CompTIA Security+ (SY0-701) Day 1 Notes

Types of Security Control

Domain 1.0 General Security Concepts

Section 1.1 Security Control

- A **security control** is a safeguard or countermeasure prescribed for an information system to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

Security Control Categories

Managerial - Organizational policies and training

- Security education, training, and awareness programs
- A policy of least privilege
- Bring Your Own Device (BYOD) policies
- Password management policies
- Incident response plan (which will leverage other types of controls)
- Personnel management control (recruitment, account generation, etc.)

Technical - Technological solutions

- Antivirus and Anti-Malware Software
- Firewalls
- Security Information and Event Management (SIEM)
- Intrusion Detection System (IDS) and Intrusion Prevention System (IPS)

Operational - Day-to-day activities

- Controls that are primarily implemented and executed by people
- Everyone scanning their badge before entering
- Everyone using their phones for MFA
- Everyone reporting suspicious emails or texts
- Everyone locking their PCs before leaving their desk

Physical - Physical safety and security devices

- Motion or thermal alarm system
- Security guards
- Picture IDs
- Locked and dead-bolted steel doors
- Biometrics

Security Control Types

Preventive - Proactive controls which act to prevent loss

- Hardening
- Security Awareness Training
- Security guards
- Change Management
- Account Disablement Policy
- Bollards
- Access Control Vestibule
- Risk reduction before an incident happens (firewall, antivirus, etc.)
- Replacing a door lock with a stronger lock

Detective - Monitoring controls that detect, record, and alert

- Log monitoring
- Security Information and Event Management (SIEM)
- Trend analysis
- Security alerts
- Video surveillance
- Configuration management system that detects changes in settings
- Motion detection with sensors
- Controls in the Accounting Department to detect fraud
- Thermal regulators/monitors for HVAC

Corrective - Follow-up controls used to minimize harm caused and prevent recurrence

- Restoring backups and recovering systems
- Patching the system
- Making changes to an ACL
- Disabling a port or protocol
- Fire extinguishers or sprinklers

Deterrent - Visible controls designed to discourage attack or intrusion

- Cable locks
- Hardware locks
- Video surveillance and guards
- Fences
- Signs
- Bollards

Compensating - An unofficial control put in place that provides equivalent protection as an official control

- An alternative method that is put in place to satisfy the requirement for a security measure that cannot be readily implemented due to financial or infrastructure constraints, or it is impractical to implement at the present time
    - A managerial, operational, and/or technical safeguard employed by an organization in lieu of a recommended security control that provides equivalent or comparable protection for an information system
    - Example: a firewall rule until the official fix (patch) can be implemented

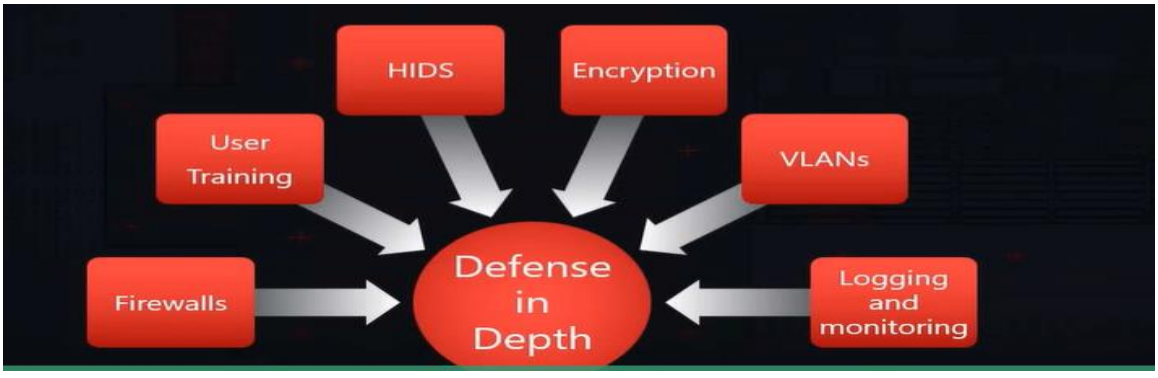
Directive - Typically prescriptive and provides clear instructions on how a security measure should be implemented or enforced

