DCN - COMPUTER NETWORK SECURITY

During initial days of internet, its use was limited to military and universities for research and development purpose. Later when all networks merged together and formed internet, the data useds to travel through public transit network.Common people may send the data that can be highly sensitive such as their bank credentials, username and passwords, personal documents, online shopping details, or confidential documents.

All security threats are intentional i.e. they occur only if intentionally triggered. Security threats can be divided into the following categories:

- **Interruption**

  Interruption is a security threat in which availability of resources is attacked. For example, a user is unable to access its web-server or the web-server is hijacked.

- **Privacy-Breach**

  In this threat, the privacy of a user is compromised. Someone, who is not the authorized person is accessing or intercepting data sent or received by the original authenticated user.

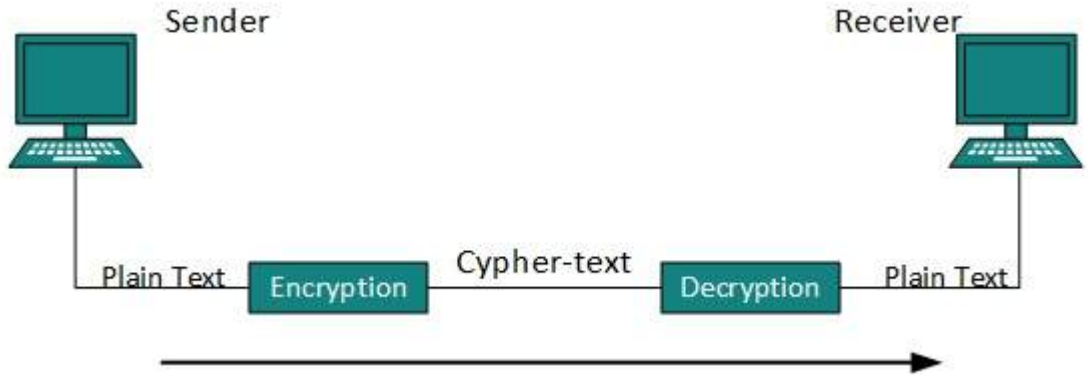
- **Integrity**

  This type of threat includes any alteration or modification in the original context of communication. The attacker intercepts and receives the data sent by the sender and the attacker then either modifies or generates false data and sends to the receiver. The receiver receives the data assuming that it is being sent by the original Sender.

- **Authenticity**

  This threat occurs when an attacker or a security violator, poses as a genuine person and accesses the resources or communicates with other genuine users.

No technique in the present world can provide 100% security. But steps can be taken to secure data while it travels in unsecured network or internet. The most widely used technique is Cryptography.



Cryptography is a technique to encrypt the plain-text data which makes it difficult to understand and interpret. There are several cryptographic algorithms available present day as described below:

- Secret Key
- Public Key
- Message Digest

Secret Key Encryption

Both sender and receiver have one secret key. This secret key is used to encrypt the data at sender's end. After the data is encrypted, it is sent on the public domain to the receiver. Because the receiver knows and has the Secret Key, the encrypted data packets can easily be decrypted.

Example of secret key encryption is Data Encryption Standard *DES*. In Secret Key encryption, it is required to have a separate key for each host on the network making it difficult to manage.

Public Key Encryption

In this encryption system, every user has its own Secret Key and it is not in the shared domain. The secret key is never revealed on public domain. Along with secret key, every user has its own but public key. Public key is always made public and is used by Senders to encrypt the data. When the user receives the encrypted data, he can easily decrypt it by using its own Secret Key.

Example of public key encryption is Rivest-Shamir-Adleman *RSA*.

Message Digest

In this method, actual data is not sent, instead a hash value is calculated and sent. The other end user, computes its own hash value and compares with the one just received.If both hash values are matched, then it is accepted otherwise rejected.

Example of Message Digest is MD5 hashing. It is mostly used in authentication where user password is cross checked with the one saved on the server.