Breakdown of Exam
Domain 1: Security Principles (26%)

Domain 2: Business Continuity, Disaster Recovery, and Incident Response (10%)
Domain 3: Access Control Concepts (22%)
Domain 4: Network Security (24%)
Domain 5: Security Operations (18%)

_____
ISC2 Code of Ethics

1. Protect society and infrastructure (Hacking)
    - Anyone may file a complaint
2. Act honorably, justly and within laws (Lying)
    - Anyone may file a complaint
3. Serve principles diligently and competently (Fulfill your duties)
    - Only employers and clients may file under a complaint, due to the nature of the code
4. Advance the information security profession (Helping cheat exams)
    - Other Professionals may file a complaint, due to the nature of the complaint
    - Professionals only

- You are required to report any witness of violation of Code of Ethics
    - Failure to report witnessed violation is a violation
    - Submit a Complaints Form to report
    - You must have a standing before you make a complaint
        - Standing: Alleged behavior must harm you or your profession in someway

_____
3 Goals of Information Security

- **C**onfidentiality
    - Protects information from unauthorized disclosure
- **I**ntegrity
    - Protects information from unauthorized changes
- **A**vailability
    - Protects authorized access to systems and data
    - Ensures information is available to authorized users

= CIA
Confidentiality Concerns

- Snooping

- Involves gathering information that is left out in the open
    - Clean desk policies protect against snooping
- Dumpster Diving
    - Looking through trash for information
        - Shredding protects against Dumpster Diving
- Eavesdropping
        - Rules about sensitive conversations prevent eavesdropping
- Wiretapping
    - Electronic Eavesdropping
        - Encryption protects against wiretapping
- Social Engineering
    - Attacker uses psychological tricks to persuade employee to give it or give access to information
        - Education and Training protects against social engineering

Integrity Concerns

- Unauthorized Modification
    - Attackers make changes without permission (can be internal=employees or external
        - Follow the Rules of Least Privilege to prevent unauthorized modification
- Impersonation
    - Attackers pretend to be someone else
        - User education protects against Impersonation
- Man-in-the-Middle (MITM)
    - Attackers place the themselves in the middle of communication sessions
    - Intercepts network traffic as users are logging in to their system and assumes their role.
    - Impersonation on an electronic/digital level.
        - Encryption prevents man-in-the-middle attacks
- Replay
    - Attackers eavesdrop on logins and reuse the captured credentials
        - Encryption prevents Replay attacks

Availability Concerns

- Denial of Service (DoS)
    - When a malicious individual bombards a system with an overwhelming amount of traffic.
    - The idea to is to send so many requests to a server that it is unable to answer any requests from legitimate users
        - Firewalls block unauthorized connections to protect against Denial of Service attacks
- Power Outages
    - Having redundant power sources and back-up generators protect against power outages
- Hardware Failures
    - Failure of servers, hard drives, network gear etc
        - Redundant components protect against hardware failure
        - Building systems that have a built-in redundancy, so that if one component fails, the other will take over
- Destruction
    - Backup data centers protect against destruction (ex=cloud)
- Service Outages
    - Service outage may occur due to programming errors, failure of underlying equipment, and many more reasons
        - Building systems that are resilient in the fact of errors and hardware failures protect against service outages

Authentication & Authorization

Access Control Process

1. Identification
    - Identification involves making a claim of identity (Can be false)
        - Electronic identification commonly uses **usernames**
2. Authentication
    - Authentication requires proving a claim of identity
        - Electronic authentication commonly uses **passwords**
3. Authorization

- Authorization ensures that an action is allowed
    - Electronic authorization commonly takes the form of **<u>access control lists</u>**
        - Access Control Lists also provides ***Accounting*** functionality
            - Accounting allows to track and maintain logs of user activity
            - Can track systems and web browsing history

Authentication + Authorization + Accounting = AAA

_____

Password Security
Controls you can implement when setting password requirements:

- Password length requirements
- Password complexity requirements
- Password expiration requirements
    - Force password changes
- Password history requirements
    - Cannot use previously used passwords

Every organization should make it easy for users to change their passwords, however, be careful of <u>password reset process</u> as it may provide an opportunity for attackers to take advantage through unauthorized password reset.
Password Managers

- Secured password vaults often protected by biometric mechanisms (ex=fingerprints)
- Facilitates the use of strong, unique passwords
- Stores passwords

_____

Multi Factor Authentication
3 types of authentication factors

1. Something you know
    - Passwords, Pins
2. Something you are
    - Biometric Security Mechanisms
    - Fingerprints
    - Voice
3. Something you have
    - Software and Hardware Tokens

You combine these factors all together = Multi Factor Authentication
*Note: Passwords combined with security questions are **NOT** multi factor authentication. Passwords and security questions are <u>both something you know</u>*
Single Sign-On (SSO)

- Shares authenticated sessions across systems
- Organizations create SSO solutions within their organizations to **avoid users repeatedly authenticating**

Non-repudiation

- Prevents someone from denying the truth
    - Physical signatures can provide non-repudiation on contracts, receipts etc
    - Digital signatures use encryption to provide non-repudiation
    - Other methods can be biometric security controls, Video-surveillance etc

---

Privacy
Organization Privacy Concerns

1. Protecting our down data
    - Protect your down organizations data
2. Educating on users
    - Educated users of how they can protect their own personal information
3. Protecting data collected by our organizations
    - Protecting data that was entrusted to the organization (ex= client's data)

2 Types of Private Information

1. Personally-Identifiable Information (PII)
    - Any information that can be tied back to a specific individual
2. Protected Health Information (PHI)
    - Health care records
        - Regulated by HIPPA

Reasonable expectation of privacy

- Many laws that govern whether information must be protected are based upon whether the person disclosing the information had a reasonable expectation of privacy
    - Ex= if you upload a YouTube video, you do not have a expectation of privacy
    - *You do have some expectation of privacy* for private electronic communications such as: email, instant chats etc
    - *You do not have a reasonable expectation* of privacy when sharing PII with an organization
    - *You do not have a reasonable expectation of privacy* when using employer resources

Risk Management

1. Internal Risks
    - Risks that arise from within the organization
        - Internal control prevents internal risks
2. External Risks
    - Risks that arise outside the organization
        - Build controls that reduce the chance of attack/risks being successful (ex= multi factor authentication, or social engineering awareness campaigns)
3. Multiparty Risks
    - Risks that affect more than one organization
    - **Intellectual property theft** poses a risk to knowledge-based organizations
    - If attackers are able to alter, delete or steal this information, it would cause significant damage to the organization and its customers/counterparties
    - Software license agreements issues risk fines and legal actions for violation of license agreements

Risk Assessment

- Identifies and triages risks

Threat

- Are external forces that jeopardize security
    - **Threat Vector**
        - Threat Vectors are methods used by attackers to get to their target (ex= social engineering, hacker toolkit, etc)

Vulnerabilities

- Are weaknesses in your security controls
    - Examples : Missing patches, Promiscuous Firewall rules, other security misconfiguration

Threat + Vulnerability = Risk

Ranking of Risks

- We rank risks by **likelihood** and **impact**

Likelihood

- Probability a risk will occur

Impact

- Amount of damage a risk will cause

2 Categories of Risk Assessment

1. Qualitative Techniques
    - Uses **subjective ratings** to evaluate risk likelihood and impact: Usually in the form of **low, medium or high** on both the likelihood and impact scales.
2. Quantitative Techniques
    - Uses subjective **numeric ratings** to evaluate risk likelihood and impact

---

Risk Treatment (Management)

- Analyzes and implements possible responses to control risk

4 Types of Risk Treatment

1. **Risk Avoidance**
    - Changes business practices to make a risk irrelevant
2. **Risk Transference**
    - Attempting to shift the impact of a risk from your organization to another organization
    - Example : Insurance policy
    - Note that you cannot always transfer the risk completely. Reputation damage etc.
3. **Risk Mitigation**
    - Actions that reduce the likelihood or impact of a risk
4. **Risk Acceptance**
    - Choice to continue operations in the face of a risk

