Fundamentals of Security

Objectives:

- 1.1 - Compare and contrast various types of security controls
- 1.2 - Summarize fundamental security concepts

- **Fundamentals of Security**
    - *Information Security*
        - Protecting data and information from unauthorized access, modification, disruption, disclosure, and destruction
    - *Information Systems Security*
        - Protecting the systems (e.g., computers, servers, network devices) that hold and process critical data
    - CIA Triad
        - *Confidentiality*
            - Ensures information is accessible only to authorized personnel (e.g., encryption)
        - *Integrity*
            - Ensures data remains accurate and unaltered (e.g., checksums)
        - *Availability*
            - Ensures information and resources are accessible when needed (e.g., redundancy measures)
    - *Non-Repudiation*
        - Guarantees that an action or event cannot be denied by the involved parties (e.g., digital signatures)

- *CIANA Pentagon*
  - An extension of the CIA triad with the addition of non-repudiation and authentication
- Triple A's of Security
  - *Authentication*
    - Verifying the identity of a user or system (e.g., password checks)
  - *Authorization*
    - Determining actions or resources an authenticated user can access (e.g., permissions)
  - *Accounting*
    - Tracking user activities and resource usage for audit or billing purposes
- Security Control Categories
  - Technical
  - Managerial
  - Operational
  - Physical
- Security Control Types
  - Preventative
  - Deterrent
  - Detective
  - Corrective
  - Compensating
  - Directive
- *Zero Trust Model*
  - Operates on the principle that no one should be trusted by default

- To achieve zero trust, we use the control plane and the data plane
  - *Control Plane*
    - Adaptive identity, threat scope reduction, policy-driven access control, and secured zones
  - *Data Plane*
    - Subject/system, policy engine, policy administrator, and establishing policy enforcement points

- **Threats and Vulnerabilities**
  - *Threat*
    - Anything that could cause harm, loss, damage, or compromise to our information technology systems
    - Can come from the following
      - Natural disasters
      - Cyber-attacks
      - Data integrity breaches
      - Disclosure of confidential information
  - *Vulnerability*
    - Any weakness in the system design or implementation
    - Come from internal factors like the following
      - Software bugs
      - Misconfigured software
      - Improperly protected network devices
      - Missing security patches
      - Lack of physical security

- Where threats and vulnerabilities intersect, that is where the risk to your enterprise systems and networks lies
  - If you have a threat, but there is no matching vulnerability to it, then you have no risk
  - The same holds true that if you have a vulnerability but there's no threat against it, there would be no risk
- *Risk Management*
  - Finding different ways to minimize the likelihood of an outcome and achieve the desired outcome

- **Confidentiality**
  - *Confidentiality*
    - Refers to the protection of information from unauthorized access and disclosure
    - Ensure that private or sensitive information is not available or disclosed to unauthorized individuals, entities, or processes
  - Confidentiality is important for 3 main reasons
    - To protect personal privacy
    - To maintain a business advantage
    - To achieve regulatory compliance
  - To ensure confidentiality, we use five basic methods
    - *Encryption*
      - Process of converting data into a code to prevent unauthorized access
    - Access Controls
      - By setting up strong user permissions, you ensure that only authorized personnel can access certain types data

- *Data Masking*
  - Method that involves obscuring specific data within a database to make it inaccessible for unauthorized users while retaining the real data's authenticity and use for authorized users
- Physical Security Measures
  - Ensure confidentiality for both physical types of data, such as paper records stored in a filing cabinet, and for digital information contained on servers and workstations
- Training and Awareness
  - Conduct regular training on the security awareness best practices that employees can use to protect their organization’s sensitive data

- **Integrity**
  - *Integrity*
    - Helps ensure that information and data remain accurate and unchanged from its original state unless intentionally modified by an authorized individual
    - Verifies the accuracy and trustworthiness of data over the entire lifecycle
  - Integrity is important for three main reasons
    - To ensure data accuracy
    - To maintain trust
    - To ensure system operability
  - To help us maintain the integrity of our data, systems, and networks, we usually utilize five methods
    - *Hashing*
      - Process of converting data into a fixed-size value

