk and enterprise/domain administrators
- Password changes and password history should be centrally enforced on a rotating 45 to 60-day basis

Auditing and Review

- In order to achieve continual improvement (CI) all users, especially root and administrative users, should be regularly audited and reviewed
- Can be internal or external, manual or automated
- Logs can be data mined using cloud services
- AUPs must be enforced
- Regular reports and summaries delivered to the proper member of the "C-Team" (CISO, CSO, CIO, etc.)

Credential Management and Naming Conventions

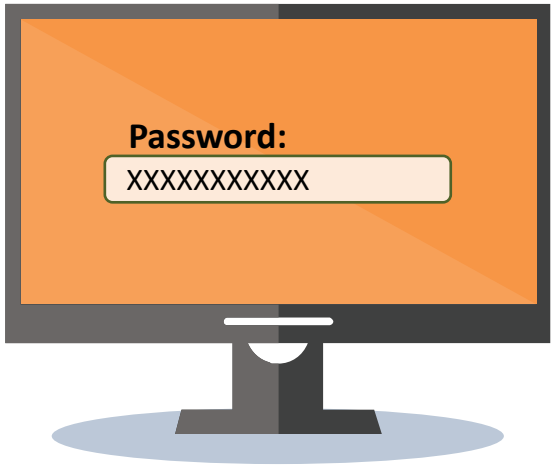
- Credentials are used for simple tasks all the way to retrieving/writing the most valuable data in an organization
- Some may be used hundreds of times a second while others only once a year
- The diversity of security models and policies makes credential management particularly challenging
- This should tie into a universal naming convention across all of your enterprise systems, services, and applications

Group-Based Access Control and Group Policy

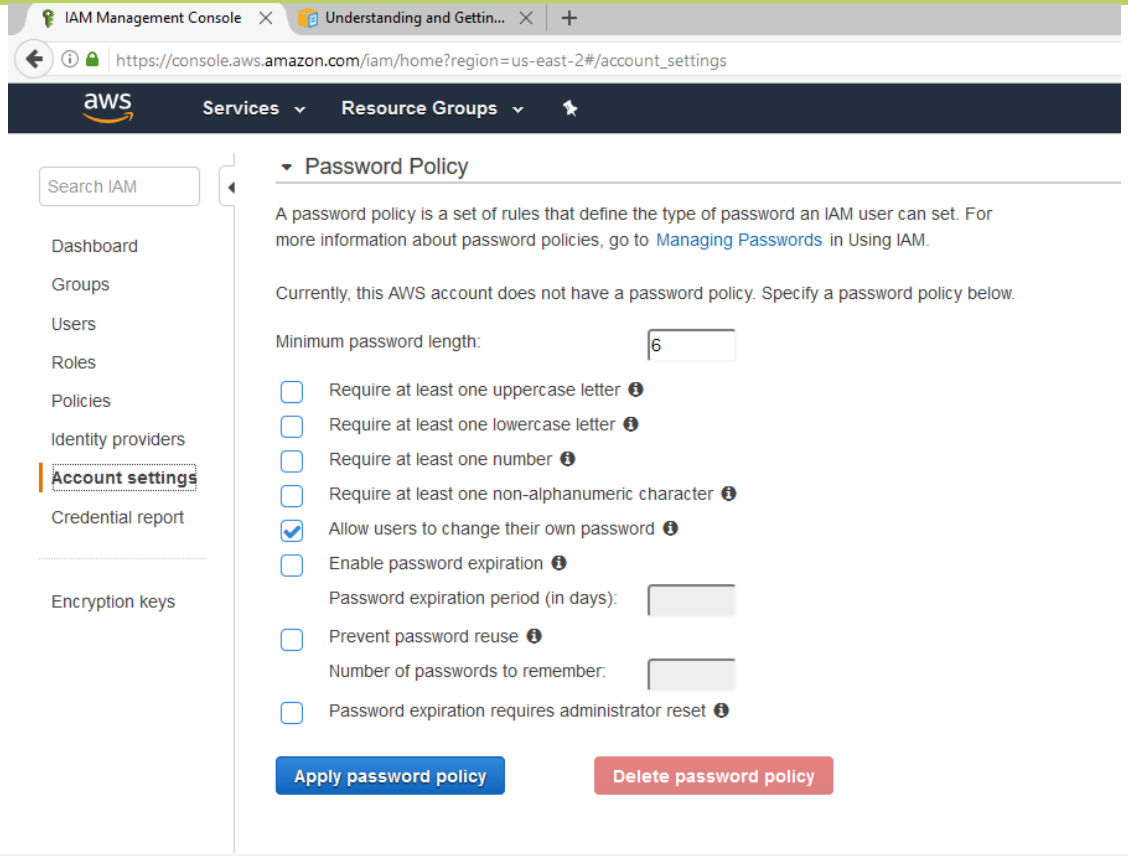
- Group-based access makes access controls and permissions easier to deploy for users with similar authorization requirements
- Cloud-based solutions (like Azure) are becoming popular due to complexity of applications and mobility
- Cloud identity management will eventually replace the group-based and enterprise group policy approach

Password Best Practices

- Deprecate password usage if and when possible
- Start using different factors for MFA policies
- Use password managers like Dashlane and LastPass, which install as browser plug-ins
- Identify all weak and duplicate passwords
- Use password generators that sync across all devices
- Remember: longer is stronger



Password Policies



Security Awareness Training

- Provide company wide security awarenes training
  - Should happen early and often
    - CBT and streaming webinars
    - E-mail bulletins
    - Classroom style
      - Physical
      - Virtual
    - Self-enabled interactive websites
    - Posters, coffee mugs, mouse pads

Security Awareness Training

- What do we want to talk about?
  - Organizations policies and procedures
    - Physical security
    - Desktop security
      - Computer
      - Physical
    - Password security
    - Phishing/hoaxes
    - Malware
    - Copyrights

Security Awareness Training

- Role-based awareness training
  - Users
  - Data/system owners
  - Data/system custodians and stewards
  - System administrators
  - Privileged users
  - Executive users
    - Executive management
    - C-suite or C-team
    - Board of Directors

Acceptable Use Policy (AUP)

- Identifies how employees are expected to use resources in the organization
  - Computer equipment
  - Software
  - Operating systems
  - Removable Storage media
  - Email
  - Web browsing
  - FTP/file-sharing
  - Remote Access
  - Mobile devices
  - Telephones
  - Wireless
  - Social media

Acceptable Use Policy

- Rules of behaviour/code of conduct
  - Language
  - Avoid illegal activities
  - Avoid disturbing or disrupting other systems
  - Do not reveal personal information
  - Do not reveal confidential information

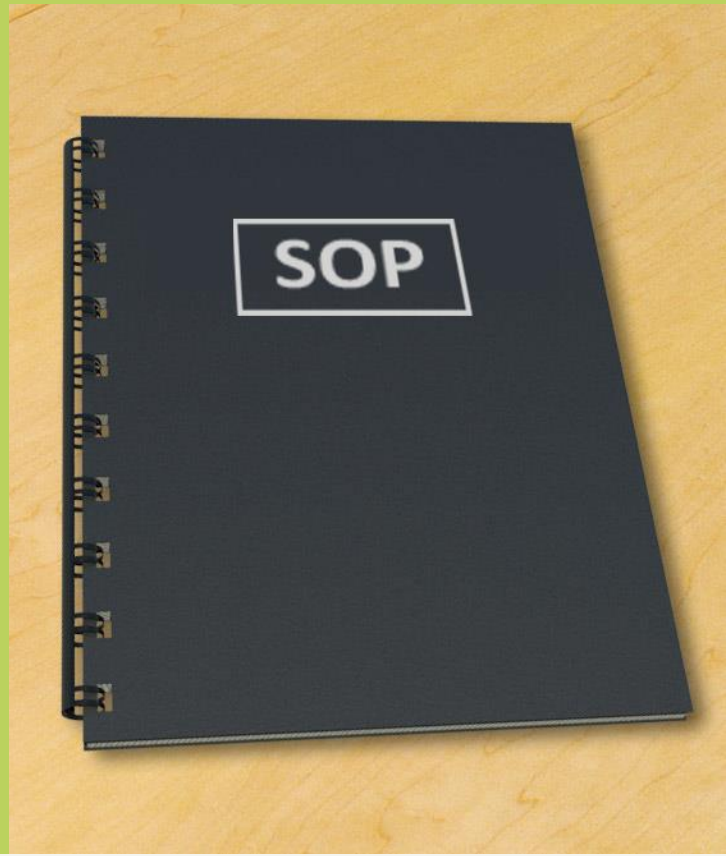
Acceptable Use Policy

- Consequences of violating AUP
  - Adverse actions
    - Written
    - Verbal
    - Suspension
    - Termination
    - Reimbursement