Risk Profile

- Combination of risks that an organization faces

Inherent Risk

- Initial level of risk, before any controls are put in place

Residual Risk

- Risk that is reduced and what is left of it is known as the residual risk

Control Risk

- New risk that may have been introduced by the controls applied to mitigate risk
    - Example : Controls Applied may be installing a firewall. While that firewall may have mitigated the inherent risk, the risk of that firewall failing is another newly introduced risk

Inherent Risk → **Controls Applied** → (Residual Risk + Control Risk)
Risk Tolerance

- Is the level of risk an organization is willing to accept

Security Controls

- Are procedures and mechanisms that reduce the likelihood or impact of a risk and help identify issues

Defense in Depth

- Uses **overlapping** security controls
- Different methods of security with a common objective

Security professionals uses different *categories to group similar security controls*
First you must group Controls by their purpose. 3 Types of Control Purposes are:

1. Prevent
    - Stops a security issue from occurring
2. Detect
    - Identify security issues requiring investigation
3. Correct
    - Remediate security issues that have already occurred

Then group them by their Control Mechanism: 3 Types of Control Mechanisms are:

1. Technical
    - Use technology to achieve control objectives
    - Examples: Firewalls, Encryption, Data Loss Prevention, Antivirus Software)
    - Technical Control a.k.a Logical Control
2. Administrative
    - Uses processes to achieve control objectives
    - Examples: User access reviews, log monitoring, performing background checks)
3. Physical
    - Controls that impact the physical world
    - Examples: Locks, Security guard

Configuration Management

- Tracks the way specific devices are set up
- Tracks both operating system settings and the inventory of software installed on a device
- Should also create Artifacts that may be used to help understand system configuration (Legend, Diagrams, etc)

Baselines

- Provide a configuration snapshot
- Dual Net
- You can use the snapshot to assess if the settings are outside of an approved change management process system
- Basically the default configuration setting set by an organization

Versioning/Version Controls

- Assigns each release of a piece of software and an incrementing version number that may be used to identify any given copy
- These verison #s are written as three part decimals, with the
    - First number representing the major version of software
    - Second number representing a major updates
    - Third number representing minor updates

Ex= IPhone IOS 14.1.2
Standardizing Device Configurations by:

- Standardizing Naming conventions
- IP Addressing schemas

_____
Security Governance
You must first identify how domestic and international **Laws and Regulations** apply to an organization
Security Policy Framework

- A framework that everyone in an organization must follow
- There are **4 types of documents** in a Security Policy Framework

1. Policies
    - Provide the foundation for an organization's information security program
    - Describes organization's security expectations
    - Policies are set by Senior Management
    - Policies should stand the test of time anticipating future changes
    - Compliance with Policies are **mandatory**
2. Standards
    - Describes the specific details of security controls
    - Compliance with Standards are **mandatory**
3. Guidelines
    - Provide advice to the rest of the organization on best practices

- Compliance with Guidelines are **optional**

4. Procedures

    - Step-by-step procedures of an objective.
    - Compliance can be **mandatory or optional**

_____

Best Practice of Security Policies

1. Acceptable Use Policies (AUP)

    - Described authorized uses of technology

2. Data Handling Policies

    - Describe how to protect sensitive information

3. Password Policies

    - Describes password security practices
    - An area where all the password requirements (length, complexity) gets officially documented

4. Bring Your Own Device Policies (BYOD)

    - Cover the usage of personal devices with company information

5. Privacy Policies

    - Cover the use of personally identifiable information
    - Can be enforced by National & Local authorities

6. Change Management Policies

    - Cover the documentation, approval, and rollback of technology changes

_____

Business Continuity

Business Continuity Planning (BCP)

- The set of controls designed to keep a business running in the face of adversity, whether natural or man-made
- Also known as Continuity Of Operations Planning (COOP)
- Directly impacts the #3 goal of security = Availability
- When planning, proactively as what *business activities, systems, and controls* will it configure

Business Impact Assessment (BIA)

- A risk assessment that uses a quantitative or qualitative process
- Begins by identifying organization's mission essential functions and then traces those backwards to identify the critical IT systems that support those functions

In Clouding, Business Continuity Planning requires collaboration between cloud providers and customers
Redundancy

- The level of protection and against the failure of a single component

Single Point of Failure Analysis

- Provides a mechanism to identify and remove single points of failure from their systems
- The SPOF analysis continues until the cost of addressing risk outweighs the benefit
- SPOF can be used in many areas other than the IT Infrastructure, it can be applied in management of HR, 3rd party vendor reliance etc)

Continued Operation of Systems

- Can be ensured in 2 ways:

1. High Availability
    - Uses multiple systems to protect against service failure (Different from AWS Cloud as in that it does not just apply to AZs but rather everything including multiple firewalls etc)
2. Fault-Tolerance
    - Makes a single system resilient against technical failures

Load Balancing

- Spreads demand across available systems

Common Points of Failure

1. Power Supply
    - Contains moving parts
    - High failure rate
        - Can use multiple power supplies
        - Uninterruptible Power Supplies (UPS) - supplies battery to devices during brief power disruptions. UPS may be backed up by an additional power generator
        - Power Distribution Units (PDUs) provide power clearing and management for a rack
2. Storage Media
    - Protection against the failure of a single storage divide
        - Redundant Array of Inexpensive Disks (RAID) : Comes in many different forms but each is designed to provide redundancy by having more discs than needed to meet business needs
        - There are 2 RAID technologies
            - Mirroring
                - Considered to be **RAID Lvl 1**
                - Server contains 2 identical synchronized discs
            - Striping

- Disc Striping with parity
- **RAID Lvl 5**
- Contains 3 or more discs
- Also includes an extra disc called Parity Block
- When one of the disc fails, the Parity Block is used to regenerate the failed disc's content

- **RAID is a Fault-Tolerance technique NOT a Back-up strategy**

3. Networking

    - Improve networking redundancy by having **multiple Internet service providers**
    - Improve networking redundancy by having dual-network interface cards **(NIC) or NIC Teaming** (similar to how you use multiple power supplies)
    - Implement **Multipath Networking**

*Fault-Tolerance mechanisms prevents systems from failing, even if one of these above points experience a complete failur*e
Always attempt to add **Diversity** in your infrastructure to improve redundancy

- Diversity in Technology Used
- Diversity of Vendors Diversity of Cryptography
- Diversity of Security Controls

Incident Response

Incident Response Plans

- Provide structure during cybersecurity incidents
- Outlines policies, procedures and guidelines that govern cybersecurity incidents

Elements of a Incident Response Plan

- Statement of Purpose
- Strategies and goals for incident response
- Approach to incident response
- Communication with other groups
- Senior leadership approval

Tips on best practices:

- When developing your Incident Response Plan, consult **NIST SP 800-61** as you develop your plan
- Also review other organization's plan

NIST SP 800-61

- Assists organization mitigating the potential business impact of information security incidents providing practical guidance.

