Chapter 1

Introduction to criptography

Security Goals :-

(1) Confidentiality :- Hidden from unauthorized access.

(2) Integrity :- Protected from unauthorized change.

(3) Availability :- Available to authorized entity.

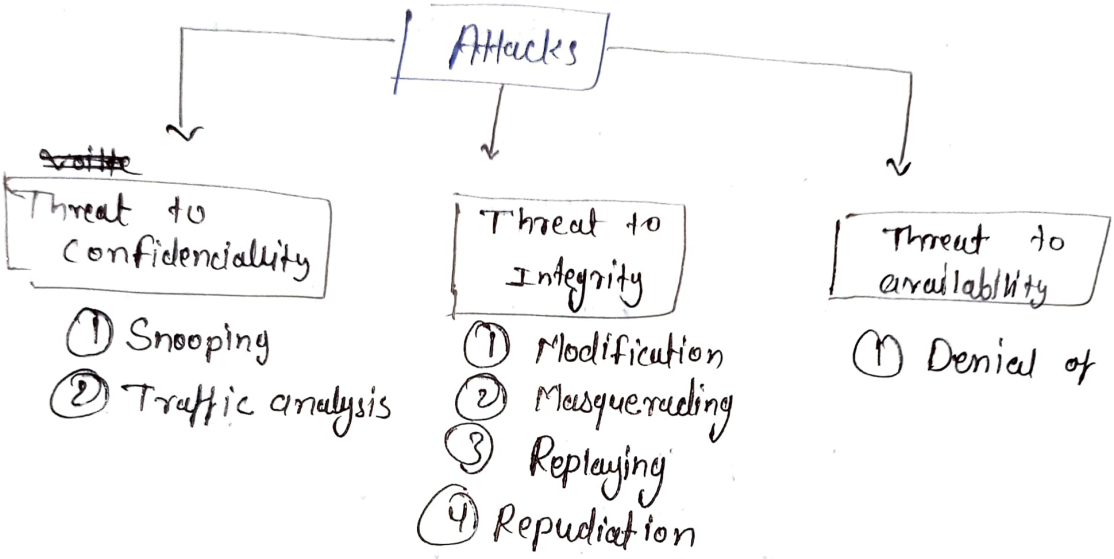
Confidentiality :- If we are sending a data to a network. then it can be accessed By unauthorized entity. we have to Prevent this.

Integrity :- While Sending a data ~~a me data~~ It can be changed by the unauthorized Entity. we have to prevent from change

Availability :- The data (information) is must available to authorized Entity.
The information is useless if not available ~~The~~ what happen when we are unable to access our own bank account.

Attacks :- Our three security goals can be threatened by security attacks.

Currently we are deviding the security Attacks according to our 3 security goals :-



Attacks Threatening Confidentiality :-

Two types of attack Threaten the confidentiality of information :-

(1) Snooping
(2) Traffic analysis.

(1) **Snooping** :- If we are transferring a file which containing confidencial information. An unauthorized entity may intercept the transmission & get the confidential information. & use this information for its own benifit.

~~In this~~

in this attack, the attacker did not modify the information. So it is Hard to detect the attacker. we can Prevent this type of attack By ~~using~~ using Encipherment technique.

(2) Traffic Analysis:- This is similar to Snooping But the only change is that ~~use~~ the information is in encrypted form. In this attack the attacker tries to find Some useful information from the encrypted data that can be helpful for its own use. The attacker tries to find location of sender or receiver.
or
The attacker tries to collect some request-response Pair to guss the nature of transection.

Attacks threatening integrity :- 4 types of attacks are used to threaten the integrity of information :-

(1) Modification
(2) Masquerading
(3) replaying
(4) Repudiation

① Modification :- After intercepting or accessing information. the attacker tries to modify the information to make it beneficial to itself.

Example :- A customer sends a message to a bank to do some transection. The attacker intercepts the message & change the type of message.

② Masqueradling :- Masqueradling or spoofing, happens when the attacker express itself as another person. & use the identity of that person.

Example :- The attacker steal the Bank card & pin of the bank customer & express itself as a customer.

Sometime the attacker expressed as receiving entity.

Example :- The person tries to visit the site of Bank But He reached to other site similar to its Bank site. Now He enter his id & password. Now the attacker use use this id & password for its own purpose.

③ Replaying :- In this attack the attacker get the copy of the message and later He tries to replay it.

Example :- A person sends a message to a bank for transection. the attacker took the copy of this message & send this message again for another transection.

④ Repudiation :- This type of attack is different from the other because it is Performed by one of the 2 parties in the communication. the Sender or the receiver.

Example of denial by sender :- The bank customer request the bank to Send money to the third Party But later He denial that He had not made such a request.