- Protects the confidentiality and integrity of the organization

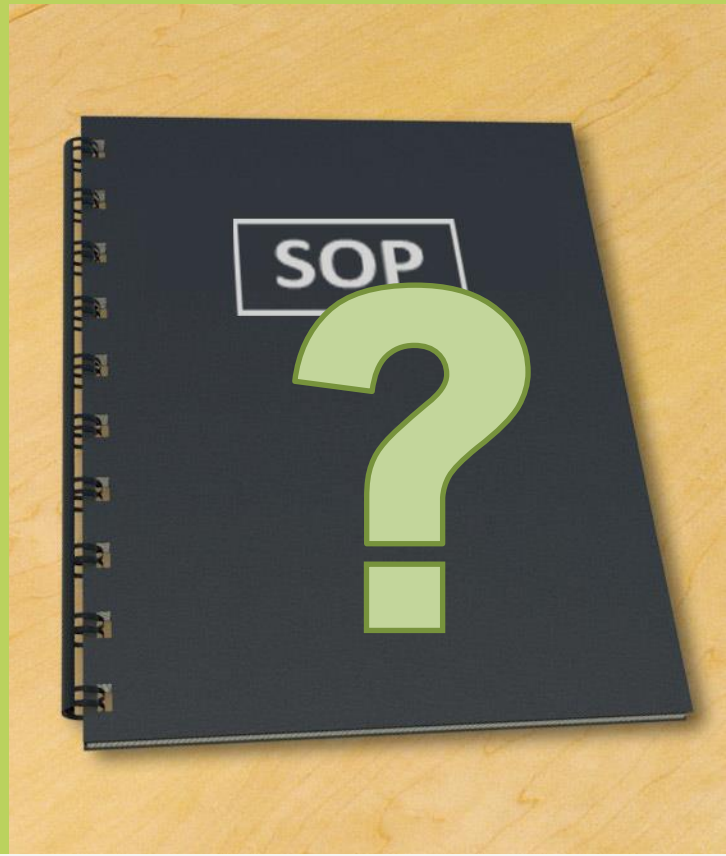
Standard Operating Procedure (SOP)

- Step-by-step instructions
  - Define how workers carry out routine operations/tasks
  - Improves
    - Efficiency
    - Quality
    - Performance
    - Communication
    - Compliance with regulations



SOP Coverage

- Define the purpose of the process, its limits, how its used
- Provide all the steps needed for the process
- Provide clarification for terms
- Provide health and safety warnings
- Provide a listing of all equipment and software and where it is
- Provide a "what if" section



Agreements

- BPA – business partners agreement
  - Agreement between partners for business purposes
    - Purpose of business
    - Contributions of each partner
    - Rights/responsibilities of each partner
- SLA – service level agreement
  - Official commitment between a provider and customer
    - Defines quality, availability, and responsibilities
- OLA is the internal version of SLA

Agreements

- ISA – interconnection security agreement
  - Document and formalize
    - the connections between two organizations
    - Security and safeguards for the connections
- MOU/A – memorandum of understanding/agreement
  - Defines responsibilities of each organization for the connection
    - Establishing, operating, and securing

NDA (non-disclosure agreement)

- Legal contract between two or more parties
  - Confidential relationship
    - Business and business/business and employee
- Identifies confidential information they wish to share with each other
  - IP, trade secrets, new idea, new process, and new product
    - Restricts the sharing of that information with others

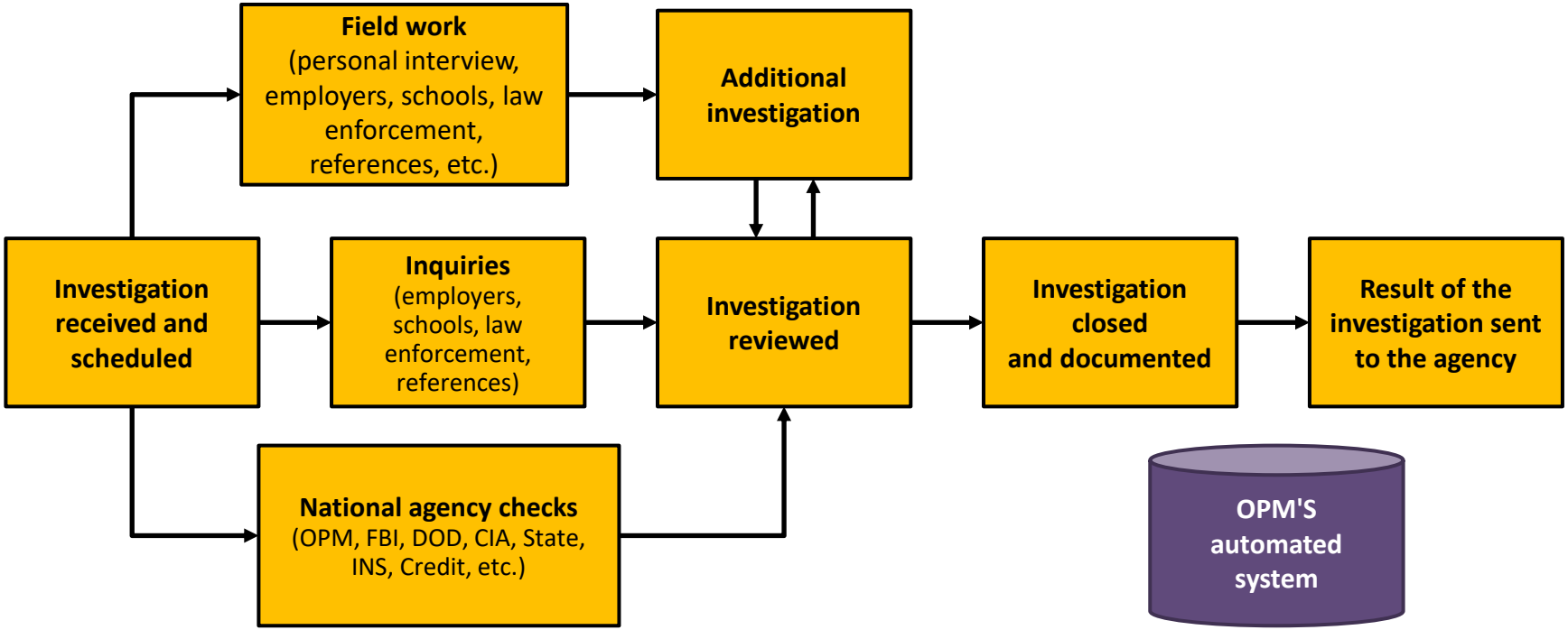
Administrative Job Controls

- Mandatory Vacations
- Separation of Duties
- Rotation of Duties
- Clean desk policy
- Background checks
- Exit interviews

Onboarding

- The process used to ramp up new or existing employees
  - Provide knowledge, skills, behaviour needed for role on team
    - Videos, printed material, CBT, lectures, formal and informal meetings, and mentors
- Security
  - Reduces ambiguity and uncertainty
    - Clearly defined roles and responsibilities
      - » Less chance of security breaches