- Documents that:
    - Guide, mandate, and enforce
    - Security policies outlining what must be done
    - Security practices outlining what must be done
    - Security compliance requirements outlining what must be done

Section 1.2 Summarize Fundamental Security Concepts

Defense in Depth

- No security strategy should have a single point of failure
  Layering multiple, independent security controls increases the difficulty for attackers and the chances of detection



CIA Triad

Confidentiality

- Ensures that only individuals who have the authority to view or access a piece of information may do so
    - Encryption
    - Access Controls

Integrity

- Ensures that only individuals who have the authority to change a piece of information may do so, and that changes are verifiable
    - Checksums / Hash Functions
    - Digital Signatures / Certificates

Availability

- Ensures that the data, or the system itself, is available for use when the authorized user needs it

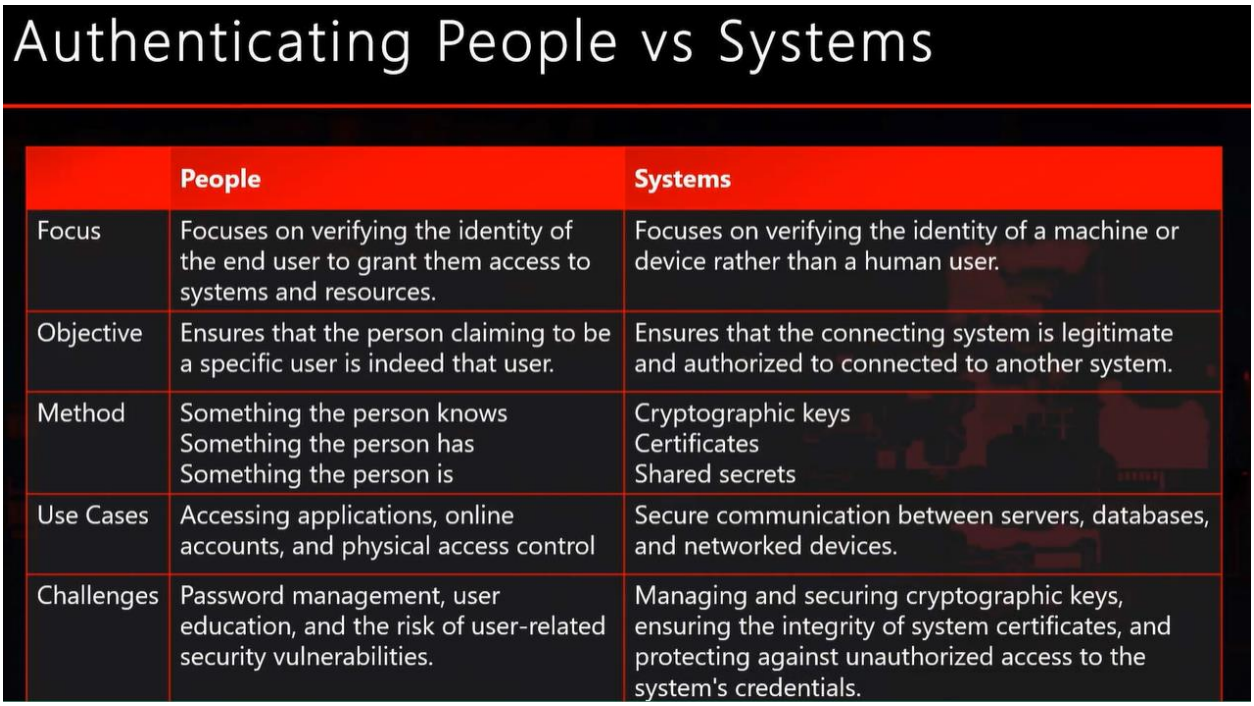
Extra: Non-Repudiation

- Ensures that no one can deny the authenticity of their signature or the validity of their actions

