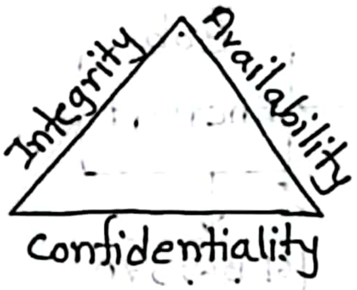
Shafinaj Jerin Asha

IT-21031

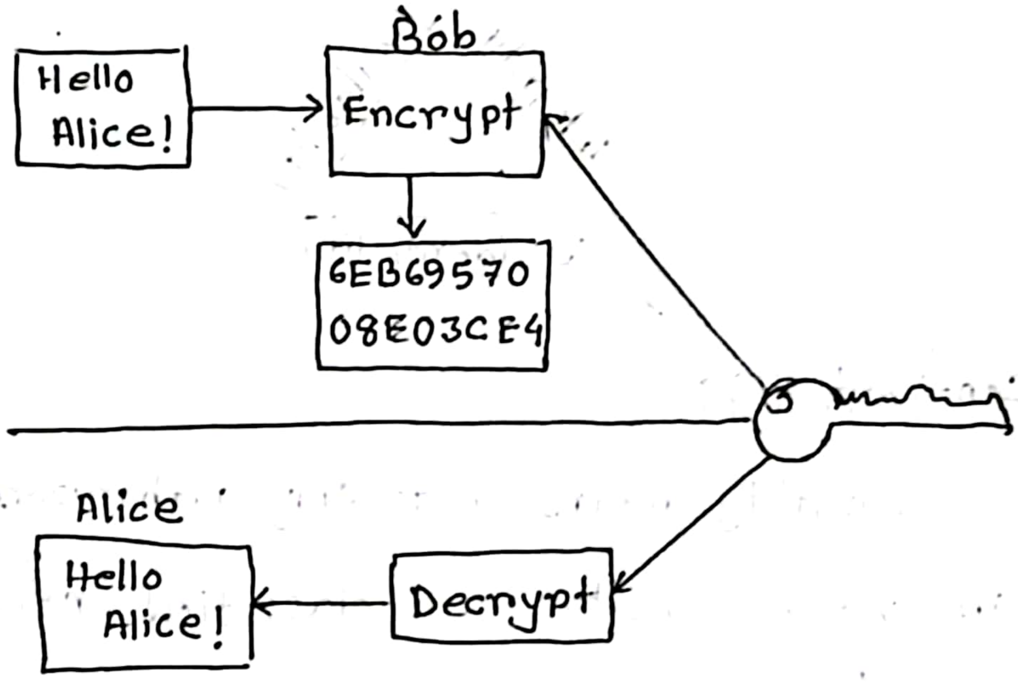
1. CIA Security goals

The goals of .CIA Triad are confidentiality, Intgrity and availability which are basic factors in information secubity.



Confidentiality:

Confidentiality means that only authorized individuals can view sensitive or classified information. The data being sent over network should not be accessed by unauthorized individuals. The attacker may try to capture the data using different tools available on the internet and gain access to your information. A primary way to avoid this is to be use encrybtion techniques to safe-guard our data ~~to~~ so that even if the attacker gains access to our data, he/she will not be able to decrypt it. Another way to protect our data is through a VPN tunnel.

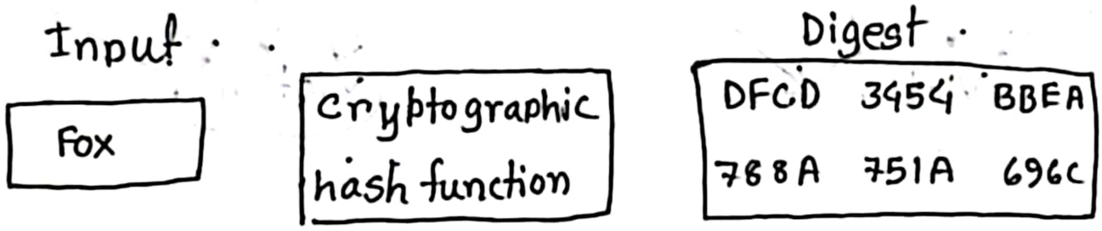


Integrity:

The idea of integrity is to make sure that data has not been modified carruption of data is a failure to maintain data integrety