OPM Investigations and Background Checks

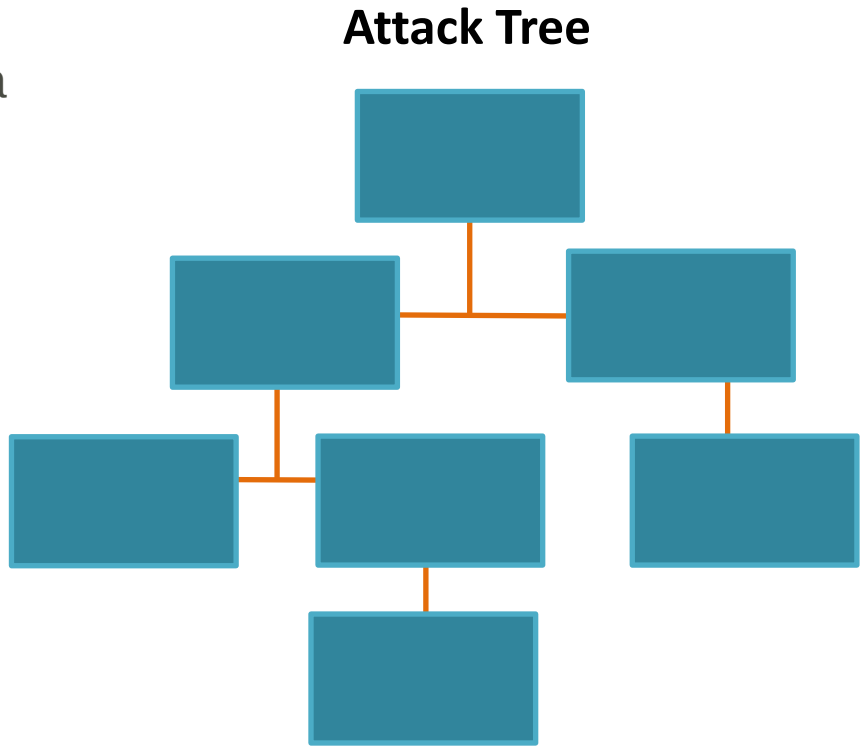


Exit interviews

- Identify factors that have led to employee leaving
  - How can the organization improve to keep employees?
- Security
  - Remind them of their agreements and responsibilities
  - Review the NDA that they signed when they started
  - Remind them they are forbidden to discuss with others
    - Security policies
    - Security mechanisms
    - Confidential data

Key Risk Assessment Definitions

- Vulnerabilities
  - Any tiny flaw that can be exposed by a threat
- Threats
  - Anything that could expose the vulnerability
- Attacks
  - The act of exposing the vulnerability using the threat
- Threat Agents (Actors)
  - The delivery mechanism

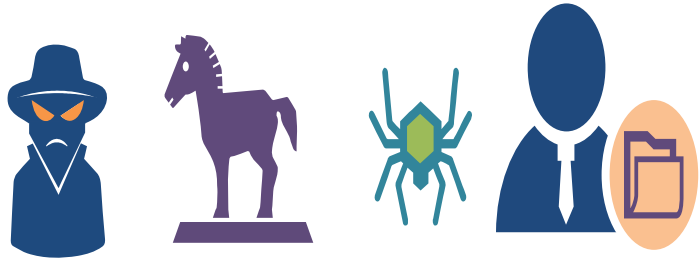


Risks

Environmental	Man-made Intentional	Man-made Unintentional
• Earthquakes • Wildfires • Flooding • Snow • Tsunamis • Hurricane • Tornado • Landslide • Asteroid	• Arson • Terrorist • Political • Break-Ins • Theft • Damage • File destruction • Information disclosure	• Mistakes • Power outage • Illness • Epidemics • Information disclosure • Damage • File destruction • Coding errors

Threat Assessment

- Assets must be valuated, categorized, labeled, and documented before threats are assessed
- The organization should also determine how risk we be handles on an asset/asset class basis
- This information should go into a Risk Register or Ledger (Log)
- Assessments of likely threats:
  - Environmental
  - Manmade
  - Internal vs. external
  - Structured vs. unstructured



Risk Assessment

- What are your assets at risk?
  - Inventory and categorization
    - Both tangible and intangible
    - Value
- Identify risks to those assets
  - Vulnerability, threats, attacks
  - Who, Why, and How
- Only focus on risks that are likely to occur
  - Maximizes available resources
  - Focus on most likely to least likely

Risk Register

- Risk Register (also called ledger or log)
  - Scatter plot/Table
  - Fulfills regulatory compliance
    - Repository of identified risks, impact, scenarios, and potential responses

Identified Risks	Root Causes	Probability And Impact	Ranking	Categories	Priorities	Time and Cost Objectives	Potential Responses	Risk Owners	Assumptions

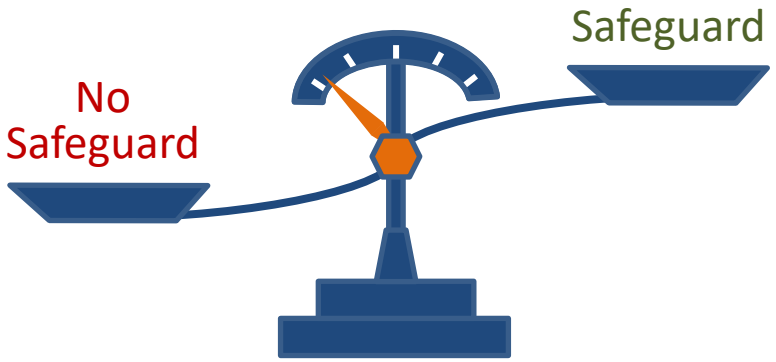
Intelligence Gathering

- Strategic intelligence
  - Obtaining, processing, reviewing, and distributing information
  - Plan the future direction and growth of a business/country based on trends, patterns, competitors, and predictable problems
  - Big Data analytics

- Strategic counterintelligence
  - Obtaining, processing, reviewing, and distributing information
  - Protect the future direction and growth of a business/country based on sabotage, espionage, threats, and terrorism (physical and economical)

Defining Risk

- Inherent (total) Risk
  - Risk the organization faces if safeguard is not implemented
- Residual Risk
  - Risk that remains once safeguard is in place
  - Residual = inherent risk – safeguards (controls)



Risk Response (treatment/handling/appetite)

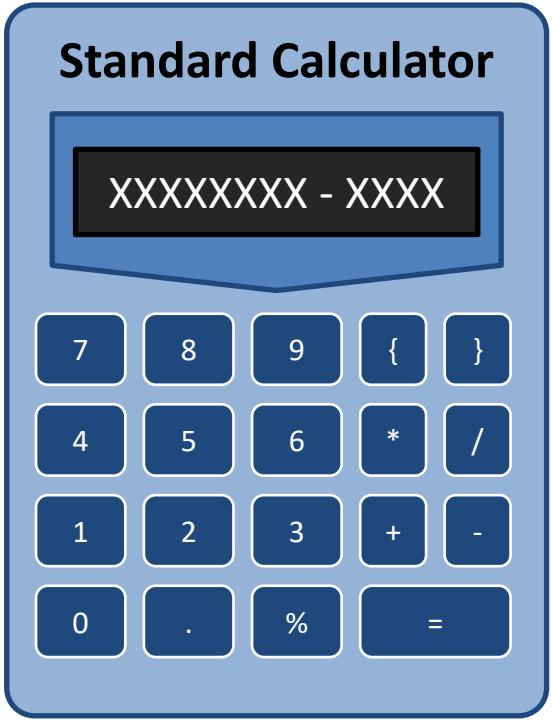
- Risk Acceptance
  - Do not implement any safeguards
    - Justification in writing is often required
- Risk Mitigation
  - Implement safeguards that will eliminate or reduce risk exposure - risk may exist but impact is reduced
- Risk Transfer/sharing
  - Pass the risk to a third-party such as insurance company or a cloud service provider
- Risk Avoidance
  - Choose not to undertake actions that introduce risk

Qualitative Risk Analysis

- Descriptive approach
  - Uses opinions, history, and scenarios to determine risk levels
  - Based on subjective risk levels and labels
- Often involves interviewing people:
  - Assets
  - Risks
  - Vulnerabilities
  - Threats
  - Impact

