Cybersecurity Principles

Objectives

- **CIA Triad:** Grasp Confidentiality, Integrity, and Availability concepts.
- **Security Controls:** Learn about Preventive, Detective, and Corrective controls.
- **Differentiate Risks:** Distinguish between Threats, Vulnerabilities, and Risks.
- **Conduct Risk Assessments:** Learn the process for evaluating risks.
- **Security Policies:** Recognize the need for effective security policies.
- **Interactive Threat Exercises:** Practice identifying and classifying threats.

What is CIA Triad?

The CIA Triad is a foundational model in information security that helps organizations ensure their information systems are secure. Each component of the triad addresses a critical aspect of security.

1.1 Confidentiality

- Confidentiality focuses on ensuring that **sensitive information is accessible only to authorized individuals.**
- **Key security components for confidentiality:** include encryption, access controls, data classification, and secure communication channels.
- **Healthcare Sector:** Electronic Health Records (EHRs) are encrypted and access-controlled to ensure that only authorized healthcare providers can view patient information.

What is secure communication channels ??

1.2 Integrity

- Integrity ensures that **data remains accurate, complete, and unaltered throughout its lifecycle.** Security measures such as data validation, checksums, digital signatures, and audit trails help maintain data integrity and prevent unauthorized modifications or tampering.
- **Key Aspects of Integrity:**
  - Data Integrity
  - Transaction Integrity
  - File Integrity
  - Message Integrity
  - System Integrity

1.2 Integrity

Example: **Financial Transactions:** Banks use cryptographic hash functions to ensure that transaction details have not been altered. Any changes to the data would be detected by comparing hash values.

Best Practices for Maintaining Data Integrity??

1.3 Availability

- Availability ensures that **systems and resources are accessible and usable when needed.** It involves implementing measures to prevent disruptions, downtime, or denial of service attacks. Redundancy, fault tolerance, disaster recovery plans, and robust network infrastructure are essential components of ensuring availability.
- Key Concepts:
    1. Redundancy
    2. Disaster Recovery
    3. Load Balancing

    Example:

    Cloud Services: Cloud providers implement redundancy and backup solutions to maintain service availability and data access in case of hardware failures or outages.

1.4 Non-Repudiation

Key Concept:

- **Digital Signatures**: Provide proof of the origin and integrity of a message, making it impossible for the sender to deny having sent it.
- **Audit Trails:** Logs that record actions performed within a system, providing evidence in the event of disputes.

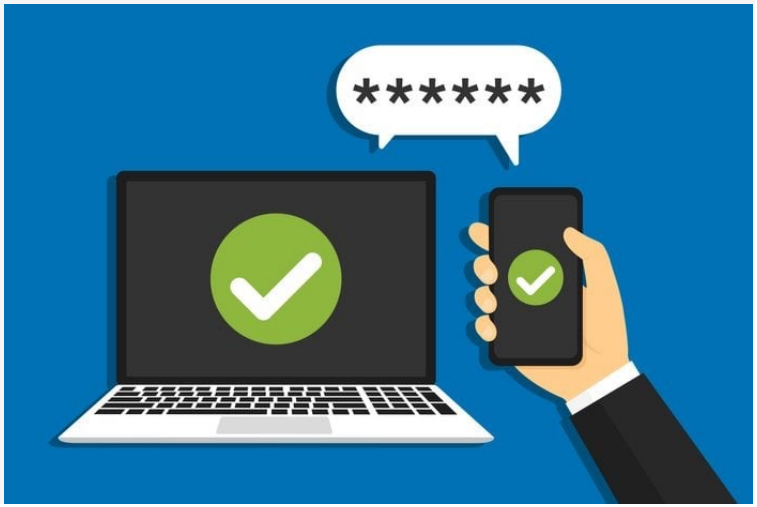
- **Example:** A user digitally signs a contract, ensuring that they cannot later deny having signed it.

1.5 Authentication

Authentication is a critical component of cybersecurity that verifies the identity of users, systems, or devices before granting access to resources or data. The primary goal of authentication is to ensure that only authorized individuals or entities can access specific systems, applications, or data, thus protecting against unauthorized access and potential breaches.

Key Aspects of Authentication:

- Something You Know
- Something You Have
- Something You Are



1.5 Authentication

Authentication Methods:

- Password-Based Authentication
- Multi-Factor Authentication (MFA)
- Biometric Authentication
- Single Sign-On (SSO)

Authentication Protocols:

- OAuth (Open Authorization)
- SAML (Security Assertion Markup Language)
- Kerberos

Quiz

Question 1: What does the "Confidentiality “component of the CIA Triad primarily ensure?

A. Data is stored without errors
B. Data is protected from unauthorized access
C. Data is available when needed
D. Data is encrypted at all times

Quiz

Question 2: Which of the following is a characteristic of "Integrity" in the CIA Triad?

A. Ensuring data is only accessible to authorized users
B. Ensuring data remains accurate and unaltered by unauthorized parties
C. Ensuring data is available during an attack
D. Ensuring data is encrypted before transmission

Quiz

Question 3: What is the main purpose of encryption in cybersecurity?