- Digital Signatures
  - Ensure both integrity and authenticity
- *Checksums*
  - Method to verify the integrity of data during transmission

- Access Controls
  - Ensure that only authorized individuals can modify data and this reduces the risk of unintentional or malicious alterations
- Regular Audits
  - Involve systematically reviewing logs and operations to ensure that only authorized changes have been made, and any discrepancies are immediately addressed

- **Availability**
  - *Availability*
    - Ensure that information, systems, and resources are accessible and operational when needed by authorized users
  - As cybersecurity professionals, we value availability since it can help us with the following
    - Ensuring Business Continuity
    - Maintaining Customer Trust
    - Upholding an Organization's Reputation
  - To overcome the challenges associated with maintaining availability, the best strategy is to use redundancy in your systems and network designs
    - *Redundancy*
      - Duplication of critical components or functions of a system with the

intention of enhancing its reliability

- There are various types of redundancy you need to consider when designing your systems and networks
  - *Server Redundancy*
    - Involves using multiple servers in a load balanced or failover configuration so that if one is overloaded or fails, the other servers can take over the load to continue supporting your end users
  - *Data Redundancy*
    - Involves storing data in multiple places
  - *Network Redundancy*
    - Ensures that if one network path fails, the data can travel through another route
  - *Power Redundancy*
    - Involves using backup power sources, like generators and UPS systems

- **Non-repudiation**
  - *Non-repudiation*
    - Focused on providing undeniable proof in the world of digital transactions
    - Security measure that ensures individuals or entities involved in a communication or transaction cannot deny their participation or the authenticity of their actions
  - *Digital Signatures*
    - Considered to be unique to each user who is operating within the digital domain
    - Created by first hashing a particular message or communication that you want to digitally sign, and then it encrypts that hash digest with the user's private key using asymmetric encryption

- Non-repudiation is important for three main reasons
  - To confirm the authenticity of digital transactions
  - To ensure the integrity of critical communications
  - To provide accountability in digital processes

- **Authentication**
  - *Authentication*
    - Security measure that ensures individuals or entities are who they claim to be during a communication or transaction
  - 5 commonly used authentication methods
    - Something you know (Knowledge Factor)
      - Relies on information that a user can recall
    - Something you have (Possession Factor)
      - Relies on the user presenting a physical item to authenticate themselves
    - Something you are (Inherence Factor)
      - Relies on the user providing a unique physical or behavioral characteristic of the person to validate that they are who they claim to be
    - Something you do (Action Factor)
      - Relies on the user conducting a unique action to prove who they are
    - Somewhere you are (Location Factor)
      - Relies on the user being in a certain geographic location before access is granted
  - *Multi-Factor Authentication System (MFA)*
    - Security process that requires users to provide multiple methods of identification to verify their identity

- Authentication is critical to understand because of the following
  - To prevent unauthorized access
  - To protect user data and privacy
  - To ensure that resources are accessed by valid users only

- **Authorization**
  - *Authorization*
    - Pertains to the permissions and privileges granted to users or entities after they have been authenticated
  - Authorization mechanisms are important to help us with the following
    - To protect sensitive data
    - To maintain the system integrity in our organizations
    - To create a more streamlined user experience

- **Accounting**
  - *Accounting*
    - Security measure that ensures all user activities during a communication or transaction are properly tracked and recorded
  - Your organization should use a robust accounting system so that you can create the following
    - Create an audit trail
      - Provides a chronological record of all user activities that can be used to trace changes, unauthorized access, or anomalies back to a source or point in time
    - Maintain regulatory compliance
      - Maintains a comprehensive record of all users' activities

- Conduct forensic analysis
  - Uses detailed accounting and event logs that can help cybersecurity experts understand what happened, how it happened, and how to prevent similar incidents from occurring again

- Perform resource optimization
  - Organizations can optimize system performance and minimize costs by tracking resource utilization and allocation decisions
- Achieve user accountability
  - Thorough accounting system ensures users' actions are monitored and logged , deterring potential misuse and promoting adherence to the organization's policies