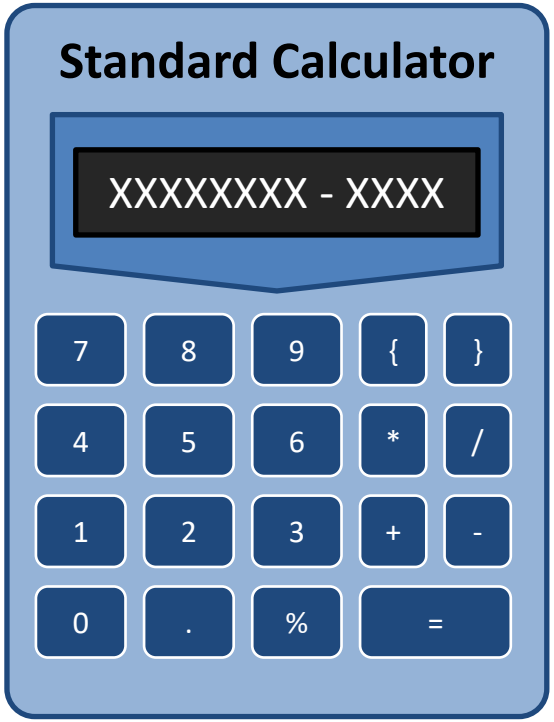
Quantitative Risk Analysis

- Scientific/Mathematical approach to get monetary and numeric results
  - Asset Values
  - Impact and magnitude
    - Severity of incident
  - Probability and likelihood of occurrence
    - Threat Frequency
  - Costs and effectiveness of safeguards
  - Probabilities based on percentages and calibrated estimation



Classic Quantitative Analysis

- AV (Asset Value)
  - Value of the asset according to the organization
- EF (Exposure Factor)
  - Percentage of asset loss caused by identified threat
- SLE (Single Loss Expectancy)
  - Potential loss if attack occurs
  - (Asset value * Exposure Factor)
- ARO (Annualized Rate of Occurrence)
  - Estimated frequency the threat will occur within a single year
- ALE (Annualized Loss Expectancy)
  - (SLE * ARO)

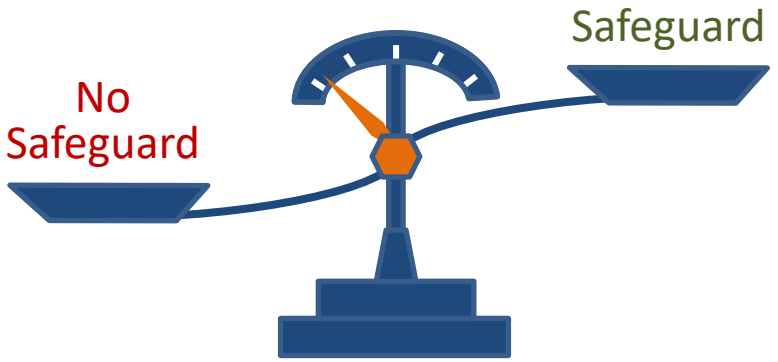


Quantitative Risk Analysis

Risk Analysis						
Asset	**Threat**	**Asset Value**	**Exposure Factor**	**Single Loss Expectancy**	**Annualized Rate of Occurrence**	**Annualized Loss Expectancy**
SRV_1	Fire	$15000	100%	$15000	0.1	$1500
SRV_2	Fire	$20000	100%	$20000	0.1	$2000
SRV_1	Flood	$15000	100%	$15000	0.0001	$1.5
SRV_2	Flood	$20000	100%	$20000	0.0001	$2.0
SRV_1	Virus (no AV software)	$15000	10%	$1500	365	$547,500
SRV_1	Virus (with AV software)	$15000	10%	$1500	1	$1500

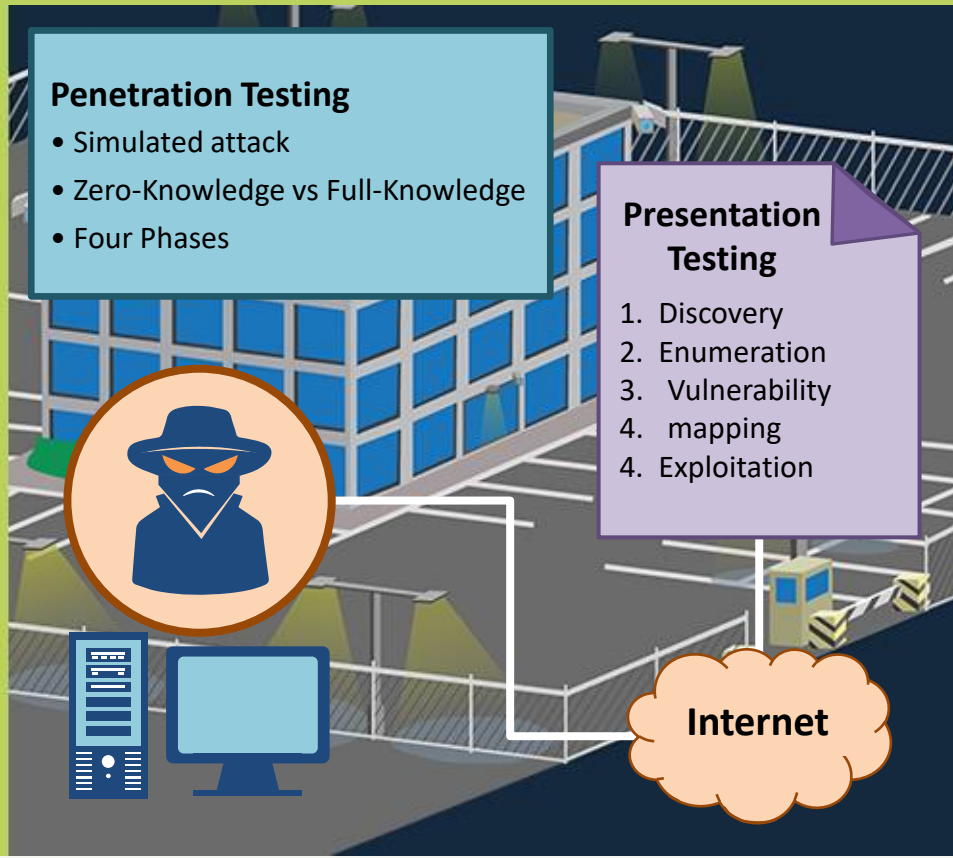
Cost/Benefit Analysis

- Compare the cost of safeguard to cost of not adding it
- What will happen if it is not added?
- Are there methods that will save us more money?
- Will the safeguard produce any vulnerabilities or create a risk?



Testing for Risks

- Often a difficult task
  - Environmental vs Man-made
  - Internal vs External
- Research using historical data and/or interviewing people
- Launching your own attacks
  - Penetration testing
    - Authorization (request form/letter)
  - Vulnerability testing
    - Authorization (request form/letter)