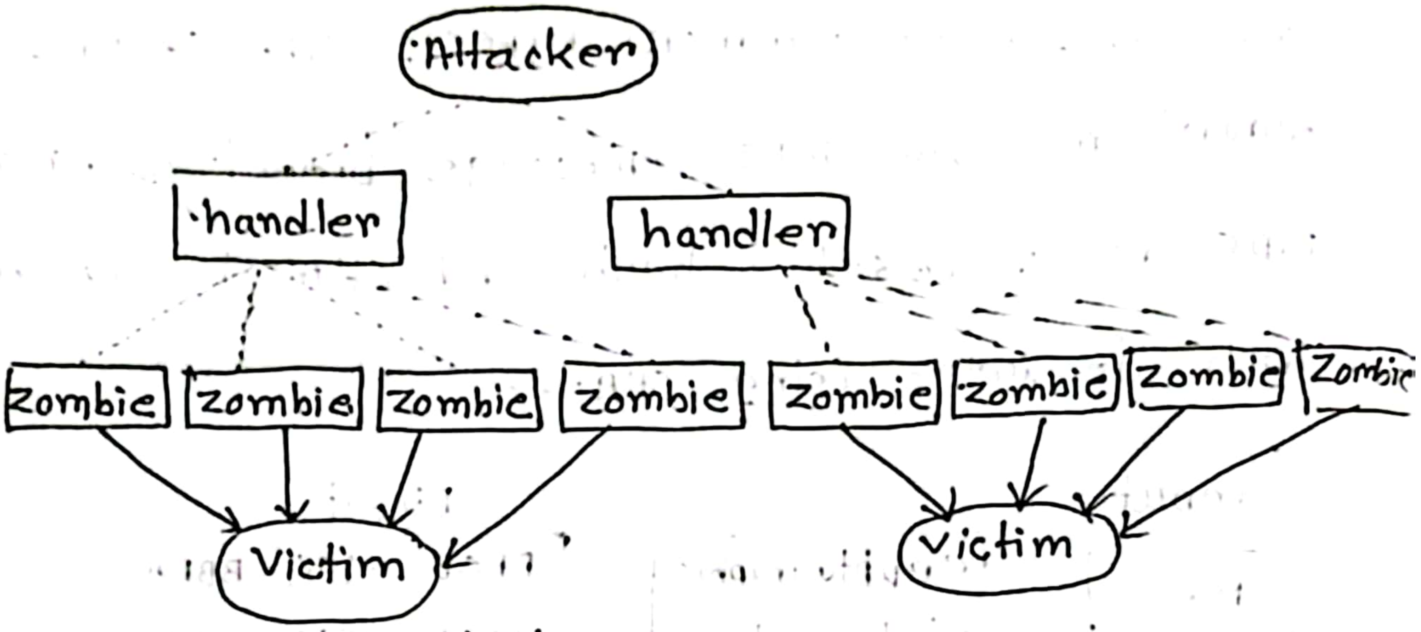
To check if our data has been modified or not, we make a use of hash function.

We have two common types: SHA (Secure Hash Algorithm) and MD5 (Message Direct 5). Now MD5 is a 128-bit hash and SHA is 160-bit hash if wee're using SHA-1.



Availability:

This means that the network should be readily available to its users. This applies to systems and to data. To ensure availability, the network administrator should maintain hardware, make regular upgrades, have a plan for fail-over and prevent bottlenecks in a network. Attacks such as DOS or DDOS may render a network unavailable as the resources of the network get exhausted.



2. Symmetric key Encryption:

Symmetric key encryption is a type of encryption where the same key is used to both encrypt and decrypt the data.

How it works:

1. The sender encrypts the message using a secret key.
2. The encrypted message (ciphertext) is sent to the receiver.
3. The receiver uses the same secret key to decrypt the message back to its original form.

Assymmetric key Encryption:

Assymmetric key encryption is a type of encryption that uses two different keys: a public key & a private key.

How it works:

1. The public key is shared with everyone.
2. The private key is kept secret by the owner.
3. If someone encrypts a message with the public key only the matching private key can decrypts it.

Types of cyber attacks:

1. Malware:

- Mallcious software like viruses, worms, ~~to~~ trojans, ransomware and spyware.
- can steal, delete or encrypt data or damage system.

2. Phishing:

-Fake emails or messages that trick users into giving away sensitive info (like passwords or eredit card numbers)

3. Denial of Service (DoS / Distributed DoS (DDoS)

- Overwhelms a system, server or network with traffic to make it unavailable.

4. Man in the middle Attack (mitM).

-An attacker interprets communication: between two parties to steal or manipulator data.

5. SQL injection:

- Attacker insert malicious SQL code into a database query to access or modify data.

6. zero-day-Exploit:

Attacks that exploit unknown vulnerability before a patch of fix is released.

7. credential stuffing:

Using stolen username /passwords from one service to break into other accounts.

8. Brute Force Attack:

Trying many password combinations until the correct one is found.

9. Cross-site Scripting (xss):

Injecting malicious scripts into webpages viewed by other, often used to steal session cookies

10. Ransomware:

A type of malware that encrypts data and demands a ransom for its release.