Authentication, Authorization, and Accounting (AAA)

Authentication

- Verifying the identity of someone or something



Authorization

- Defining what can and cannot be done after authentication
    - Authorization Models
        - Mandatory Access Control (MAC) – Access decisions are based on fixed security labels. Users cannot change access permissions.
        - Discretionary Access Control (DAC) – The resource owner decides who has access.
        - Role-Based Access Control (RBAC) – Access is granted based on roles within an organization.
        - Rule-Based Access Control (RuBAC) – Access is granted based on a set of rules defined by the system administrator.
        - Attribute-Based Access Control (ABAC) – Access is granted based on attributes (e.g., user, resource, environment conditions).

Accounting

- Recording and tracking every action that is performed

Gap Analysis and Zero Trust

Gap Analysis

- A security assessment process
- Comparing current security measures and practices with established:
    - Standards
    - Best practices
    - Compliance requirements
- Goal:
    - Identify gaps or discrepancies between the current state of security and the desired or recommended state.
    - Helps organizations prioritize security improvements and develop a roadmap for enhancing their security posture by addressing identified deficiencies.
- Key Steps:
    - Identifying Security Requirements
    - Assessing Current Security Measures
    - Identifying Gaps
    - Prioritizing Remediation
    - Developing Remediation Plans

Zero Trust

- A new model for cybersecurity
- **Never trust, always verify.**
- Trust is never implicit
    - Continually analyze and evaluate the risks to assets and business functions
- Focuses on:
    - Strict identity verification
    - Continuous monitoring
    - Least privilege access
    - Micro-segmentation

Zero Trust and Planes

Control Plane – Responsible for defining and managing security policies.

- **Policy Engine** – Evaluates access requests and makes decisions based on policies and risk.
- **Policy Administrator** – Enforces decisions made by the Policy Engine and configures the Policy Enforcement Points.
- **Adaptive Identity** – Dynamically adjusts identity verification requirements based on context and risk.
- **Threat Scope Reduction** – Minimizes the attack surface by limiting trust zones and reducing access.
- **Policy-Driven Access Control** – Uses predefined security policies to control access rather than static trust assumptions.

Data Plane – Responsible for executing and enforcing access requests.

- **Policy Enforcement Point (PEP)** – The actual gateway that enforces access decisions (e.g., firewalls, proxies).
- **Implicit Trust Zone** – A network segment that traditionally allowed unrestricted trust; Zero Trust seeks to eliminate these.
- **Subject/System** – The user, device, or service requesting access to resources.

Physical Security

- Measures and safeguards designed to protect:
  - Physical assets
  - Resources
  - Facilities
- From unauthorized access, damage, theft, or harm.

Types of Physical Security

- **Bollards** – Short, sturdy vertical posts installed to block vehicles from entering a protected area. (Preventive/Deterrent)
- **Access Control Vestibule** – A secure entry system with two gateways, only one of which opens at a time to prevent piggybacking. (Preventive)
- **Fencing** – A physical barrier to define a perimeter and secure a building. (Preventive/Deterrent)
- **Video Surveillance** – The use of cameras to monitor activities for prevention, detection, and evidence. (Deterrent/Detective)
- **Security Guards** – Personnel responsible for monitoring, patrolling, and responding to incidents. (Preventive/Deterrent/Detective)
- **Access Badge** – An identification card with authentication technology (e.g., RFID, magnetic strip) for secure entry. (Preventive/Deterrent/Detective)
- **Lighting** – Provides illumination around or inside a building to deter intruders and support monitoring. (Deterrent)
- **Sensors**
  - Infrared Radiation (Light)
    - Detects motion
    - Detects temperature changes
  - Pressure
    - Detects changes in pressure such as weight or environment
    - Detects unauthorized access
    - Detects tampering
  - Microwave
    - Uses microwave signals to detect motion
  - Ultrasonic
    - Uses soundwaves to detect motion

Deception and Disruption Technology

Honeypot

- A decoy system or resource designed to attract and deceive potential attackers.
- Purpose: monitor, detect, and study unauthorized access or cyberattacks while diverting them away from critical systems or assets.