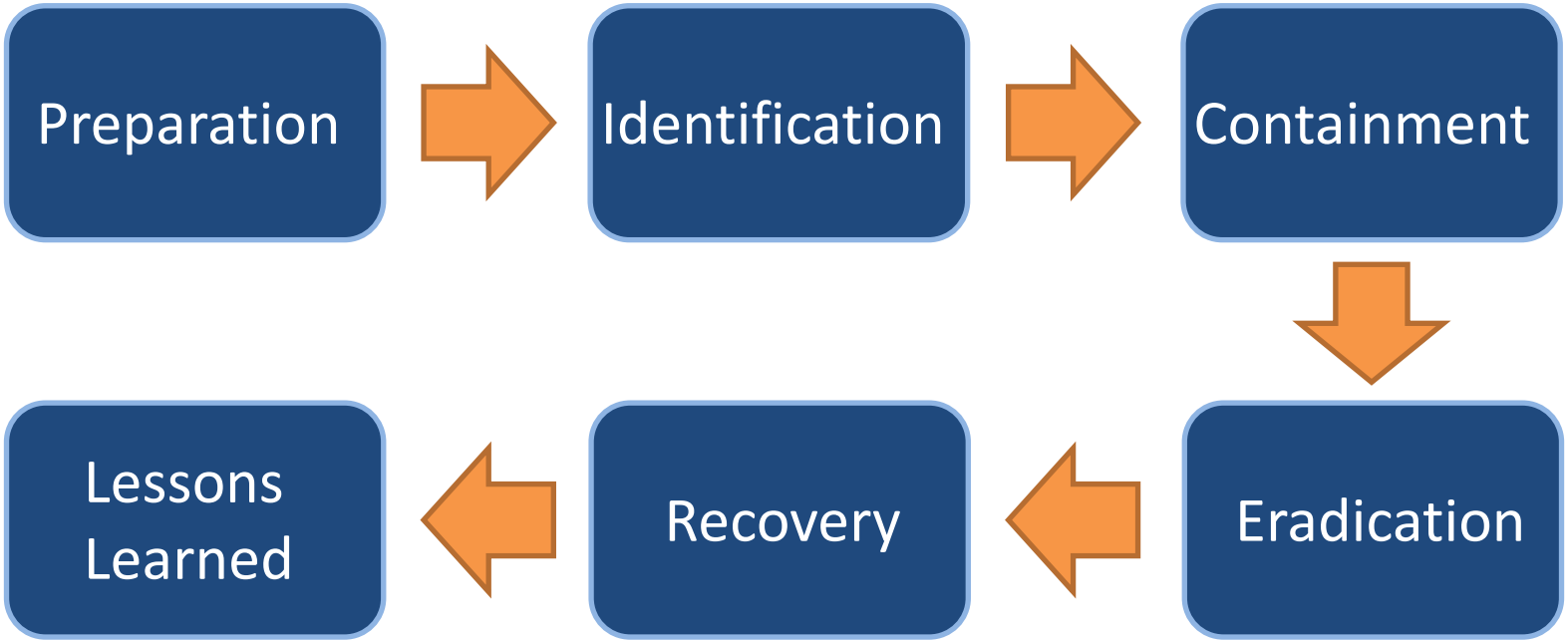
Incident Response

- Steps taken when a negative event disrupts normal operations
- Severity of incident will determine level of action
  - How critical is the target?
  - What is the impact on operations?
- Goals
  - Reduce the immediate impact
  - Maintain and restore business operations
  - Deter future attacks
  - Provide after-action reports and lessons learned to management

Incident Response Plan

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

Incident Response Process



Preparation

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

Identification

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

Containment

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

Eradication

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

Recovery

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

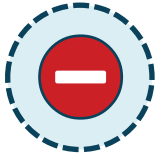
Lessons Learned

Knowledge gained from the process of conducting the program

Sessions usually held at the response close-out

To share and use knowledge derived from an experience

Endorse the recurrence of positive outcomes



Prevent the recurrence of negative outcomes

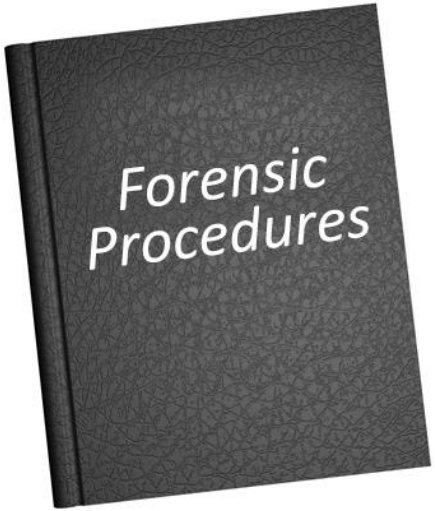
Forensic Investigation

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

Forensic Investigation Procedures

- Investigations need to be carried out in a standardized manner
  1. Identification of the crime
  2. Collection of evidence
  3. Examination of the evidence
  4. Analysis of the evidence
  5. Reporting on the findings of the analysis

- Note: Detailed documentation must be kept at all times!

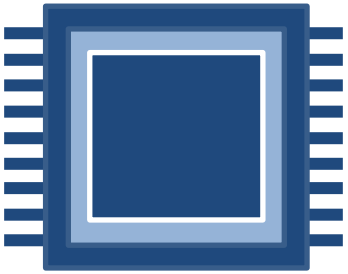


Chain of custody

- Part of Collection phase
- Follows evidence through entire life cycle until possible court date
- Involves strict procedures for collecting, handling and tagging evidence
- Provides a history and timeline of the handling of the evidence
  - Maintains evidence integrity
  - Provides accountability
  - Prohibits tampering

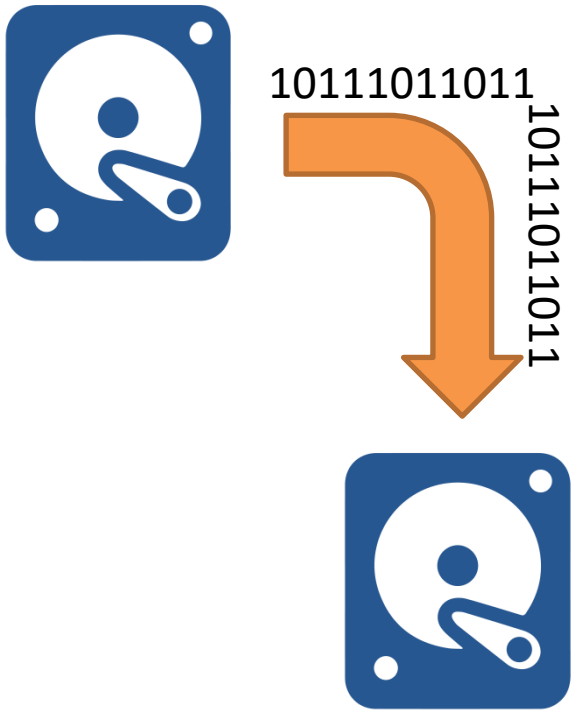
Order of Volatility

- CPU and its cache
- Kernel statistics, tables, and caches
- Memory (RAM)
- Temporary file systems, swap/slack space
- Disk drives and volumes
- Attached removable drives
- Logged data to a remote location
- Copies of data to archived media/cloud
- Witnesses



Data Acquisition

- Capture system images
  - Use write-blockers
  - Forensic kits
- Network traffic and logs
- Capture video
- Record time offsets
- Take hashes
- Create screenshots
- Witness interviews



Data Sanitization Tools

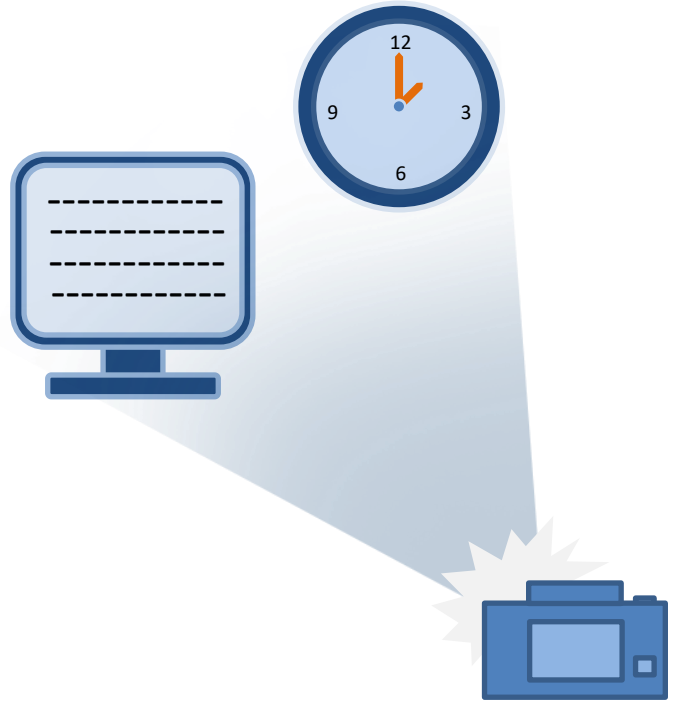
- Data sanitization is the practice of purposely, permanently, and irretrievably removing or destroying the data stored on a data storage device
- A device that has been properly cleaned has no serviceable residual data
- Even advanced forensic tools should not be able recover the erased data from the sanitized component
- Example: WipeDrive and SecureErase are trusted software utilities for securely wiping hard drive data used and approved by the U.S. Department of Defense

Data Sanitization Tools

- Data storage devices such as:
  - Internal and external hard disk drives
  - USB flash drives
  - Memory cards
  - CDs and DVDs
  - PDAs (Blackberries, iPhones) and more must be subject to sanitization policies
- End-users are often unaware of the need to ensure the privacy of the information stored on various formats
- Security breaches and data loss/leakage often violate policies and procedures and even larger compliance