A. To identify security breaches
B. To prevent unauthorized access by transforming data into an unreadable format
C. To recover lost data
D. To monitor network traffic

Exercise : Identifying and Classifying Security Threats

- **Threat Scenario:**

  An employee receives an email that appears to be from a trusted vendor, asking for login credentials to update account information.

- **Task:**

  Identify and classify the potential security threats based on the information provided.

- **Discussion:**

  Discuss how you would mitigate these threats and what security controls would be appropriate.

Exercise : Identifying and Classifying Security Threats

Threat Type:
Phishing

Threat Category:
Social Engineering

Immediate Actions:

- Do Not Respond or Click
- Verify the Request
- Report the Email

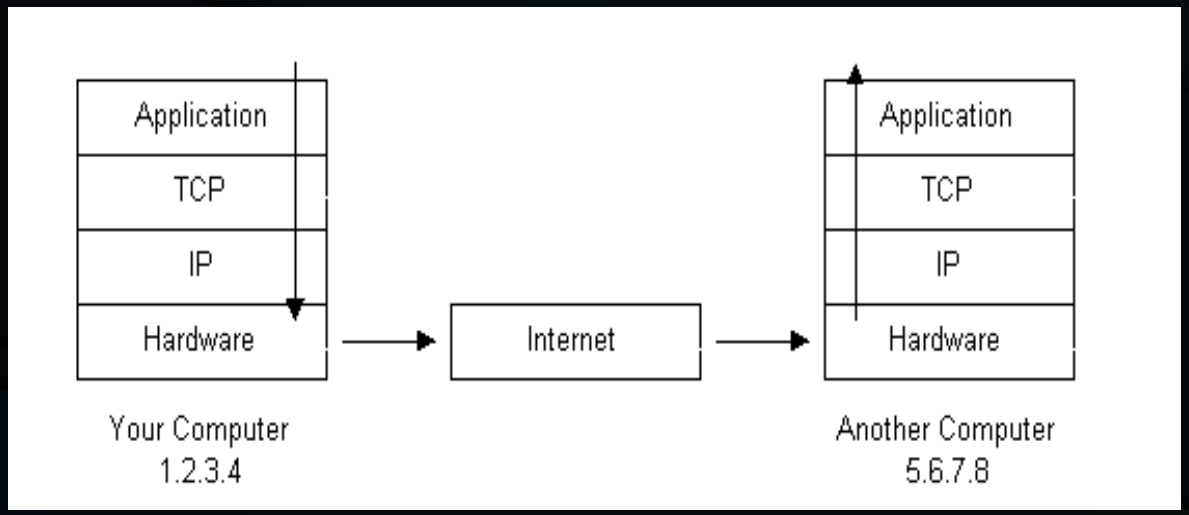
Mitigation Strategies:

- Employee Training
- Email Filtering

Computer Networks

- An interconnection of multiple devices, also known as hosts, that are connected using multiple paths for the purpose of sending/receiving data or media. Computer networks can also include multiple devices/mediums which help in the communication between two different devices; these are known as Network devices and include things such as routers, switches, hubs, and bridges.

How Computers communicate

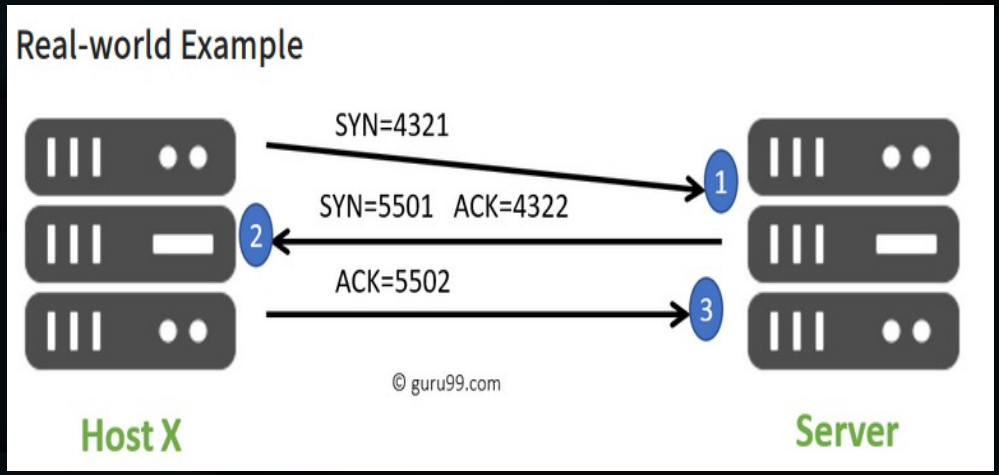


3 way handshake

TCP message types

Message	Description
Syn	Used to initiate and establish a connection. It also helps you to synchronize sequence numbers between devices.
ACK	Helps to confirm to the other side that it has received the SYN.
SYN-ACK	SYN message from local device and ACK of the earlier packet.
FIN	Used to terminate a connection.

Real-world Example



Common network protocols

- HTTP/HTTPs
- SMTP
- DHCP
- DNS
- SSH/Telnet
- FTP/SFTP
- SMB
- RPC
- SNMP
- SySlog