Honeynet

- A network of interconnected honeypots and other security mechanisms designed to simulate a controlled and isolated environment that attracts and traps potential attackers.
- Purpose: monitor, detect, and study cybersecurity threats and attacks, while providing a safe environment for analyzing the tactics, techniques, and procedures (TTPs) of malicious actors.

Honeyfile

- A type of honeypot file designed to lure attackers seeking to steal sensitive or valuable data.
- Mimics real files or data, often with enticing names or content.
- Purpose: monitor and gather information about unauthorized access attempts to files and attacker TTPs.

Honeytoken

- A type of honeypot marker embedded in files or databases designed to alert defenders when accessed.
- Purpose: detect malicious activity and track attackers.
- Example: a fake set of credentials planted in a database.

1.3 Explain the Importance of Change Management and the Impact to Security

Change Management

- A structured and systematic approach to planning, implementing, managing, and controlling changes.
- Responsible for controlling the lifecycle of all changes by ensuring changes are properly:
    - Evaluated
    - Authorized
    - Coordinated
- Minimizes potential risks to security.

Change

- Any addition, modification, or removal of anything that could have an effect on IT services.*

All additions, modifications, and removals should be done in accordance with security best practices.

Change Steps:

- Submitting the change request
- Conducting a change assessment
- Approving the change
- Implementing the change
- Documenting the change
- Reviewing the change

Business Processes Impacting Security Operations

- Ownership - the responsibility and accountability assigned to an individual or group for specific security processes, controls, or assets.

- Stakeholders - individuals, groups, or organizations that have an interest in, or are affected by, security operations and business processes.
- Impact analysis - the process of identifying and evaluating the potential consequences of changes, incidents, or disruptions on business and security operations.
- Test results - documented outcomes of security testing activities, such as vulnerability assessments, penetration tests, or system validation, used to inform decision-making.
- Backout plan - a predefined procedure for reverting changes or updates if they cause unexpected issues or failures in security or business operations.
- Maintenance window - a scheduled period of time allocated for performing updates, patches, or system maintenance with minimal impact on business operations.
- Standard operating procedures - step-by-step instructions that guide consistent execution of security and operational tasks to ensure reliability and compliance.

Technical Implications

- Allow lists/deny lists - lists that specify which entities (e.g., IP addresses, domains, applications) are explicitly permitted (allow list) or blocked (deny list) from accessing systems or resources.
- Restricted activities - actions or operations that are prohibited or limited to ensure compliance, reduce risks, or protect system integrity.
- Downtime - periods when a system, application, or service is unavailable, either planned (e.g., maintenance) or unplanned (e.g., outages).
- Service restart - the process of stopping and starting a service to apply changes, restore functionality, or resolve errors.
- Application restart - restarting a specific software application to apply updates, fix issues, or refresh system performance.
- Legacy applications - older software still in use that may lack modern security features, vendor support, or compatibility with new technologies.
- Dependencies - systems, applications, or processes that rely on one another, where failure or changes in one can affect the performance or security of others.

Documentation

- Updating diagrams - ensuring visual representations of systems, networks, or processes remain accurate and current.
- Updating policies/procedures - revising organizational guidelines and workflows to reflect changes in technology, security requirements, or compliance standards.

Version Control - a system or process for managing changes to documents, code, or configurations over time, allowing tracking, rollback, and collaboration while maintaining integrity and history.

1.4 Explain the Importance of Using Appropriate Cryptographic Solutions

Cryptography

- "Secret Writing"
    - Transforms a plaintext message into ciphertext
        - Uses a key (or pair of keys) and one of two algorithms:

Symmetric Algorithm – An encryption method where the same key is used for both encryption and decryption.