Forensic Investigation Procedures

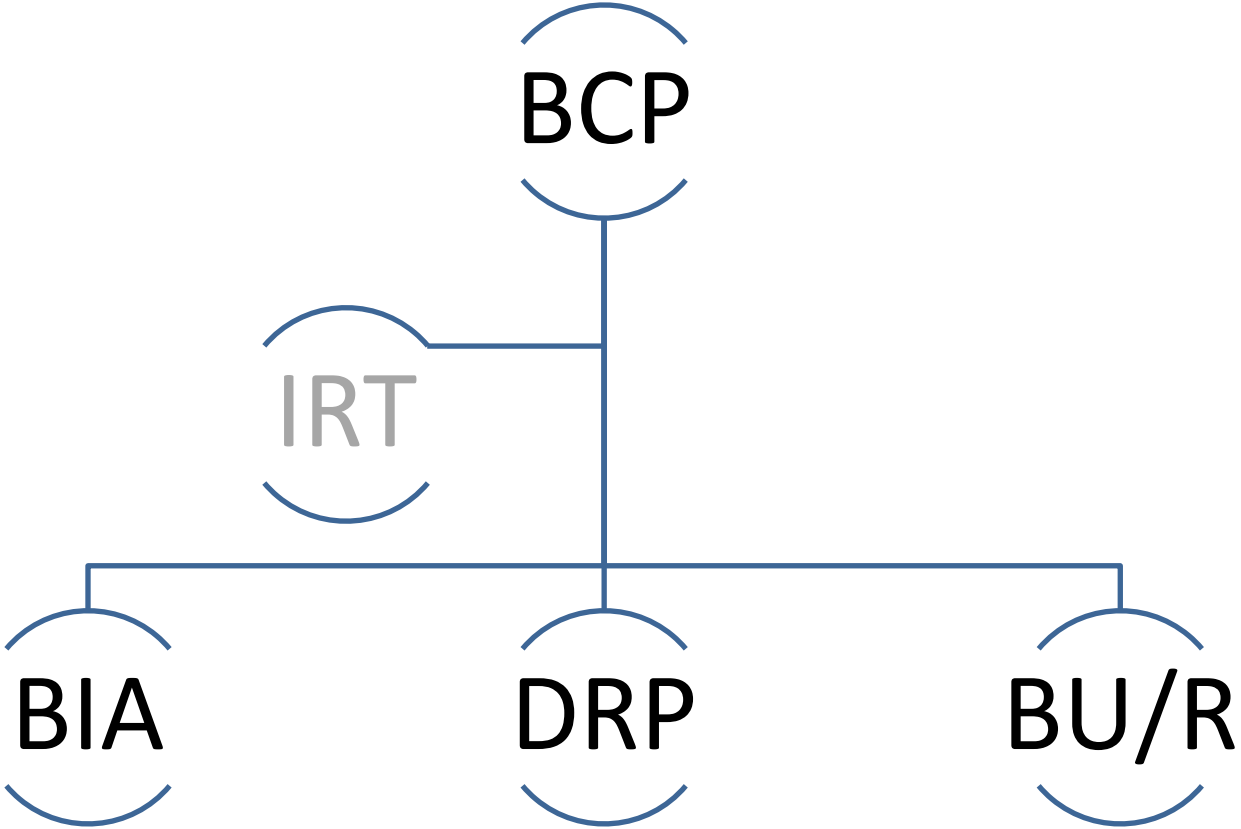
- Considerations
  - Record time offset
  - Network traffic and logs
  - Capture video/take pictures
  - Interview witnesses
  - Use hashes for integrity
    - MD5, SHA-1, SHA-2, SHA-3



Forensic Investigation Procedures

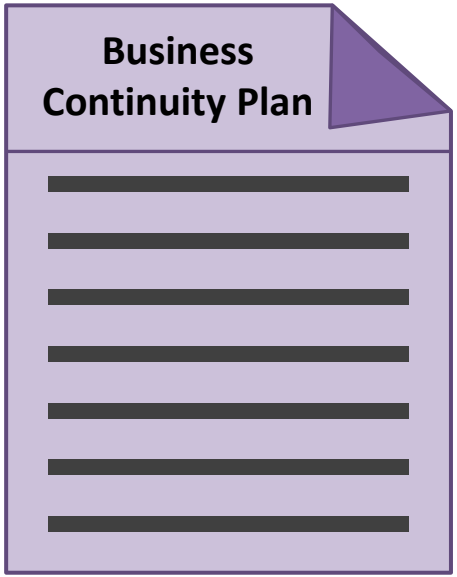
- Techniques (EnCase)
  - Validation
    - Encrypted volume detection
  - Filtering
    - Filtering SIDs on shared systems for privacy reasons
  - Pattern matching
    - Regular expressions and metacharacters in forensic kits
  - Hidden data discovery and extraction
  - Searching slack space
  - Tracing
- **Also has After-Action Reports (AAR) and lessons learned**

Business Continuity Planning (BCP)



Business Continuity Plan

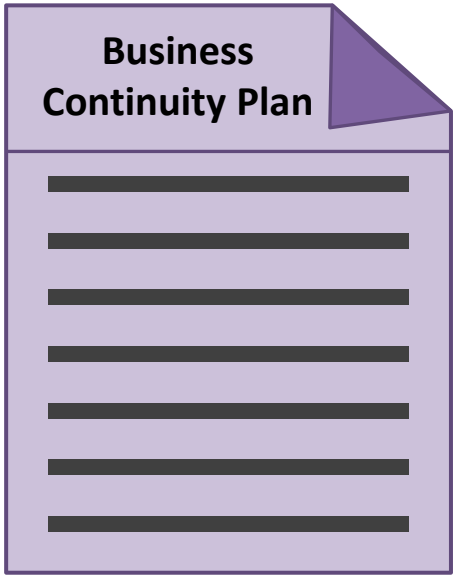
- Ensures business operates a pre-determined level when disaster strikes
  - Documents approved by executive management
- Outlines risks to business
  - Populates Risk Register/Ledger
  - Requirements to mitigate incidents
- Identifies procedures needed to recover from a disaster
  - What is acceptable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



Business Continuity Plan

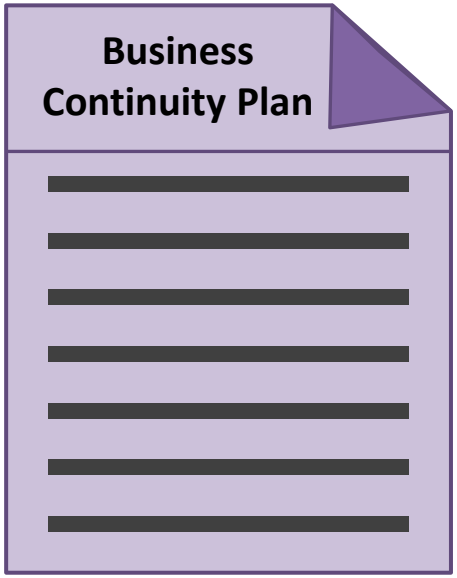
- Living document/plan for continual operations in case of an incident or event
  - Always changing with the needs of your business
  - Plan, Develop, Test, Update on a regular basis

- Steering Committee
  - Coordinator – responsible for success of BCP
  - Project leader – planning, developing, testing
  - Team members – provide insight into business functions
    - Representatives from each department/unit



Business Continuity Plan

- NIST BCP (SP 800-34, Revision 1)
  1. Develop a continuity planning policy statement
  2. Conduct the business impact analysis (BIA)
  3. Identify preventive controls
  4. Create contingency strategies
  5. Develop an information system contingency plan
  6. Ensure plan testing, training, and exercises
     - Checklist reviews, Tabletop exercises, Simulations, Parallel Tests, Full Test
       – After-action report
  7. Ensure plan maintenance

