جامعة المستقبل
AL MUSTAQBAL UNIVERSITY

كلية العلوم

قسم الأمن السيبراني

Lecture: (3)

Confidentiality, integrity, availability

Subject: software security

second Stage

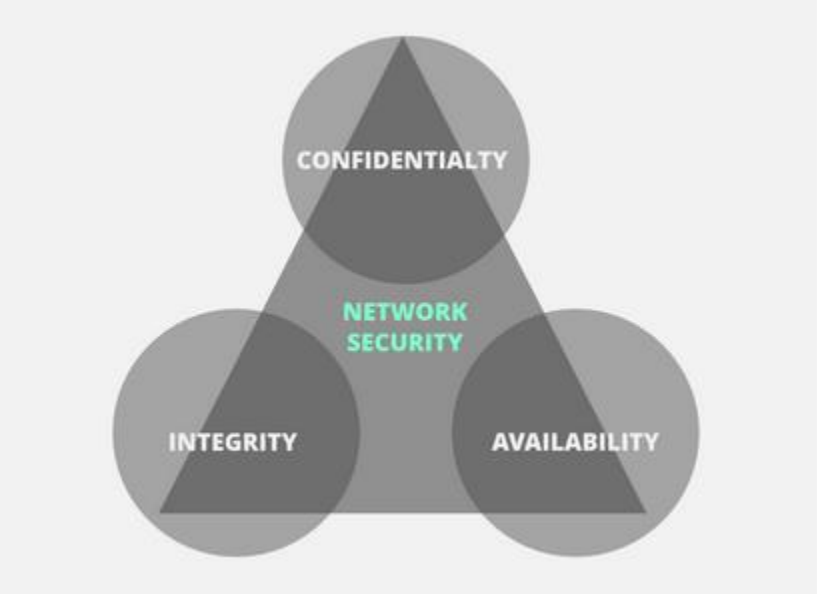
Lecturer: Asst. Lecturer. Suha Alhussieny

CIA Triad

When talking about network security, the **CIA** triad is one of the most important models which is designed to guide policies for information security within an organization.

CIA stands for :

1. Confidentiality
2. Integrity
3. Availability



Confidentiality, Integrity, and Availability (CIA) are the three core principles of information security, often referred to as the CIA triad. These principles form the foundation for designing and evaluating the security of systems, data, and processes. Here's a detailed overview of each component:

1. Confidentiality

- **Definition:** Confidentiality ensures that sensitive information is accessed only by authorized individuals or systems and is protected from unauthorized disclosure.

- **Purpose:** To protect information from being disclosed to unauthorized parties, thereby preventing breaches of privacy and security.

- **Key Concepts and Practices:**

  - **Encryption**
  - **Access Controls**

- **Examples of Confidentiality Breaches:**

  - **Data Leaks:** Sensitive information, like personal data or trade secrets, being exposed due to inadequate access controls.

  - **Unauthorized Access:** Hackers gaining access to confidential information through phishing, malware, or other attack vectors.

2. Integrity

- **Definition:** Integrity ensures that data is accurate, consistent, and has not been tampered with or altered by unauthorized parties.

- **Purpose:** To maintain the trustworthiness and accuracy of information, ensuring that it remains unchanged from its original state unless properly authorized.

- **Key Concepts and Practices:**

  - **Checksums and Hashing:** Using checksums or cryptographic hashing (e.g., SHA-256) to detect alterations in data. Any changes to the data will result in a different hash value.

  - **Digital Signatures:** Applying digital signatures to data to verify its origin and ensure it has not been modified during transmission.

- **Examples of Integrity Breaches:**

  - **Data Tampering:** Unauthorized modification of data, such as altering financial records, which can lead to fraud or misinformation.

  - **Man-in-the-Middle Attacks:** Attackers intercepting and altering data during transmission, potentially compromising the integrity of communication.

3. Availability

- **Definition:** Availability ensures that information and systems are accessible and usable when needed by authorized users.
- **Purpose:** To ensure that systems and data are available to users in a timely manner, supporting the continuity of business operations.
- **Key Concepts and Practices:**
  - **Redundancy:** Implementing redundant systems, such as backup servers, failover clusters, and data backups, to ensure continuous availability even if a component fails.
  - **Load Balancing:** Distributing workloads across multiple systems or servers to prevent overload and ensure that resources are available even under heavy usage.
- **Examples of Availability Breaches:**
  - **DDoS Attacks:** Overloading a system with traffic to make it unavailable to legitimate users.
  - **Hardware Failures:** System crashes or server outages leading to unavailability of critical services.

Q1/

1. What does the "C" in the CIA triad stand for?

a) Cybersecurity
b) Confidentiality
c) Control
d) Cryptography
e) Compliance

2. Which of the following ensures that data remains unchanged unless modified by authorized users?

a) Confidentiality
b) Availability
c) Integrity
d) Authentication
e) Encryption

3. What is the primary purpose of encryption in cybersecurity?

a) Ensuring data is available at all times
b) Preventing unauthorized access to sensitive information
c) Verifying data origin and authenticity
d) Distributing workloads evenly
e) Detecting unauthorized data modifications

4. A DDoS attack primarily affects which aspect of the CIA triad?

a) Confidentiality
b) Integrity
c) Availability
d) Authentication
e) Authorization

5. Which of the following security practices ensures data integrity?

a) Digital signatures
b) Phishing attacks
c) Data redundancy
d) Load balancing
e) Man-in-the-middle attacks

6. Which of the following is an example of an integrity breach?

a) Hackers accessing confidential data
b) A server going offline
c) Financial records being altered without authorization
d) A phishing attack
e) Encryption of sensitive information

7. What security control helps protect data from unauthorized disclosure?

a) Load balancing
b) Digital signatures
c) Access controls
d) Data redundancy
e) Man-in-the-middle attacks

8. Which of the following is an example of an availability breach?

a) Unauthorized access to private files
b) Data leakage due to weak encryption
c) A system crash preventing users from accessing services
d) A hacker modifying stored data
e) Using checksums to verify data integrity

9. What mechanism is used to detect unauthorized changes in data?

a) Load balancing
b) Hashing
c) DDoS protection
d) Redundancy
e) Access control lists

10. What is a key method to ensure continuous availability of services?

a) Applying strong passwords
b) Implementing redundancy
c) Encrypting data
d) Using phishing simulations
e) Limiting access control

11. What is the primary goal of the CIA triad in cybersecurity?

a) Preventing all cyber attacks
b) Ensuring system performance
c) Guiding information security policies
d) Increasing network speed
e) Reducing system costs

12. Which of the following best describes a man-in-the-middle (MITM) attack?

a) Unauthorized modification of financial records
b) Intercepting and altering communication between two parties
c) Overloading a system to make it unavailable
d) Encrypting data to protect it from hackers
e) Using strong passwords to prevent breaches

13. Which security measure helps ensure confidentiality?

a) Data backups
b) Load balancing
c) Encryption
d) Redundancy
e) Hashing

14. Which attack aims to make a system or service unavailable to legitimate users?

a) Phishing
b) Ransomware
c) DDoS attack
d) SQL injection
e) Man-in-the-middle attack

15. What does a digital signature verify?

a) The availability of data
b) The originality and authenticity of data
c) The encryption strength of data
d) The speed of a network
e) The hardware compatibility of a system

Q2/ define the integrity and what Key Concepts and Practices ?