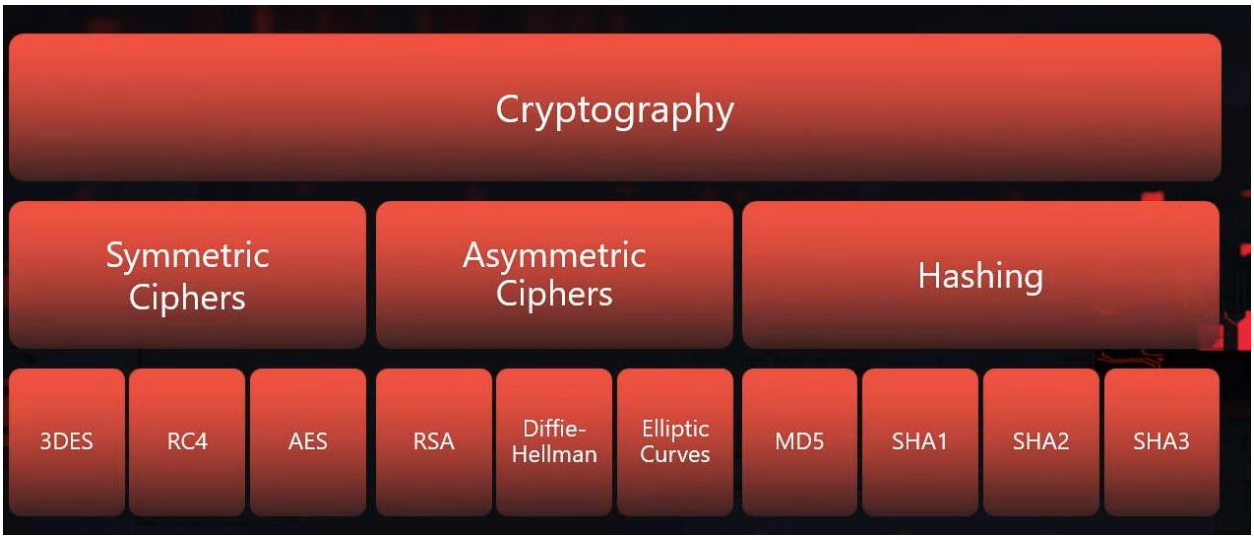
- Key Note: Same key used for both encryption and decryption
- Encryption and decryption operations are similar (or identical)
- Used for bulk encryption and decryption of data
- Faster than asymmetric algorithms

Asymmetric Algorithm – An encryption method that uses two separate keys: a public key and a private key.

- Key Note: A separate key is used for encryption and decryption (together called a keypair)
- Public Key and Private Key
- Relies on "hard problems" (such as factoring large primes) for security
- Slower than symmetric ciphers
- Great for key agreement/exchange and digital signatures
    - In practice, asymmetric ciphers are used to distribute keys for symmetric ciphers
    - Diffie-Hellman Key Exchange (DHKE) can be used to negotiate symmetric keys without directly exchanging them
        - **Diffie-Hellman Key Exchange (DHKE):** A method of securely exchanging cryptographic keys over a public channel. It allows two parties to establish a shared secret key without transmitting the actual key, making it secure against eavesdroppers.

Signing / Digital Signatures

- **Review: Confidentiality**
    - Encrypt using the recipient's public key
    - Decrypt using the associated private key
- **Digital Signatures**
    - To prove identity, the process is reversed:
        - Encrypt (sign) with the sender's private key
        - Recipients decrypt with the sender's public key
        - This proves who wrote the message (authentication), ensures integrity, and provides non-repudiation
    - In practice, signing an entire message is inefficient, so a **hash of the message** is signed instead.


Cryptography
Symmetric Ciphers
Asymmetric Ciphers
Hashing
3DES
RC4
AES
RSA
Diffie-Hellman
Elliptic Curves
MD5
SHA1
SHA2
SHA3