Armaan Shamsaasef

The CIA Triad

Notes: The CIA Triad (SY0-701 - 1.2)

Core Concept: The CIA Triad is the foundational model of information security. It is not the agency, but a framework of three core principles used to guide security policies.

The Three Principles:

1. Confidentiality
2. Integrity
3. Availability

---

1. Confidentiality

- Definition: Ensuring that data is kept private and secret, and is not disclosed to unauthorized individuals, entities, or processes.
- Primary Goal: Prevent unauthorized access to data.
- Key Question: "Who is authorized to see this information?"
- Common Implementation Tools:
    - Encryption: The primary method for protecting confidentiality (e.g., at-rest, in-transit).
    - Access Controls: Using permissions, usernames/passwords, and multi-factor authentication (MFA) to restrict access.
    - Steganography: Hiding data within another file (e.g., an image or audio file).

---

2. Integrity

- Definition: The assurance that data is trustworthy, accurate, and has not been modified from its original state by unauthorized parties.
- Primary Goal: Protect data from unauthorized alteration.
- Key Question: "Has this data been changed?"
- Common Implementation Tools:

    - Hashing: Creating a unique, fixed-size fingerprint (hash) of data. Any change to the data creates a different hash, revealing the tampering.
    - Digital Signatures: Used to verify the authenticity and integrity of a message/software.
    - Certificates: Provide a trusted third-party validation of integrity.
    - Non-repudiation: Prevents a sender from denying they were the source of the information, which is a function of integrity.

---

3. Availability

- Definition: Ensuring that information and systems are accessible and operational when needed by authorized users.
- Primary Goal: Prevent loss of access to data or services.
- Key Question: "Can I access the data when I need it?"
- Common Implementation Tools:
    - Redundancy: Duplicating critical components (e.g., servers, network paths, power supplies) to eliminate single points of failure.
    - Fault Tolerance: The system's ability to continue operating properly even if a component fails.
    - Disaster Recovery & Business Continuity Plans: Procedures to restore systems and operations after an outage.
    - Patches & Updates: Keeping systems updated to prevent crashes or exploits that could cause downtime.

Balancing the Triad

- The three principles must often be balanced. Increasing one can sometimes decrease another.
- Example: Enforcing extremely complex security (Confidentiality) can slow system performance and hinder Availability. The goal is to find the right balance for the organization's needs.

Key Takeaway: All security controls are implemented to support one or more of these three principles of the CIA Triad.