Building a Incident Response Team
IR Team should consist of:

- Management

- Information Security Personnel
- SMEs
- Legal Counsel
- Public Affairs
- Human Resources
- Physical Security

If your organization lacks personnels from these areas:

- Use incident response service providers to assist if necessary

---

Incident Communication Plan

- Communications Plans ensure that all participants have timely, accurate information
- Make sure to minimize or limit communications to third parties (Media etc)
- You will have to choose whether or not to involve law enforcement
    - Drawbacks of law enforcement engagement can be release of sensitive details to public which may be unfavorable to the organization
- Always involve your own organization's legal team to ensure compliance with laws and organization's obligations with 3rd parties.
- Describe communication paths on how information will trickle down the organization

---

Incident Identification

- Organizations have a responsibility to collect, analyze and retain security information

Data is crucial to incidence detection
Incident Data Sources

- IDS/IPS - Intrusion Detection System/Intrusion Prevention System
    - Designed to **only provide an alert** about a potential incident
- Firewalls
- Authentication Systems
- Integrity Monitors
- Vulnerability Scanners
- System Event Logs
- Netflow Records
- Antimalware Packages

Security Incident and Event Management (SIEM)

- Security solution that collects information from diverse sources, analyzes it for signs for security incidents and retains it for later use.
- **Centralized log repositories**
- Basically take a load of data, feed it to the SIEM, and it will spit out details regarding risk

*When these systems and security mechanisms **FAIL** do detect risks before dealt with internally, an **EXTERNAL** source (customer) may be first to detect a risk*

*Therefore, IR Team should have a consistent method for **receiving, recording, and evaluating external reports***

_____
First Responder Duty

- First responders (whomever they are, whom encounters the risk first) have a set of responsibilities as they may have the power to tremendously reduce risk

Highest Priority

- The highest priority of a First Responder must be **containing damage through isolation**

_____
Disaster Recovery
Disaster Recovery (DR)

- Restores normal operations as quickly as possible following a disaster

- Disaster recovery plan steps in when **business continuity plan fails**
- Disaster recovery plan effort is not finished until organization is completely back to normal
- Flexibility is key during a disaster response

Initial Response Goals

1. Contain the damage through isolation
2. Recover normal operations

Communications required for an effective DR

- Initial Report
- Status updates
- Ad hoc messages

Once Initial Response is implemented, the **DR team shifts to Assessment Mode**
Assessment Mode

- Goal of this mode is to triage/analyze the damage and implement recover operations on a permanent basis
- Depending on circumstances there may be an intermediary mode of Temporary Recovery but will gradually move to Permanent Recovery

Recovery Time Objective (RTO)

- Is the targeted amount of time to restore service after disruption

Recovery Point Objective (RPO)

- Is the targeted amount of data to recover

Recovery Service Level (RSL)

- Is the targeted percentage of service to restore
- Also the percentage of service that must be available during a disaster

---

Backups

- Provides an organization with a fail-safe way to recover their data in the event of
    - Technology failure
    - Human error
    - Natural disaster

Backup Methods

1. Tape Backups
    - Practice of periodically copying data from a primary storage device to a tape cartridge
    - Traditional method - outdated
2. Disk-to-disk Backups
    - Writes data from Primary Disks to special disks that are set aside for backup purposes
    - Backups that are sent to a storage area network or a network attached storage are also fitting in this category of backup
3. Cloud Backups
    - AWS, Azure, GC

Different Types of Backups

1. Full Backups
    - Include a complete copy of all data
        - Snapshots and images are types of full backups
2. Differential Backups
    - Includes all data modified since the last full backup
    - Supplements Full Backups
3. Incremental Backups
    - Include all data modified since the last full *or incremental backup*

Scenario: Joe performs full backups every Sunday evening and differential backups every weekday evening. His system fails on Friday morning. What backups does he restore?
A: 1) Sundays Full Backup
2) Thursday's differential backup
Scenario: Joe performs full backups every Sunday evening and incremental backups every weekday evening. His system fails on Friday morning. What backup does he restore?
A: 1) Sunday's Full Backup
2) Monday, Tuesday, Wednesday, Thursday incremental backups
Trade off: Incremental backups takes longer to restore but requires smaller storage

---

Disaster Recovery Sites

- Provide alternate data processing facilities
- Usually stay idle until emergency situation arises

3 Types of Disaster Recovery Sites/Alternate Processing Facility

1. Hot Site

    - Premier for of disaster recovery facility
    - **Fully operational Data Centers**
    - Can be activated in moments or automatically deployed
    - Very expensive

2. Cold Site

    - Used to restore operations eventually, but requires a significant amount of time
    - **Empty Data Centers**
    - Stocked with core equipment, network, and environmental controls but **do not have the servers or data required to restore business**
    - Relatively Inexpensive
    - Activating them may take weeks or even months

3. Warm Site

    - Hybrid of Hot and Cold
    - Stocked with core requirements **and data**
    - Not maintained in parallel fashion
    - Similar in expense as a Hot Site
    - Requires significant less time from IT Staff
    - Activating them may take hours or days

Disaster Recovery Sites *don't only provide a facility for technology operations, but* ***also serve as an Offsite Storage Location.*** They are:

- Geographically distant
- Site Resiliency
- Allows backups to be physically transported to the disaster recovery facility either manually or electronically called "**Site Replication**"
- Online or offline backups

    - Online backups are available for restoration immediately, but is very expensive
    - Offline backups may require manual intervention, but is very inexpensive

Alternate Business Process

- A change of an organization's business protocols to match the current Disaster Recovery Plan

---

Disaster Recovery Testing Goals

1. Validate that the plan functions correctly
2. Identify necessary plan updates

5 Types of Disaster Recovery Testing

1. Read-through

    - Simplest form of Disaster Recovery Testing
    - Asks each team member to review their role in the disaster recovery process and provide feedback
    - Known as “Checklist Reviews”

2. Walk-through

    - A more comprehensive approach but similar to Read-Through
    - Gathers the team together for a formal review of the disaster recovery plan
    - Known as “Tabletop Exercise ”

3. Simulation

    - Uses a practice scenario to test the Disaster Recovery Plan
    - Scenario based- very specific circumstances

4. Parallel Test

    - While above are all theoretical approaches, the Parallel Test actually activates the Disaster Recovery Environment
    - However, they do not switch operations to the backup environment

5. Full Interruption

    - **Most effective**
    - Activate Disaster Recovery Environments
    - Also switch primary operations to the backup environment
    - Can be very disruptive to business

Testing strategies often combine multiple types of tests

Physical Access Controls

Facilities that require Physical Security:

1. Data Centers

    - Most important

2. Server Rooms

    - Has sensitive information in **less** secure locations

3. Media Storage Facilities

    - If in a remote location may require as much security as the Data Centers

4. Evidence Storage Locations
5. Wiring Closets

    - Literally a cluster of wires
    - Needs to be protected as it offers access to digital eavesdroppers and network intruders

6. Distribution Cabling

- Neatly organized cables in the ceiling

7. Operations Center

_____

Types of Physical Security

1. Gates
    - Allows you to focus on other security controls
2. Bollards
    - Block vehicles while allowing pedestrian traffic

CPTED

- Crime Prevention Through Environmental Design
    - Basically giving principles to design your crime prevention mechanisms in a way that is appropriate with your environmental surroundings

CPTED Goals

1. Natural Surveillance
    - Design your security in a way that allows you to observe the natural surroundings of your facility
        - Windows, Open Areas, Lightning
2. Natural Access Control
    - Narrowing the traffic to a single point of entry
        - Gates, etc
3. Natural Territory Reinforcement
    - Making it visually and physically obvious that the area is closed to the public
        - Signs, Lightnings

_____

Visitor Management

- Visitor management procedures protect against intrusions

Visitor Procedures

- Describe allowable visit purposes
- Explain visit approval authority
- Describe requirements for unescorted access
- Explain role of visitor escorts
- All visitor access to secure areas should be logged

- Visitors should be clearly identified with distinctive badges
- Cameras add a degree of monitoring in visitor areas
- Cameras should always be **disclosed**

Physical Security (Human Security)

- Receptionists may act as Security Guards
- Sometimes an “aggressive” look is sometimes desirable
- Robots may replace human security patrols

Two Person Rule (Two-Person Integrity)

- Two people must enter sensitive areas together

Two Person Control

- Two people must have control access to very sensitive functions, requiring an agreement of 2 persons before action
    - Ex=Requiring 2 Keys to trigger a launch of Nuclear Missiles

---

Logical Access Controls

Account Management Tasks

- Implementing Job Rotation schemes
    - Implementing for employees to rotate job functions for purpose of diversity and integrity in work
- Mandatory Vacation policies
    - People on vacation should not have access to sensitive data
- Managing Account Lifecycle
    - Ensuring that as employees move around an organization with different roles, that they are given access to corresponding roles