Example of denial by receiver :- If a Person purchasing some product from the ~~online~~ ~~or~~ manufacturer and Pays for it electronically, but the manufacturer later denies that He had Not received Payment.

Attacks threatening Availability :-

we have only one attack that threatening availability :- ① Denial of Services.

① Denial of Services :- It is very common attack. It Slow down or totally Interrupt the Service of a System.

The attacker tries to send many bogus ~~letter~~ message to the server so the Server ~~it~~ crashes because of heavy load.

The attacker might intercept & delete the server Response so that client assume that server is Not responding The attacker also intercept the client request, & causing the client to send many request.

Prerously we devided ~~out~~ the types of security attacks according to our 3 security goals.

Now we deviding the attacks according to the modification of the information.

According to this we have 2 types of categoury of attacks

(1) Active Attacks
(2) Passive Attacks.

~~Passive~~

(1) Passive Attacks :- In the Passive attack the goal of the attacker is obtain information only.

This means the attacker does not modify the information, & does not harm the system. The system continu with normal operation.

However the attack can Harm the sender or receiver of the message, Becausse of misuse of information.

For this reason, it is difficult to detect this type of attack, until the sender or receiver finds out about the leaking of confidential information.

It is prerented By Encypherment of data.

Example:- (1) Snooping
(2) Traffic analysis.

Active Attacks :- An active attack may change the data or harm the system.

Attacks that threaten the integrity and availability are active attacks.

It is ~~easy~~ easy to detect But Hard to Prevent. Because the attacker can launch this type attack in variety of ways.

Services :-

(1) **Data confidentiality** :- Protect data from disclosure attack.

It is designed to prevent Snooping & traffic analysis attack.

(2) **Data integrity** :- It is designed to protect data from modification, insertion, deletion and replaying by an adversary.

(3) **Authentication** :- This service provides the authentication of the party at the other end of the line.

In connection-oriented communication it authenticate Both sender and the receiver.

But in connectionless-communication it ~~and~~ authenticate the sender of the data.

(iv) Nonrepudiation :- Nonrepudiation service protects against repudiation by either the sender or the receiver of the data. This service uses the id of the sender and the receiver. So that both can prove itself if either one is denial.

(v) Access control :- This service provides the protection against the unauthorized access of data.

Security Mechenism :- The security mechanisms Provide the security service defined Prevously.

(1) Enciphermont :- Hiding or corering data, can Provide confidentiality.
Two techniques are used for this :-
(1) Cryptography
(2) Steganography

(2) Data Integrity :- This mechanism appends short checkvalue to the data that has been created By specific mechanism from data itself. The receiver receives Both data & checkvalue. Now the receiver calculate the new checkvalue from the data & compare with received checkvalue If both the checkvalues are same then the intigrity of data is Preserved.

(3) Authentication Exchange :- In this mechanism, two entities exchange some message to prove their identity to each other.

(4) Traffic Padding :- Add some bogus data into the message which creates some confution for the receiver.

(5) Routing control :- This means that continously Changing different available routes between the sender & the receiver so that if the attacker is continously monitering at the particular route. then He is able to see only some packets.

(6) Notarization :- This mechanism is used to prevent the repudiation. In this mechanism we are selecting the third trusted party to control the communication b/w two entities.

(7) Access control :- It is a method to prove that a user has accen right to data or resources.

These Mechanisms are theoritical to impement security we need some technique to implement our 3 security goals.

Two techniques are used :-

1. Cryptography
2. Steganography.

Cryptography :- Cryptography means "Secret writting" or art of transforming message to make them secure to attacks.

In past the cryptography is only reffered to as 'Encryption' and 'decryption' of message using secret keys.

Today this involve 3 mechanisms :-

1. Symmetric key Encipherment
2. Asymmetric key Encipherment
3. Hashing.

(1) Symmetric key Encipherment :- Sometime called Privet key or Secrete key Encipherment.

Symmetric key Encipherment uses a single Secrete key for Both encryption & decryption.

Encryption/decryption can be though a electronic locking. In symmetric key encipherment, the Sender puts the message in a box and locks the box using the Shared secret key & the receiver unlocks the box with the Same key & take out the message.

2. Asymmetric - key Encipherment :- Sometimes called "Public - key cryptography"

In this mechanism we have 2 keys

(1) Public key
(2) Private key

The Sender of the message encrypt the message using the receivers Public key Now this message can be decrypted by only the Private key of the receiver.

(3) Hashing :- It is a fixed - length - message digest created from variable length message. It is smaller then the message.

the Sender sends bothe the message & the digest. to the receiver. Hashing is used as a checkvalue that provides integrity of the message.

Steganography :- The Steganography means "Covered writting".

In this we Hide our message in Diagram or Photo & Send to the receiver. we do ~~een~~ Not encrypt the text. It is very Past technology.