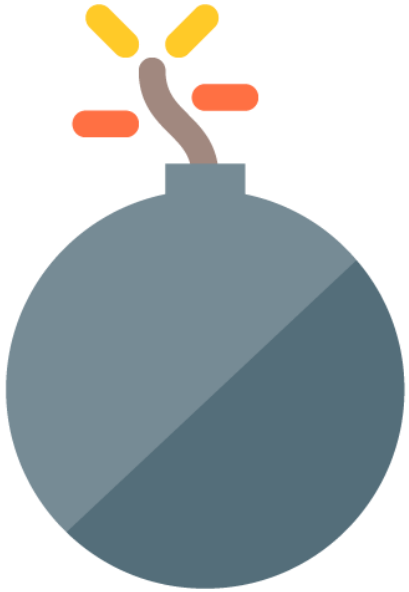


Business Impact Analysis

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

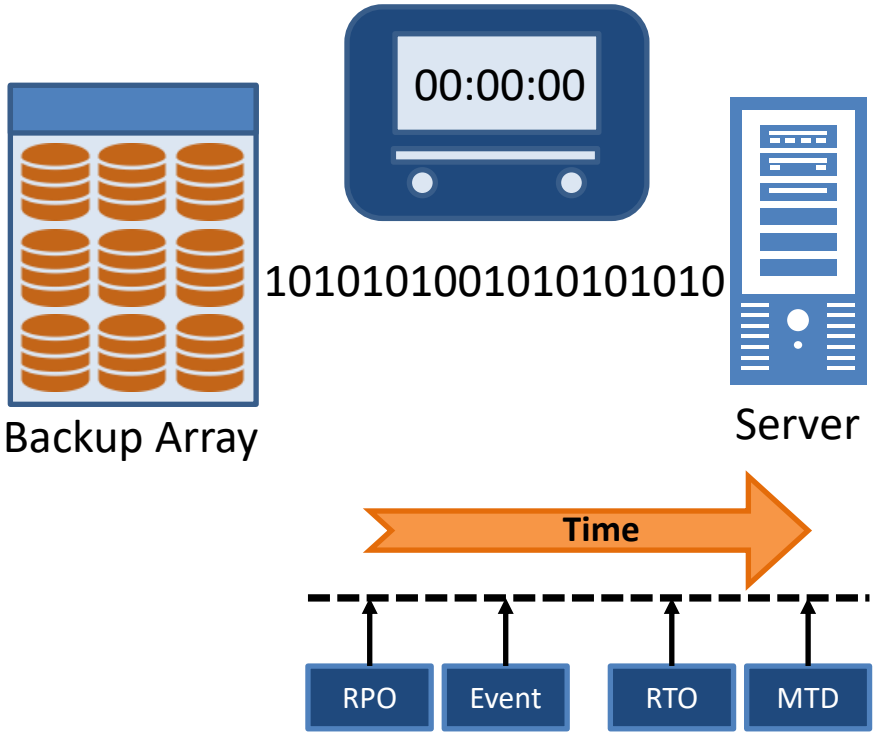
BIA Impact (Magnitude)

- Safety
- Life
- Property
- Revenue
- Reputation
- Legal
- Borrowing costs



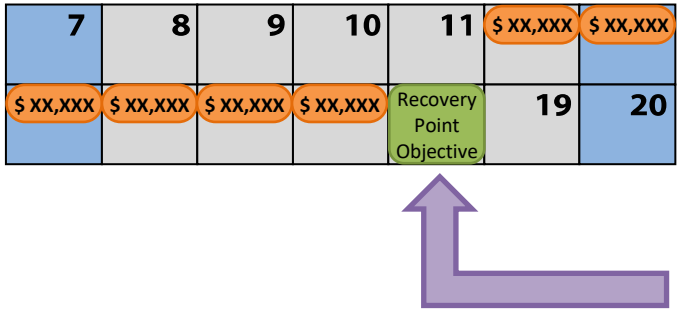
Recovery Time Objective (RTO)

- The amount of time available to recover the resource, service, function
  - Must be equal to or less than MTD
- Any solutions must be accomplished within this time frame or we experience a loss
  - Add physical security
  - Add redundancy
  - Purchase insurance
  - Invest in backup generators
  - Invest in faster
  - Safeguard media off-site

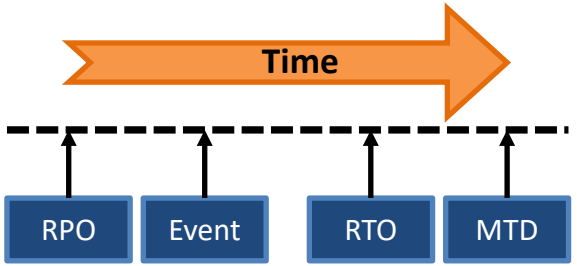


Recovery Point Objective (RPO)

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



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

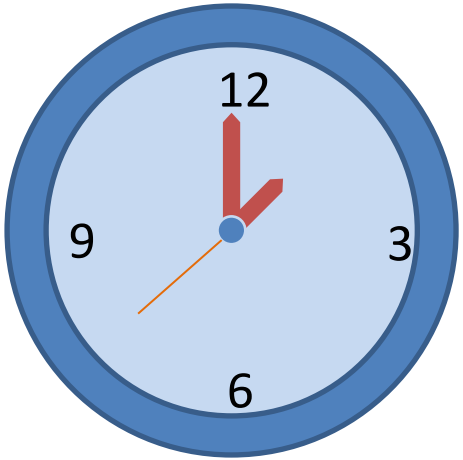


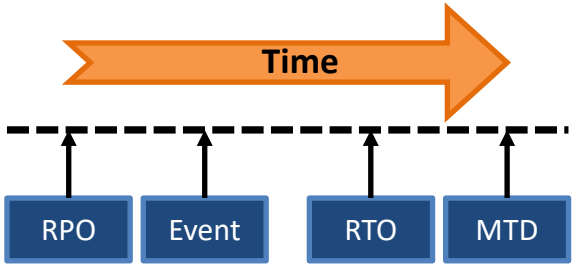
MTBF and MTTR

- Mean Time Between Failure (MTBF)
  - A measure of how reliable a hardware system or component is
  - For most devices, the measure is in thousands or tens of thousands of hours between failures
  - For example, an SSD drive may have a mean time between failure of 10 years
- Mean Time To Repair (MTTR)
  - How long does it take to repair?
    - Measures time to fix
    - Average value predicted based on experience and documentation
    - (Total down time)/(number of breakdowns)

Determining Recovery Time

- Maximum Tolerable Downtime (MTD)
  - Absolute maximum amount of time that a resource, service, function can be unavailable before we start to experience a loss
  - Consider…
    - Finances
    - Life/safety
    - Regulatory
    - Legal/contracts
    - Reputation
    - Property



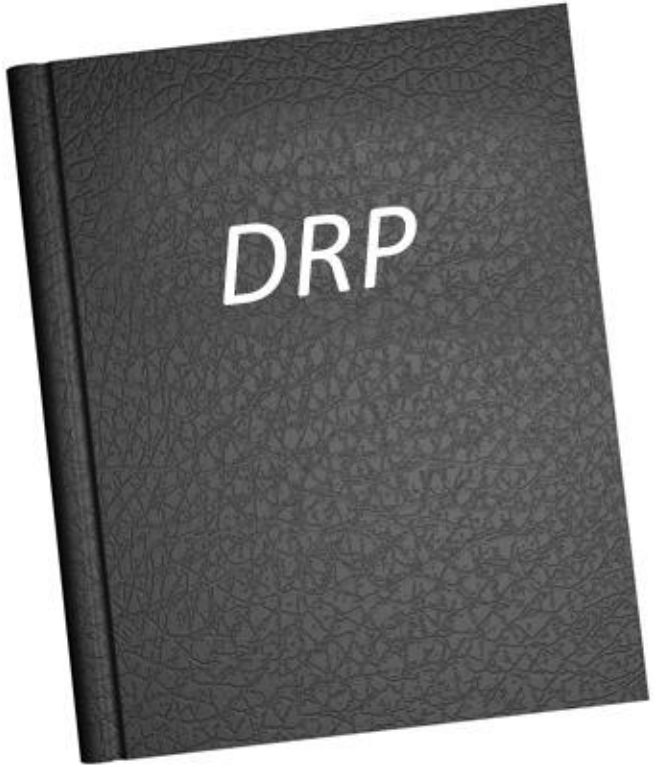


Disaster Recovery

- Ensuring that the company can recover to an established baseline of continuity after any kind of catastrophe
- The processes that will be followed when a disaster strikes
  - A single drive
  - An entire server
  - An area of the facility
  - An entire building
  - An entire site or campus

Disaster Recovery

- Disaster recovery plan
  - Major component of your BCP
  - Outlines the technical aspects involved for restoration
    - **Order of restoration**
      - **Most critical to least critical**
    - Backups and restores
    - Contact information
    - Step-by-step instructions
    - Locations of documents and software and keys



Geographic Considerations

- Offsite backups
  - Keep a copy of your backups off site in a secure location
- Distance
  - Same city, different city, different country, cloud
- Location selection
  - Security standards and practices
- Legal implications
  - Laws in that area
- Data sovereignty
  - Can I even store or operate there?