---

Account Monitoring Procedures

1. Account Audits
    - Completed by pulling all permission list, review, and make adjustments
    - Protects against Inaccurate Permissions
        - Inaccurate Permissions
            - Wrong permissions assigned that results in too little access to do their job or too much access (violates least privilege)

- Result of **Privilege Creep**
    - A condition that occurs when users switch roles and their previous role's access to system has not been revoked

2. Formal Attestation Process
    - Auditors review documentation to ensure that managers have formally approved each user's account and access permissions.
3. Continuous Account Monitoring
    - Watch for suspicious activity
    - Alert administrations to anomalies
    - Will catch any unauthorized use of permissions or acts
    - Flags Access Policy Violations
        - Impossible travel time logins
        - Unusual network location logins
        - Unusual time-of-day logins
        - Deviations from normal behavior
        - Deviations i volume of data transferred
4. Geotagging
    - Adds user location information to logs
5. Geofencing
    - Alerts when a device leaves defined boundaries

_____

Provisioning and Deprovisioning

- Involves the process of creating, updating and deleting user accounts in multiplace applications and systems
- Crucial to Identity and Access Management Task

Provisioning

- After onboarding, administrators create authentication credentials and grant appropriate authorization

Deprovisioning

- During the off-boarding process, administrators disable accounts and revoke authorizations at the appropriate ti**me.**
- **Prompt Termination (quickly actin**g after off boarding) is critical
    - Prevents users from accessing resources without permission
    - More important if employee leaves in unfavorable terms

Routine Workflow (For offboarding)

- Disable accounts on a scheduled basis for **planned departures**

Emergency Workflow (For offboarding)

- Immediately suspends access when user is **unexpectedly terminated**

Incorrect Timed Account-Deprovisioning may:

- Inform a user in advance of pending termination
- Allow user to access to resources after termination

*It is a good idea to **Deactivate the account first** before permanent removal as it can be reversed*

Authorization

- **Final step** in the Access Control Process
- Determines what an authenticated user can do

Principle of Least Privilege

- User should have the **minimum** set of permission necessary to perform their job
    - Protects against internal risks as a malicious employee's damage will be limited to their access
    - Protects against external risk as if an account was hacked, the damage they can do would be limited to the permissions on the stolen account.

Mandatory Access Control (MAC) System - **Confidentiality**

- Permissions are determined by the system/operating system
- Users cannot modify any permissions
- Rule-based access system
- Most Stringent/strict

Discretionary Access Control (DAC) System - **Availability**

- Permissions are determined by the file owners
- Most Common type of access control
- Flexible

Role-Based Access Control (RBAC) Systems - **Integrity**

- Permissions are granted to groups of people/ job functions
- Group based

Computer Networking

Network

- Connect computers together
- Can connect computers within an office (LAN) or to the global internet

Local Area Networks (LANs)

- Connect devices in the same building
- LANs are connected to **Wide Area Networks (WANs)**

Wide Area Networks (WANs)

- Connect across large distances
- Connects to different office locations and also to the internet
- When an **LAN is connected to WAN = Internet**

How Devices Connect to a LAN

1. Ethernet
    - Connecting a physical Ethernet cable to an internet jack behind the ball
    - The Ethernet Cable is called the **RJ-45** connectors a.k.a **8 Pins Connector**
    - Super fast but requires physical cables
    - FYI: RJ-11 Cables are used for telephone connections. They have 6 Pins
2. Wireless Networks (Wi-Fi)
    - Create **Wireless LANs**
3. Bluetooth
    - Creates a Personal Area Network (**PAN**s)
    - Designed to support a single person
    - Main purpose is to create a wireless connection between a computer and its peripheral devices
4. **Near Field Communication (NFC)** Technology
    - Allows **extremely short** range wireless connections (ex= wireless payment)

TCP/IP - Transmission Control Protocol/Internet Protocol

- A set of standardized rules that allow computers to communicate on a network such as the internet.
- Protocol suite at the **heart of networking**

Internet Protocols

- Main function is **to provide an addressing scheme, known as the IP address**
- Routes information across networks
- Not just used on the internet
- Can be used at home or an office
- Deliver packets(chunks of information) from source → destination
- Serves as a **Network Layer Protocol**
    - Supports Transport Layer Protocols - which have a higher set of responsibilities

2 Types of Transport Layer Protocols

1. Transmission Control Protocol (TCP)
    - Responsible for majority of internet traffic
    - Is a **Connection-Oriented protocol**

- Connection Oriented protocol means the **connection is established before** data is transferred
- Connection is ensured through TCP Three-Way Handshake

    - TCP packets include special flags that identify the packets known as **TCP Flags**. Within the TCP Flags:

        - SYN Flag: Opens a connection
        - FIN Flag: Closes an existing connection
        - ACK: Used to acknowledge a SYN or FIN packet

TCP Three-Way Handshake

1. Source SYN sent to request open connection to Destination
2. Destination sends ACK + request (SYN) to reciprocate a open connection
3. Source acknowledges and sends ACK

- Guarantees delivery through the destination system acknowledging receipt
- Widely used for critical applications (email , web traffic etc)

2. User Datagram Protocol (UDP)

- **Connectionless Protocol**, not connection-oriented
- Lightweight
- Does NOT use Three-Way Handshake
- System basically send data off to each other blindly, hoping that it is received on the other end
- Does not perform acknowledgments
- Does not guarantee delivery
- It's often used for **voice and video applications** where guaranteed delivery is not essential. Every single packet doesn't have to reach the destination for video and voice to be comprehensible.

OSI (Open Systems Interconnection) Model

- Describes networks as having 7 different layers

Layer 1: Physical Layer

- Responsible for sending bits over the network
- Uses wires, radio waves, fiber optics or other means

Layer 2: Data Link Layer

- Transfers data between 2 Nodes connected to the same physical network

Layer 3: Network Layer

- Expands networks to many different nodes
- **Internet Protocol (IP)**

Layer 4: Transport Layer

- Creates connection between systems
- Transfers data in a reliable manner
- **TCP and UDP**

Layer 5: Session Layerauthenti

- Manages the exchange of communications between systems

Layer 6: Presentation Layer

- Translates data so that it may be transmitted on a network
- Encryption and Decryption

Layer 7: Application Layer

- How users interact with data, using web browsers or other apps

TCP Model vs OSI Model

OSI	TCP Model
Layer 1: Physical Layer	
Layer 2 :Data Link Layer	Layer 1: Network Interface layer (Physical + Data)
Layer 3 :Network Layer	Layer 2: Internet Layer
Layer 4 :Transport Layer	Layer 3: Transport Layer
Layer 5: Session Layer	Layer 4: Application Layer (Session+Presentation+Application)
Layer 6: Presentation Layer	
Layer 7: Application Layer	

_____

For the **Internet Protocol (IP)** to successfully **deliver traffic** between any two systems on a network, it has to use an **addressing scheme**

IP Addresses

- Uniquely identify systems on a network
- Written in **dotted quad notation** (ex- 192.168.1.100). Also known as **IPv4**
    - Means 4 numbers separated by periods
    - Each of these numbers may range between **0-255**
        - Why 255?
            - Each number is represented by 8-bit binary numbers
            - Those bits can represent 2 to the power of 8 = 256 possible values
            - But we start at 0 so 256-1=255
- No duplicates of IP addresses on Internet-connected systems (Just like your phone#)
- Allow duplicates if on private networks
    - Your router or firewall takes care of translating private IP Addresses to public IP addresses when you communicate over the internet
    - This translating process is called **NAT (Network Address Translation)**
- IP Addresses are divided into **2 parts**
    - 1) Network Address
    - 2) Host Address

