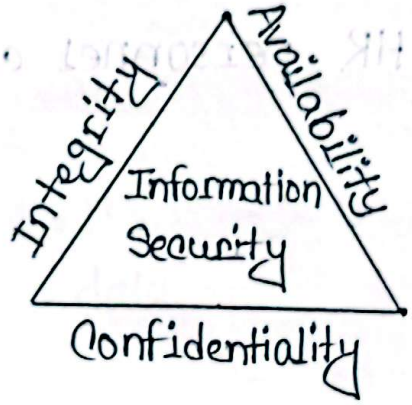
1. CIA security goals.

The Central Intelligence Agency (CIA) aims to protect the confidentiality, integrity and availability of it's information, aligning with the CIA Triad security model. This model is a framework for ensuring that sensitive data remains secure, accurate and accessible only to authorized personnel.



The CIA security goals are the core objectives that any good cybersecurity strategy or system should aim to achieve. They're known as the CIA Traid. The CIA security goals are given below:

① Confidentiality:

Goal: Prevent unauthorized access to sensitive

information.

What it protects: Personal data, trade secrets, classified information.

Achieved through:

: Encryption
- Access control (e.g. passwords, biometrics)
- Network security (VPNs, firewalls)
- Data classification and handling policies

Example: Only HR personnel can acess employee salary records.

② Integrity

Goal: Ensure that data is accurate, consistent, and hasn't been tampered with.

- What it protects: Trustworthiness and reliability of data.

- Achieved through:
  - Hashing and checksums
  - Digital signatures
  - Version control
  - Audit logs

Example: A financial transaction must not be altered between sender and receiver.

③ Availability

Goal: Ensure information and systems are accessible to authorized users when needed.

What it protects: Timely and reliable access to data and systems.

Achieved through:

- Redundancy (e.g., backup servers)
- Disaster recovery plans
- DDoS protection
- System maintenance

Example: Online banking must be available to users 24/7, even during peak hours or under attack.

Sheta Saha AT-21009

2. Types of Cyber Attacks

1. Phishing :

Phishing is tricking users into giving up sensitive info (passwords, credit card numbers) via fake emails or websites.

It targets confidentiality

Example: You get a fake email from "your bank" asking you to log in.

2. Malware (Viruses, Trojans, Worms, Ransomware)

Malware is malicious software that can steal, corrupt or lock your data.

It targets confidentiality, Integrity and Availability.

Example: Ransomware encrypts your files and demands payment to unlock them.

3. Man-in-the-Middle (MitM) Attack

Man-in-the-Middle Attacker intercepts communication between two parties.

It targets confidentiality and Integrity.

Example: Intercepting your login details on a public Wi-Fi network.

4. SQL Injection

SQL Injection is inserting malicious SQL code into a website input to manipulate databases.

It targets Integrity and confidentiality;

Example: Retrieving or altering all users' data from a poorly secured login form.

5. Denial of service (DoS)/ Distributed Denial of service (DDoS)

Denial of Service(DoS)/ Distributed Denial of service (DDoS) is overloading a system or server so legitimate users can't access it.

It targets availability.

Example : A DDoS attack crashes an online store on Black Friday.

6. Zero-Day Exploit

Zero-Day Exploit is attacking a software vulnerability before it's known or patched.

It targets any of the CIA Triad elements.

Example: Exploiting a bug in your web browser before an update is released.

7. Brute Force Attack

Brute Force Attack is attempting to guess passwords using automated tools.

It targets - confidentiality

Example: Repeatedly trying millions of combinations to break into an email account.

8. Social Engineering

Social Engineering is manipulating people into giving up confidential info or access.

It targets - Confidentiality

Example: Pretending to be IT support and asking someone for their password.

9. DNS Spoofing / Poisoning

DNS Spoofing/Poisoning is redirecting traffic from legitimate sites to fake ones.

It targets Confidentiality and Integrity.

Example: You think you're visiting your bank's site, but it's a fake copy.

10. Supply Chain Attacks

Supply Chain Attacks is attacking a less secure partner/vendor to get into your network.

It targets usually confidentiality and Integrity.

Example: The infamous Solarwinds attack that compromised thousands of organizations.

Shefu Saha IT-21009

3. Symmetric and Asymmetric Key Encryption

Symmetric Key Encryption:

Symmetric key Encryption uses the same key for both encryption and decryption of data.

How it works:

1. The sender encrypts the message using a secret key.
2. The recipient uses the same key to decrypt the message.

Example Algorithms:

i. AES (Advanced Encryption Standard)

ii. DES (Data Encryption Standard)

iii. RC4

Asymmetric Key Encryption

Asymmetric encryption uses two keys.

- A public key to encrypt
- A private key to decrypt

How it works:

1. The sender encrypts the message with the recipient's public key.
2. Only the recipient's private key can decrypt it.

Example:

- RSA (Rivest-Shamir-Adleman)
- Ecc (Elliptic Curve Cryptography)
- DSA (Digital Signature Algorithm)

Shetu Saha IT-21009

4. Steganography

Steganography is the practice of hiding a secret message within an ordinary, non-secret file or message to avoid detection.

Unlike encryption, which obscures the content, steganography hides the fact that a message exists at all.

Common Forms of Steganography

1. Image Steganography:

- Hiding data within the pixels of an image.
- Example: Using the Least Significant Bit (LSB) of each pixel to embed data without noticeably changing the image.

2. Audio Steganography

- Hiding data in audio files (like MP3 or WAV)
- Tiny changes in amplitude or frequency can store information.

3. Video Steganography

- Combining image and audio steganography to hide data in video files.

4. Text Steganography

Altering text formats, using invisible characters or manipulating word patterns to embed messages.

5. Network Steganography

Hiding data in network traffic, such as in TCP/IP headers or packet timing.

Shefu Saha IT-21009