Recovery Sites

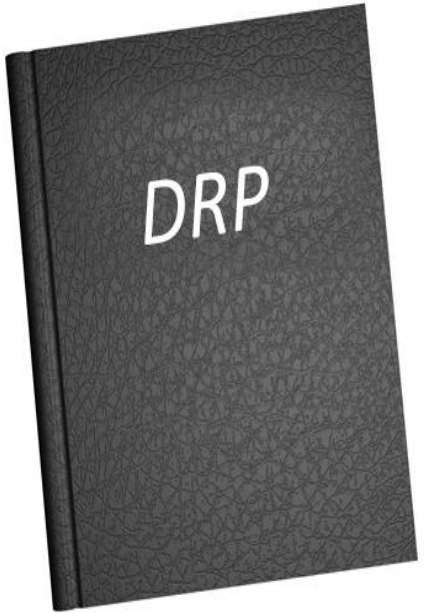
- Cold site
  - An empty location
  - No equipment
    - Everything needs to be brought in and set up
- Warm site
  - A location that is set up with needed equipment
  - No configuration or resources
    - Configurations need to be done and restored
- Hot site
  - Duplicate of the main site that is ready immediately

Recovery Sites

- Exclusive site
  - Only for you
  - You pay the full fee to have it reserved for you
    - If you need it, you have access to it
- Time-shared
  - For multiple companies
  - Companies share the fee to have it reserved for them
    - If one company needs it, they have access to it
    - What if both need it at the same time?
- Mobile sites
  - Special trailers, streamlines, 18-wheelers

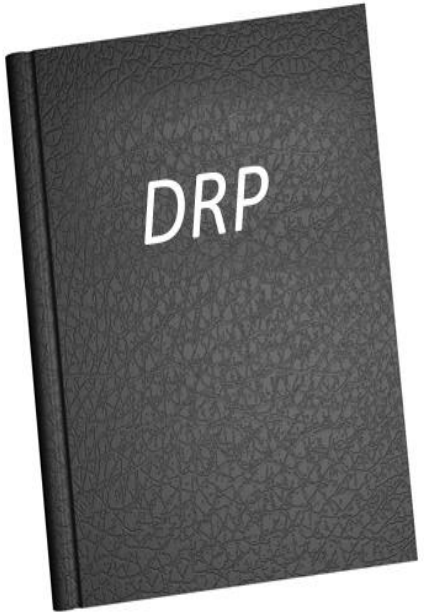
Disaster Recovery Testing and Exercises

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



Disaster Recovery Testing and Exercises

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

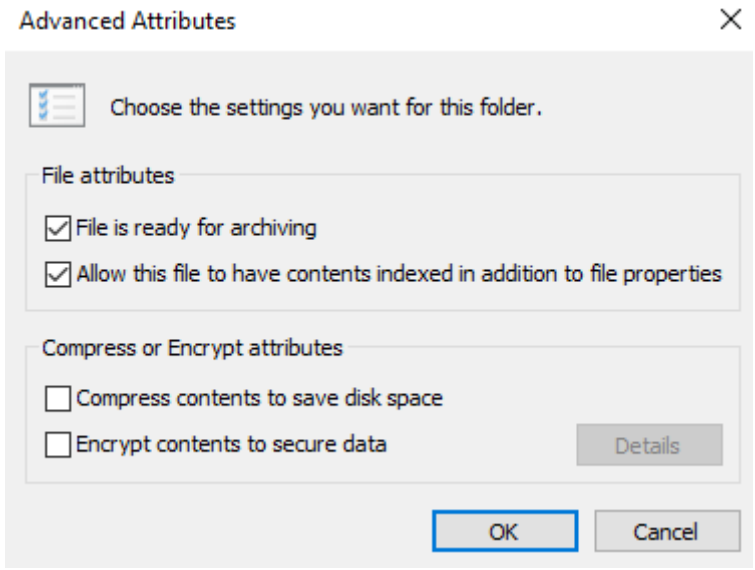


Backup Utilities

- Backup utilities and data backups are also prime targets of attackers
- Key escrow and code escrow can be a good solution
- Storing backup data securely in the cloud is a growing trend
- Physical security and access controls over backups are critical

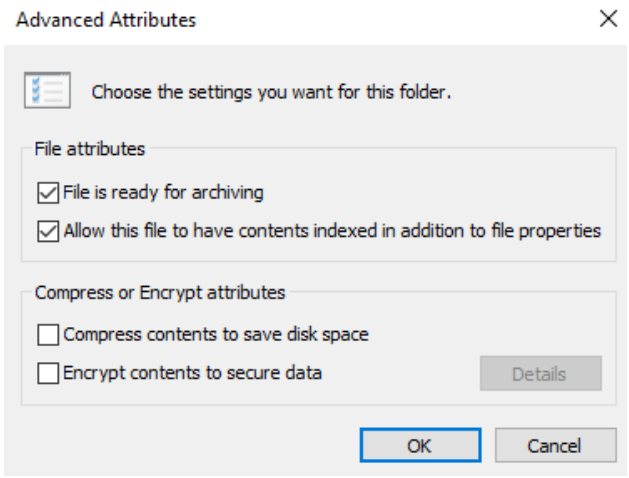
Backups

- Full
  - Backs up everything regardless of archive bit being set or not
    - Clears the archive bit once backup completes
  - Longest to back up
    - Depends on how much has to be backed up
  - Quickest to restore
    - Only the most recent full backup is required



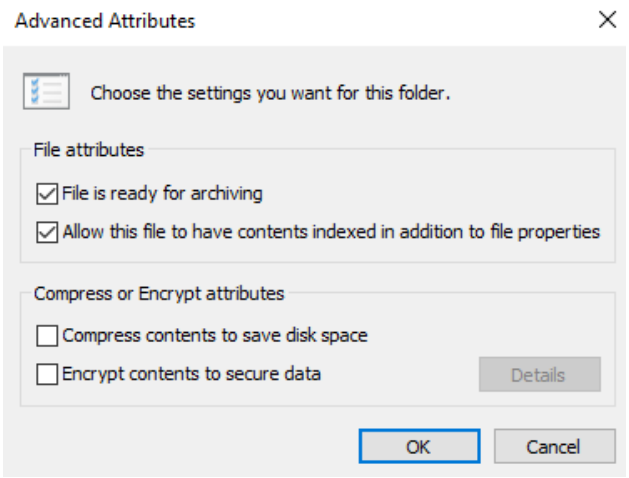
Backups

- Incremental
  - Backs up any file that has the archive bit set
    - Any new file or any file that has changed since
      - The last full backup
      - The last incremental backup
    - Clears the archive bit once backup completes
  - Quickest to back up
    - Only files with archive bit backed up
  - Slowest to restore
    - The last full backup and every incremental backup since are required



Backups

- Differential
  - Backs up any file that has the archive bit set
    - Any new file or any file that has changed since
      - The last full backup
    - Does NOT clear the archive bit once backup completes
  - Slow to back up
    - All files with archive bit set backed up
  - Quick to restore
    - The last full backup and the most recent differential backup needed



Backups

- Snapshots
- Easier and faster backups and restores
  - Immediate point-in-time virtual copy of source
    - Should be replicated to another media to be considered a backup
  - Time to back up does not increase with amount of data
- Improved RTO and RPO
  - Restores are faster
  - Less data is lost with an outage