The divide of the 2 parts can come in anywhere

This uses a concept called **sub-netting**

- Sub-netting divides domains so traffic is routed efficiently

- IPv4 (Containing 4 numbers) is running out so we are shifting to → **IPv6**
    - **IPv6**
        - Uses 128 bits (compared to 32 bits (8x4num bers = 32) for IPv4
        - Consists of 8 groups of 4 hexadecimal numbers
            - ex= fd02:24c1:b942:01f3:ead2:123a:c3d2:cf2f

IP Addresses can be assigned in 2 ways

1. Static IPs
    - **Manually** assigned IP Address by an administrator
    - Must be unique
    - Must be within appropriate range for the network
2. Dynamic Host Configuration Protocol (DHCP)
    - **Automatic** assignment of IP Address from an administrator configured pool

Typically,
Servers are configured with **Static IP Addresses**
End-user devices are configured with **Dynamically-Changing IP Addresses**

_____
Network Ports

- Like Apartment #s, guide traffic to the correct **final destination**
- IP addresses uniquely identifies a system while the Network Ports uniquely identifies a particular location of a system associated with a specific application
- Think of it as
    - IP Addresses - Street # of an Apartment
    - Network Ports- Unit # of an Apartment

Network Port Numbers

- **16-bit** binary numbers
- 2 to the power of 16 = 65,646 possible values
    - 65,646-1 (for 0) = 0-**65,535** possibilities

Port Ranges

- 0 - 1,023 = Well-known ports
    - Reserved for common applications that are assigned by internet authorities
    - Ensures everyone on the internet will know how to find common services such as : web servers, email servers
        - **Web-servers** use the Well-known **port 80**
        - **Secure Web-servers** use the Well-known **port 443**

-

- 1,024 - 49,151 = Registered ports
    - Application vendors may register their applications to use these ports
        - Examples
            - Microsoft Reserve port 1433 for SQL Server database connections
            - Oracle Reserve port 1521 for Database
- 49,152 - 65,535 = Dynamic ports
    - Applications can use on a temporary basis

Important Port #s

Administrative Services

- Port 21 : File Transfer Protocol (FTP)
    - Transfers data between systems
- Port 22 : Secure Shell (SSH)
    - Encrypted administrative connections to servers
- Port 3389 : Remote Desktop Protocol (RDP)
    - Encrypted administrative connections to servers
- Ports 137, 138, and 139 : NetBIOS - Windows
    - Network Communications using the NetBIOS protocol
- Port 53 : Domain Name Service (DNS)
    - All systems use Port 53 for DNS lookups

Mail Services

- Port 25 : Simple Mail Transfer Protocol (SMTP)
    - Exchange email between servers
- Port 110 : Post Office Protocol (POP)
    - Allows clients to retrieve mail
- Port 143 : Internet Message Access Protocol (IMAP)
    - Allows to retrieve mail

Web Services

- Port 80 : Hypertext Transfer Protocol (HTTP)

- For unencrypted web communications

- Port 443: Secure HTTP (HTTPS)
    - For encrypted connections

Securing Wireless Networks

Service Set Identifier (SSID)

- The name of your Wi-Fi
- You can disable visibility of Wi-Fi (Hide)
- Has an administrative password to the access point (connection)
- Ensure to immediately change default administrator passwords
- You can configure what Type of Network you want
    - 1) Open Network
        - Open for anyone to use (No Password Wifi)
    - 2) Other authentication required Network
        - 1) Preshared Keys (Home Wifi, Office, Cafe)
            - Changing Preshared keys is difficult
            - Prevents individual identification of users
        - 2) Enterprise Authentication
            - Uses individual passwords
    - 3) Captive Portals
        - Used in Starbucks, Airports, Tim-Hortons
        - Provide authentication on unencrypted wireless networks
        - Intercepts web requests to require Wi-Fi login

Wireless Encryption

- A best practice for network security
- Encryption hides the true content of network traffic from those without the decryption key
- Takes, Radio Waves, and makes it secure

The **Original** approach to Security was: **Wired Equival7ent Privacy (WEP)**

- This is now considered **insecure**

The **Second** approach was : **Wi-Fi Protected Access (WPA)**

- Changes keys with the Temporal Key Integrity Protocol (TKIP)
- Changes the encryption key for each packet : preventing an attacker from discovering the key after monitoring the network for along period of time
- This is now considered **insecure**

The **Improved** approach is : **Wi-Fi Protected Access v2 (WPA2)**

- Uses an advanced encryption protocol called **Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP)**
- **WPA is now considered SECURE**

The **New** approach is : **Wi-Fi Protected Access v3 (WPA3)**

- Supports **Simultaneous Authentication of Equals (SAE)**
    - SAE is a secure key exchange protocol based upon the Diffie-Hellman Technique, to provide more secure initial setup of encrypted wireless communications
- Also supports CCMP protocol

In Summary,
Open Network : Insecure
WEP : Insecure
WPA: Insecure
WPA2 : Secure
WPA3: Secure

Ping and Traceroute
Command Line Network (CLI)

- Provides quick and **easy way to access network configurations** and **troubleshooting** information
- Used my giving **Commands**

Important Commands

1. **ping**
    - Checks whether a remote system is **responding** or accessible
    - Works using the Internet Control Message Protocol (ICMP)
        - Basically sending a request and acknowledgement to confirm a connection
        - Troublingshooting with Ping:
            - You can ping the remote system:
                - a) if you receive a response : it is not a network issue and a local web server issue
                - b) if you don't receive a response : you may next ping *another system* located *on the internet* : if that responds : this will tell you your internet is successful and the issue is with the web server or network connection
                - c) if you ping many systems on internet and there is no response, it is likely that the problem is on your end
                - d) You can ping a system on your Local Network : if that responds, there's probably an issue with your network's connection to the internet
                - e) If a Local Network does not respond : Either your Local network is down or there is a problem with your computer
                - f) Last Resort : Repeat process on another computer

- Some systems do not respond to ping requests
    - Example : A firewall may block ping requests

2. **hping**
    - Creates customized ping requests
    - A variant of the basic “ping” command
    - Allows you to interrogate a system to see if it is present on the network
    - Old and not monitored but still works

3. **traceroute**
    - Determines the **network path** between two systems
    - If you want to know how packets are traveling today from my system Located in Toronto to a LinkedIn.com webserver, wherever that is located
    - Works only on **Mac and Linux**
    - In **Windows**, it is : **tracert**

4. **pathping**
    - **Windows only** command
    - Combines ping and tracert functionality in a single command

---

Network Threats

Malware

- One of the most significant threats to computer security
- Short for Malicious Software
- Might steal information, damage data or disrupt normal use of the system
- Malwares have 2 components:
    - 1) **Propagation Mechanism**
        - Techniques the malware uses to spread from one system to another
    - 2) **Payload**
        - Malicious actions taken by malware
        - Any type of malware can carry any type of payload

Types of Malware

1. Virus
    - Spreads **after** a user takes some type of **user action**
        - Example : Opening an email attachment, Clicking a Link, Inserting an infected USB
    - Viruses do not spread unless someone gives them a hand
    - *User education protects against viruses*

2. Worms

- Spread on their **own** by exploiting vulnerabilities
- When a worm infects a system, it will use it as it's base for spreading to other parts of the Local Area Network
- Worms spread because the systems are vulnerable
- *Patching protects against worms*

3. Trojan Horse

- **Pretends** to be a useful legitimate software, with **hidden malicious effect**
- When you run the software, it may perform as expected however will have **payloads** behind the scene
- *Application Control protects against Trojan Horses*

- Application Controls limit software that can run on systems to titles and versions

Botnets

- Are a collection of **zombie computers** used for malicious purposes
- A network of infected systems

- Steal computing power, network bandwidth, and storage capacity
- A hacker creating a botnet begins by

- 1) Infecting a system with malware through any methods
- 2) Once the malware takes control of the system (hacker gains control), he or she joins/adds it to the preconceived botnet