- To perform accounting, we usually use different technologies like the following
  - *Syslog Servers*
    - Used to aggregate logs from various network devices and systems so that system administrators can analyze them to detect patterns or anomalies in the organization's systems
  - *Network Analysis Tools*
    - Used to capture and analyze network traffic so that network administrators can gain detailed insights into all the data moving within a network
  - *Security Information and Event Management (SIEM) Systems*
    - Provides us with a real-time analysis of security alerts generated by various hardware and software infrastructure in an organization

- **Security Control Categories**
    - 4 Broad Categories of Security Controls
        - *Technical Controls*
            - Technologies, hardware, and software mechanisms that are implemented to manage and reduce risks
        - *Managerial Controls*
            - Sometimes also referred to as administrative controls
            - Involve the strategic planning and governance side of security
        - *Operational Controls*
            - Procedures and measures that are designed to protect data on a day-to-day basis
            - Are mainly governed by internal processes and human actions
        - *Physical Controls*
            - Tangible, real-world measures taken to protect assets

- **Security Control Types**
    - 6 Basic Types of Security Controls
        - *Preventive Controls*
            - Proactive measures implemented to thwart potential security threats or breaches
        - *Deterrent Controls*
            - Discourage potential attackers by making the effort seem less appealing or more challenging
        - *Detective Controls*
            - Monitor and alert organizations to malicious activities as they occur or

shortly thereafter

- *Corrective Controls*
  - Mitigate any potential damage and restore our systems to their normal state
- *Compensating Controls*
  - Alternative measures that are implemented when primary security controls are not feasible or effective
- *Directive Controls*
  - Guide, inform, or mandate actions
  - Often rooted in policy or documentation and set the standards for behavior within an organization

- **Gap Analysis**
  - *Gap Analysis*
    - Process of evaluating the differences between an organization's current performance and its desired performance
  - Conducting a gap analysis can be a valuable tool for organizations looking to improve their operations, processes, performance, or overall security posture
  - There are several steps involved in conducting a gap analysis
    - Define the scope of the analysis
    - Gather data on the current state of the organization
    - Analyze the data to identify any areas where the organization's current performance falls short of its desired performance
    - Develop a plan to bridge the gap

- 2 Basic Types of Gap Analysis
  - Technical Gap Analysis
    - Involves evaluating an organization's current technical infrastructure
    - identifying any areas where it falls short of the technical capabilities required to fully utilize their security solutions
  - Business Gap Analysis
    - Involves evaluating an organization's current business processes
    - Identifying any areas where they fall short of the capabilities required to fully utilize cloud-based solutions
  - *Plan of Action and Milestones (POA&M)*
    - Outlines the specific measures to address each vulnerability
    - Allocate resources
    - Set up timelines for each remediation task that is needed

- **Zero Trust**
  - Zero Trust demands verification for every device, user, and transaction within the network, regardless of its origin
  - To create a zero trust architecture, we need to use two different planes
    - Control Plane
      - Refers to the overarching framework and set of components responsible for defining, managing, and enforcing the policies related to user and system access within an organization
      - Control Plane typically encompasses several key elements
        - *Adaptive Identity*
          - Relies on real-time validation that takes into account the user's behavior, device, location, and more

- *Threat Scope Reduction*
  - Limits the users' access to only what they need for their work tasks because this reduces the network's potential attack surface
  - Focused on minimizing the "blast radius" that could occur in the event of a breach
- *Policy-Driven Access Control*
  - Entails developing, managing, and enforcing user access policies based on their roles and responsibilities
- *Secured Zones*
  - Isolated environments within a network that are designed to house sensitive data

- Control Plane uses a Policy Engine and a Policy Administrator to make decisions about access
  - *Policy Engine*
    - Cross-references the access request with its predefined policies
  - *Policy Administrator*
    - Used to establish and manage the access policies

- Data Plane
  - Consists of the following
    - *Subject/System*
      - Refers to the individual or entity attempting to gain access
    - *Policy Enforcement Point*
      - Where the decision to grant or deny access is actually executed