

Network Fundamentals

Key Terms

- **Bit** - A binary digit (0 or 1), the atomic unit of computing.
- **Byte** - A group of 8 bits treated as a single entity.
- **Software** - Computer programs and data that can be dynamically modified.
- **Network** - A system of interconnected components (e.g., routers, hubs, cabling).
- **Defense-in-Depth** - A security strategy integrating people, technology, and operations across multiple layers.
- **Authentication** - Verifying a user's identity.
- **Authorization** - Validating an identity and its access permissions.
- **Identification** - Asserting and confirming an identity.
- **Confidentiality** - Restricting information access to authorized users.
- **Integrity** - Protecting information from modification or destruction.
- **Availability** - Ensuring reliable access to information.
- **Non-Repudiation** - Preventing denial of an action (e.g., message sending verification).
- **Vulnerability** - A weakness that could allow unauthorized actions.
- **Threat** - A source of harm that exploits vulnerabilities.
- **Risk** - The possibility of a threat exploiting a vulnerability.
- **Threat Actor** - An individual or group that exploits vulnerabilities.

Summary of the CIA Triad

The **CIA Triad** is a foundational model in information security, representing the three core principles of securing data and systems. These principles are:

1. Confidentiality:

- Ensures that sensitive information is accessed only by authorized individuals or systems.
- Techniques used: Encryption, access controls, authentication, and data classification.

2. Integrity:

- Ensures that data remains accurate, complete, and unaltered during storage, processing, or transmission.
- Techniques used: Checksums, hashing, digital signatures, and version control.

3. Availability:

- Ensures that data and resources are accessible to authorized users when needed.
- Techniques used: Redundancy, backups, failover systems, and disaster recovery plans.

The CIA Triad is essential for designing and evaluating security policies, procedures, and technologies to protect information assets effectively.