How are Botnets Used

- Renting out computing power for profit
- Delivering spam
- Engaging in DDoS attacks
- Mining Bitcoin and Cryptocurrencies
- Perform Brute Force Attacks - against passwords

Botnet Command and Control

- Hackers command botnets through Command and Control Networks as they relay orders
- Communication **must be indirect** (hides the hackers true location) and redundant
- Must be highly redundant (too much, alot) because security analysts will shut them down one by one. Its a *cat and mouse game, whoever controls the Command and Control channels retains control of the Botnet the longest*

Types of Command and Control Mechanisms for Ordering Botnets

- Internet Relay Chat (IRC)
- Twitter
- Peer to Peer within the Botnet

In Summary Botnets:

1. Infect Systems
2. Convert to bots
3. Infect others
4. Check in through Command and Control Network

5. Get Instructions
6. Deliver payload

Eavesdropping Attacks

- All eavesdropping attacks rely on a compromised communication path between a client and a server
    - Network Device Tapping
    - DNS poisoning
    - ARP poisoning
- During poisoning attacks hackers may use the Man-in-the-Middle technique to trick the user to connect to the attacker directly, then the attacker directly connects to the server. Now the original user logs in to a fake server set up by the attacker and the attacker acts as a relay, the man in the middle, and can view all of the communications.
- The user will not know that there is a Man-in-the-Middle intercepting communications.

Man-in-the-browser Attacks

- Variation of Man-in-the-Middle attack
- Exploit flaws in browsers and browser plugins to gain access to web communications

*If the attacker is able to control the network traffic, they may be able to conduct a **Reply Attack***
Replay Attack

- Uses previously captured data, such as an encrypted authentication token, to create a separate connection to the server that's authenticated but does not involve the real end user
- The attacker cannot see the actually encoded credentials
- They can only see the encoded version of them
- Prevent Replay Attacks by including unique characteristics:
    - Token
    - Timestamp

SSL Stripping

- Tricks browsers into using unencrypted communications
- A variation of eavesdropping attack
- A hacker who has the ability to view a user's encrypted web communication exploits the vulnerability to **trick the users browser** into **reverting** to **unencrypted** communications for the world to see
- Strips the SSL or TLS protection

Implementation of Attacks
Cryptographic systems may have flaws = vulnerability = attacks
Fault Injection Attacks

- Use externally forced errors
- Attacker attempts to compromise the integrity of a cryptic device by causing some type of external fault

- For example : Attacker might use high-voltage electricity to cause malfunction that undermines security

- These failures of security may cause systems to fail to encrypt data property.

Side Channel Attacks

- Measure **encryption footprints**
- Attackers use footprints monitor system activity and to retrieve information that is actively being encrypted

    - For example : If a cryptographic system is improperly implemented, it may be possible for an attacker to capture the electromagnetic radiation emanating from that system and use the collected signal to determine the plain text information that is being encrypted
    - **Timing Attacks**

        - A type of Side Channel Attack
        - Measure **encryption time**
        - Attackers precisely measures how long cryptographic operations take to complete, gaining information about cryptographic process that may be used to undermine security

---

Threat Identification and Prevention

Intrusion Detection Systems (IDS)

- Monitors network traffic for signs of malicious activity
- MIS USE DETECTION AND ANOMALY DETECTION

    - Examples of malicious activity

        - SQL Injections
        - Malformed Packets
        - Unusual Logins
        - Botnet Traffic

- Alerts administrators
- Requires someone to take action

Intrusion Prevention System (IPS)

- Automatically block malicious activity
- It is not a perfect system. They make **2 errors**

        - 1) False Positive Error

            - IDS/IPS triggers an alert when an attack did not actually take place

        - 2) False Negative Error

            - IDS/IPS fails to trigger an alert when an actual attack occurs

Technology used to identify suspicious traffic:

1. Signature Detection Systems

- Contain databases with rules describing malicious activity
- Alert admins to traffic matching signatures = **Rule based Detection**
- Cannot detect brand new attacks

    - Reduce false positive rates

- Reliable and time-tested technology

2. Anomaly Detection Systems

    - Builds models of “normal” activity, and finds an **Outlier**
    - Can detect brand ne attacks

        - But has high false positive rate
        -

Anomaly Detection , Behavior-based Detection , Heuristic Detection = Same Thing

---

IPS Deployment Modes

1. In-band Deployments

    - IPS sits **in the path** of network traffic
    - It can block suspicious traffic from entering the network
    - Risk : It is a single point of failure so it may disrupt the entire network

2. Out-of-band (passive) Deployments

    - IPS sits **outside** of network traffic
    - IPS is connected to a SPAN port on a switch

        - Which allows it to receive copies all traffic sent through the network to scan
        - It cannot disrupt the flow of traffic

    - It can **react** after suspicious traffic enters the network
    - It cannot pre detect as it can only know its existence once it enters the network

---

Malware Prevention

- Antimalware software protects against many different threats
- Antimalware software protects against viruses, worms, Trojan Horses and spyware

Antivirus software uses **2 types** of mechanisms to protect:

1. Signature Detection

    - Watches for **known patterns** of malware activity

2. Behavior Detection

    - Watches for **deviation**s from normal patterns of activity
    - This type of mechanism is found in advanced malware protection tools like the **Endpoint Detection and Response (EDR)**

- Offer real-time, advanced protection
- Goes beyond basic signature detection and performs deep instrumentation of endpoints
- They analyze:
    - Memory
    - Processor use
    - Registry Entries
    - Network Communications
- Installed on Endpoint devices
- Can perform **Sandboxing**
    - Isolates malicious content

Port Scanners
Vulnerability Assessment Tools

1. Port Scanner
    - Looks for open network ports
    - Equivalent of rattling all doorknobs looking for unlocked doors
    - **nmap**
        - Popular port scanning tool /command
2. Vulnerability Scanner
    - Looks for known vulnerabilities
    - Scans deeper than Port Scanner, actually looks at what services are using those ports
    - Has a database for all known vulnerability exploits and tests server to see if it contains any of those vulnerabilities
    - **Nesssus**
        - Popular vulnerability scanner
3. Application Scanner
    - Tests deep into application security flaws

Network Security Infrastructure
Data Centers

- Have significant cooling requirements
- Current Standard of Temperatures
    - Maintain data center **air temperatures between 64.6 F and 80.6 F** = Expanded Environmental Envelope
- Humidity is also important
    - Dewpoint says : **Humidity 41.9 F and 50.0 F**
        - This temperature prevents condensation and static electricity

- HVAC is important (Heating, Ventilation and Air Conditioning Systems)
- Must also look out for fire, flooding, electromagnetic interference

Fire Suppression Methods

1. Wet Pipe Systems
    - Contains water in the pipes ready to deploy when a fire strikes
    - High Risk for data center
2. Dry Pipe Systems
    - Do not contain water **until** the valve opens during a **fire alarm**.
    - Prevents burst pipes, by removing standby water
3. Chemical Systems
    - Removes oxygen

Always place **MOUs**

- Memorandum of Understanding
- Outlines the environmental requirements

Security Zones

- Firewalls divide networks into security zones to protect systems of differing security models

Types of Security Zones

1. Network Border Firewall
    - Three network interfaces, connects **3**:
        - Internet
        - Intranet
            - Data Center Network
            - Guest Network
            - Wireless Network
            - Endpoint Network
        - DMZ
            - You can place systems that must accept connections from the outside world such as mail, web servers
            - Because it is open, higher risk of compromise
            - If the DMZ is compromised, firewalls will still protect

Zero Trust Approach : Systems do not gain any trust based solely upon their network location
3 Special-Purpose Networks

1. Extranet

- Special intranet segments that are accessible by outside parties like business partners

2. Honeynet
    - Decoy networks designed to attract attackers
3. Ad Hoc Networks
    - Temporary networks that may bypass security controls

East-West Traffic

- Network traffic **between** systems located in **data center**

North-South Traffic

- Networks traffic **between** systems in the **data center** and systems on the **Internet**

Routers and Switches
Routers, **Switches** and **Bridges** are the building blocks of computer networks
Switches

- Connect devices to the network
- Has many network ports
- Reside in wiring closets and connect the computers in a building together
- Ethernet jacks are at the other end of network cables connected to switches
- Wireless access points (WAPs) connect to switches and create Wi-Fi networks
    - The Physical APs itself has a wired connection back to the switch
- **Switches can only create Local Networks**
- **Layer 2 of OSI Model - Data Link Layer**
- **Some** switches can be in the **Layer 3 of OSI Model - Network Layer** (can interpret IP Addresses)
    - For this to happen, they must use **Routers**

Routers

- Connect networks to each other, making intelligent packet routing decisions
- Serves as a central aggregation point for network traffic heading to or from a large network
- Works as the air traffic controller of the network
- Makes best path decisions for traffic to follow
- Use Access Control Lists to limit some traffic that are entering or leaving a network, this type of filtering does not pay attention to Connection states and are called

Stateless Inspection

Virtual LANs (VLANs)

- Separates systems on a network into logical groups based upon function
- Extend broadcast domain

- Users on the same VLAN will be able to directly contact each other as if they were connected to the same switch

- We use VLANs to create **network segmentation** which reduces security risk by liming the ability of unrelated systems to communicate with each other
- **Micro Segmentation**

  - Extreme segmentation strategy
  - Temporary

Configuring VLANs

1. Enable VLAN trunking

   - Allow switches in different locations on the network to carry the same VLANs

2. Configure VLANs for each switch port

———

Firewalls

- Often sit at the network perimeter
- Between Router and Internet

Switch
I
I
I
Switch —---------- Router —---------- Firewall —---------- Internet
I
I
I
Switch
Firewalls connect 3 networks together

1. Internet
2. Internal Network
3. DMZ

   - Contains systems that must accept direct external connections
   - Isolates those systems due to risk of compromise
   - Protects internal network from compromised DMZ systems

Older Firewalls use **Stateless Firewalls**

- Evaluate each connection independently

Modern Firewalls use **Stateful Inspection**

- Keeps track of established connection

Firewalls are basically rules to enter or exit.
Firewall rule must provide

1. Source system address

2. Destination system address
3. Destination port and protocol
4. Action (Allow or Deny)

Firewalls operate on the **Principle of Implicit Deny**

- If the firewall receives traffic not explicitly allowed by a firewall rule, then that traffic must be blocked
- Basically saying, if you don't have a passcard, you cannot get in as the door is always closed

The Newest type of Firewalls are called **New Generation Firewalls (NGFW)**

- Incorporate **contextual information** into their decision making
- Evaluate requests based on identity of user, nature of application, time of day etc.

Other Firewall Roles

1. Network Address Translation (NAT) Gateway
    - The firewall translates between the public IP Addresses used on the internet and private IP Addresses used on the local networks
2. Content/URL Filtering
3. Web application firewall
    - Understands how HTTP protocol works and dive deep into those application connections, looking for signs of SQL Injection, Cross-site scripting, and other web application attacks

Firewall Deployment Options

1. Choose deployment methodology
    1. Network Hardware
        - Physical devices that sit on a network and regulate traffic
    2. Host-Based software Firewalls
        - Software applications that reside on a server that performs other functions

Most organizations choose to use both network firewalls

2) Choose between Open-source Vs Proprietary technology

- Network Hardware are always Proprietary
- Software Firewalls may be either Proprietary or Open Source

3) Choose Deployment Mechanism

1. Hardware Appliance
2. Virtual Appliance

VPNs and VPN Concentrators
VPNs provide **2** security functions:

1. Site-to-Site VPNs
    - Connect remote offices to each other and headquarters
    - Ex= Branch → HQ
2. Remote Access VPNs
    - Provide remote access to corporate networks for **mobile users**

VPNs

- Works by using encryption to create a virtual tunnel between two systems over the internet
- Everything on one tunnel is encrypted and decrypted when it exits
- VPNs require an **endpoint** that **accepts** VPN connections
- **Endpoints** can be many things:
    - Firewalls
    - Router
    - Server
    - Dedicated VPN Concentrators - **Used for High Volume**

Firewalls, Router, Server does not contain specialized hardware that accelerates Encryption

IPSec (Internet Protocol Security) Protocol

- Creates encrypted tunnels
- Works at Layer 3 : Network Layer
- Supports Layer 2 Tunneling Protocol (L2TP)
- Provides secure transport
- Difficult to configure
- **Often used for Static Site-to-Site VPN Tunnels**

SSL/TLS VPNs

- Works at the Application Layer over TCP port 443
- Works on any system on a web browser
- Port 443 = Almost bypass any firewall

HTML5 VPNs

- Work entirely within the web browser
- A remote access VPN

When implementing a remote Access VPN admins must choose :

1. Full Tunnel VPN
    - All network traffic leaving the connected device is routed through the VPN tunnel, regardless of final destination
2. Split Tunnel VPN

- Only traffic destined for the corporate network is sent through the VPN tunnel
- Other traffic is routed directly over the Internet (risk of eavesdropping)
- Not as safe so not recommended

Split-Tunnel VPN provides users with a **false sense of security**
Always on VPN

- Connects automatically
- Takes control from the user
- Always protected by strong encryption

Network Access Control (NAC)

- Intercepts network traffic coming from unknown devices and verifies that the system and users are authorized before allowing further communication
- Uses **802.1x authentication.** This requires 3 devices

    1. Supplicant - Device that sends request
    2. Authenticator - The switch
    3. Authentication Server - Backend

Supplicant(Sends credentials) → Authenticator(Receives and passes it to AS) → Authenticator Server (authenticates and sends results to authenticator → Authenticator → Supplicant → Access
NAC Roles

1. User and device authentication (what we discussed above)
2. Role-based access

    - Once authenticator learns the identity of requested user it places the user in the network based upon that user's identity

3. Posture checking/Health Checking

    - Before granting access, it check for compliance requirements

        - Validating current signatures
        - Verifying for antivirus presence
        - Ensuring proper firewall configuration
        - If it Fails the posture check

            - It will be placed into a quarantine VLAN where they will have limited internet access and no access to internal resources

        - Posture checking is done through an Agent or Agentless

---

Internet of Things

- Smart devices

IOT Security Challenges

- Difficult to update

- Connect to home and office wireless (Risk for malicious actors)
- Connects back to cloud services for command and control, creating a pathway for external attackers

Security of IOT

- Check for weak default passwords
- Make sure to regularly update and patch
- Some have Automatic Updates and some require Manual Websites
- If worried get **Firmware Version Control**
    - Updates are applied in orderly fashion
- **Security Wrappers** (For organizations that must run vulnerable systems)
    - Mini firewall for devices
    - Device is not directly reached through network
    - Only process vetted requests
- Most secure way is **Network Segmentation** - isolating network to a isolated section where they will not have access to trusted networks
- Application firewalls provide added protection for embedded devices

Network Segmentation is the ***most important*** control for ***embedded devices***

Cloud Computing

Cloud Computing

- Delivering computing resources to a remote customer over a network
- Official Definition: A model for enabling ubiquitous, convenient, on-demand network access to shared pool of configurable computing resources (networks, servers, storage, applications, services) that can be rapidly provisioned and released with menial management effort or service provider interaction

Cloud Service Categories

1. Software as a Service (SaaS)
    - Customer purchases an entire app
2. Infrastructure as a Service (IaaS)
    - Customer purchase servers/storage and create their own IT solutions
3. Platform as a Service (PaaS)
    - Customer purchases app platform

Cloud Deployment Models

1. Private Cloud
    - Dedicated Cloud Infrastructure
2. Public Cloud

- Organization uses a multi-tenancy infrastructure (Shared)

3. Hybrid Cloud
    - Uses both Private and Public
4. Multi Cloud
    - Combines resources from two different public cloud vendors (AWS + Azure)
5. Community Cloud
    - Shared Consortium

No cloud model is inherently superior to other approaches. It all depends on context

---

Managed Service Providers (MSPs)

- Offer information technology services to customers

Managed Security Service Providers (MSSPs)

- Provide security services for other organizations as a manage service
- Must be carefully monitored
- Lot of service
    - Manage an entire security infrastructure
    - Monitor system logs
    - Manage firewalls
    - Manage Access & Identity Management
- MSSPs are also known as **Security as a Service (SECaaS)**

Cloud Access Security Brokers (CASB)

- Add a third-party security layer to the interactions that users have with other cloud services
- Works in 2 ways
    - 1) Network-Based CASB
        - Broker intercepts traffic between the user and the cloud service, monitoring for security issues
        - Broker can block request
    - 2) API- Based CASB
        - Does not sit on traffic unlike Network-Based CASB
        - The broker queries the cloud service via API
        - Broker may not be able to block requests, depending upon API capabilities

---

Vendor Relationship Management

- Ensure that vendor security policies are at least as stringent as your own
- Vendor lock-in makes it difficult to switch vendors down the road. So be careful
- Conduct due diligence
- Socialize with team
- Present to stakeholders
- Schedule weekly meetings

Steps of Vendor Selector

1. Vendor Selection
    - Due Diligence
2. Onboarding
    - Verify details of contract
    - Confirm security incident notification
3. Monitoring
4. Offboarding

Vendor Agreements
Non-Disclosure Agreements (NDA)

- Keep your mouth shut

Service-Level Requirements (SLR)

- Document specific requirements that a customer has about any aspect of a vendor's service performance
- Once agreed sign the **Service Level Agreement (SLA)**

Memorandum of Understanding (MOU)

- A letter that documents aspects of relationship
- Commonly used when a legal dispute is unlikely but customer and vendor wish to document their relationship to avoid future misunderstanding
- Usually used when a department another company is dealing with another department

Business Partnership Agreement (BPA)

- Partnership agreement to conduct business

Interconnection Security Agreement (ISA)

- Details that two organizations will interconnect their network

Master Services Agreement (MSA)

- Big project - documentation of expected services

- Statement of Work (SOW) is used when another project comes up
- SOW is governed by terms in MSA. SOW is like am abeyance or patch

Ensure Security Requirements are mentioned in all agreements

Data Security
Encryption

- Uses math to make data unreadable to unauthorized individuals
- Transforms text from plaintext to **ciphertext**
- Uses decryption algorithm key to read message

You can use Encryption in 2 different environments:

1. Data at Rest
    - Stored data
    - Can be in:
        - File
        - Disk
        - Device
2. Data in Transit
    - Data that is moving
    - HTTPS
    - Email
    - Mobile Applications
    - VPN (Network)

Symmetric vs Asymmetric Cryptography
Symmetric Encryption

- You encrypt and decrypt with the **same** shared secret key
- It's like a password to a message
- You will keep needing more keys as network populates

Asymmetric Encryption

- You encrypt and decrypt with **different keys** from the same pair

Keys used for Asymmetric encryption and decryption (public & private) ***must be from the same pair***
Advanced Encryption Standard (AES) → Symmetric
Rivest-Shamir-Adleman (RSA) → Asymmetric

Hash Functions

- One-way function that transforms a variable length input into a unique, fixed-length output

- One-way function = Cannot be reversed
- The output of a hash function will always be same length, regardless of input size
- No two inputs to a hash function should produce the same output

All criterias above must be met to have an effective Hash Function
2 Ways Hash Function can **fail**:

1. If they are reversible
2. If they are not collision-resistant

Common Hash Functions
You must know which functions are considered insecure and which remain secure

1. Message Digest 5 (MD5)

    - Ron Rivest created MD5 in 1991
    - MD5 is the 5th series of hash functions
    - Message digest is another term for hash
    - MD5 produces 128-bit hashes
    - MD5 is **no longer secure**

2. SHA-1

    - Produces a 160-bit hash value
    - Contains security flaws
    - SHA-1 is no longer secure

3. SHA-2

    - Replaced SHA-1
    - Consists of a family of 6 has functions
    - Produces output of 224, 256, 384 and 512 bits
    - Uses a mathematically similar approach to SHA-1 and MD5
    - SHA-2 is **no longer secure**

4. SHA-3

    - Designed to replace SHA-2
    - Uses a completely different has generation approach than SHA-2
    - Produces hashes of user-selected fixed strength
    - Some people do not trust SHA algorithms because NSA created it

5. RIPEMD

    - Created as an alternative to government-sponsored hash functions
    - Produces 128, 160, 256, and 320-bit hashes
    - Contains flaws in the 128-bit version
    - 160 bit is widely used. Even in **Bitcoin**

Hash Based Message Authentication Code (HMAC)

- **Combines symmetric** cryptography and **hashing**
- Provides authentication and integrity
- Create and verify message authentication code by using a secret key in conjunction with a hash function

---

Data Lifecycle

- Explains the different stages of data in the cloud

Cycle

1. Create
2. Store
3. Use
4. Share
5. Archive
6. Destroy

    - Must be done in a secured manner
    - Data Sanitization Techniques

        - Clearing overwrites sensitive information to frustrate causal analysis
        - Purging
        - Destroying, shredding, pulverization, melting and burning

_____

Data Classification

- Assign information into categories, known as classification, that determine **storage**, **handling**, and **access requirements**

Assign Classification Based Upon:

1. Sensitivity of Information
2. Criticality of Information

Classification Levels

1. High, Medium, Low
2. Public vs Private

Labeling Requirements

- Requirement to identify sensitive information

3 Types of Information classified by **External Groups**

1. Personally Identifiable Information (PII)

    - Traceable to a specific person

2. Protected Health Information (PHI)

    - Covered by ***HIPPA***

3. Payment Card Information (PCI)

    - Covered by ***PCI DSS***

_____

Logging and Monitoring

Logging establishes:

1. Accountability
    - Who caused the event
    - A.K.A Identity Attribution
2. Traceability
    - Uncover all other related events
3. Auditability
    - Provide clear documentation of the events

Realistically, logging data of a company can be overwhelming. **Artificial Intelligence** can help solve security data overload
Security Information and Event Management (SIEM) has **2** functions:

1. They act as a central secure collection point
    - All systems send log entries directly to the SIEM
    - Firewall log, Web server log, Database log, Router log, they are all sent to to SIEM where it will provide an overall picture
2. Source of Artificial Intelligence

Intrusion Detection System

- Triggers the initial alert

_____
Security Awareness and Training
Social Engineering

- Manipulating people into divulging information or performing an action that undermines security.

6 Reasons why Social Engineering works:

1. Authority
2. Intimidating
3. Consensus
4. Scarcity
5. Urgency
6. Familiarity

Education is the solution

_____
Impersonation Attacks
Spam

- Unsolicited commercial email
- Phishing
    - Phishing is a category of spam
    - Steales credentials

- Spear Phishing
    - Highly target phishing
    - Customized phishing attacks
- Whaling
    - Phishing targeted on executives
- Pharming
    - Using fake websites
- Vishing
    - Voice phishing

- Sda
    - Smishing and Spim
        - SMS and IM spam
    - Spoofing
        - Faking an identity

_____
Security Awareness Training

- Programs help educate user about risks

Security Training

- Provides users with the knowledge they need to protect the organization's security

Security Awareness

- Keeps the lessons learned during security training top of mind for employees. Reminder

Security Training Methods

- Instruction in on-site classes
- Integration with orientations
- Education through online computer-based training providers
- Participation in vendor-provided classroom training
- Implement Role-based training
- Consider frequency of training
- Review training materials regularly to ensure relevance

Use a Diversity of Training Techniques

- Phishing simulations
- Gamification
- Capture the Flag exercises