Cryptography and Network Security

Presented By:

Dileep Kumar Yadav

Assistant Professor

CSE Dept.

VBS PU Jaunpur

Cryptography and Network Security

"Three people can keep a secret only if two of them are dead"

Cryptography and Network Security

- Cryptography is a greak word
- Crypto-hidden
- Graphy-to write

Cryptography

- It is the art and science of achieving security by encoding message to make them non readable.

Cryptanalysis

- It is the technique of decoding message from non readable format to readable format.

Cryptology

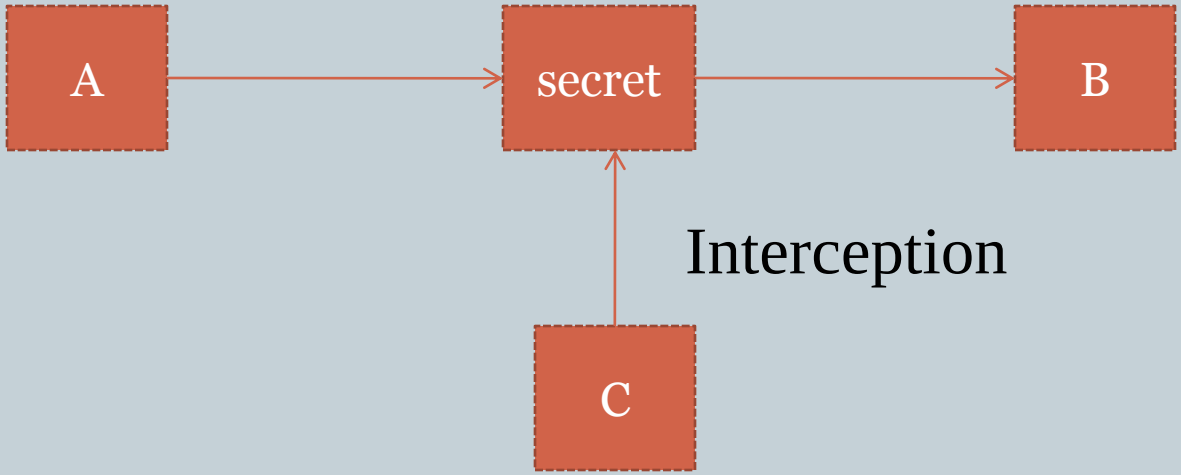
- Combination of both
- Cryptography + cryptanalysis=cryptology

Principle of Security Services

- P- Privacy or Confidentiality
- A- Authentication
- N- Non-Repudiation
- I- Integrity

Privacy or Confidentiality

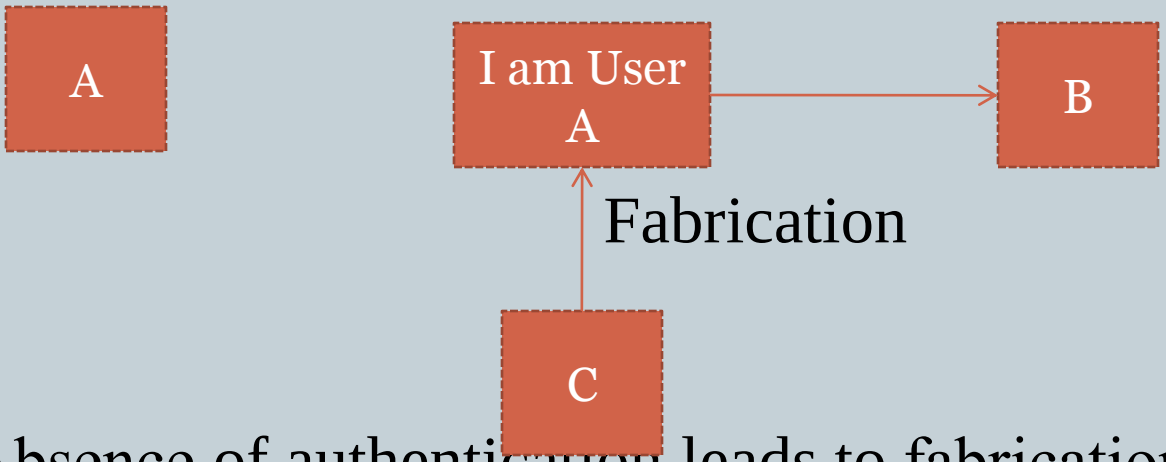
- The principle of confidentiality specifies that only the sender and the intended recipients should be able to access the contents of a message.



"Loss of Confidentiality leads to interception"

Authentication

- Authentication mechanism helps establish proof of identities. The authentication process ensures that the origin of an electronic message or document is correctly identified.



"Absence of authentication leads to fabrication"

Non-Repudiation

- There are situation where a user sends a message and later on refuses that he had not sent that message.
- It provides evidence for the existence of a message.
- For example-suppose user A could send a fund transfer request to bank B over the internet. After the bank perform the fund transfer as par A instruction A could claim that he or she never sent the fund transfer instruction to the bank. Thus A repudiates or denies.
- The principle of non-repudiation defeats such possibilities of denying something.

General Principle

- Access Control
- Availability

Security Attack

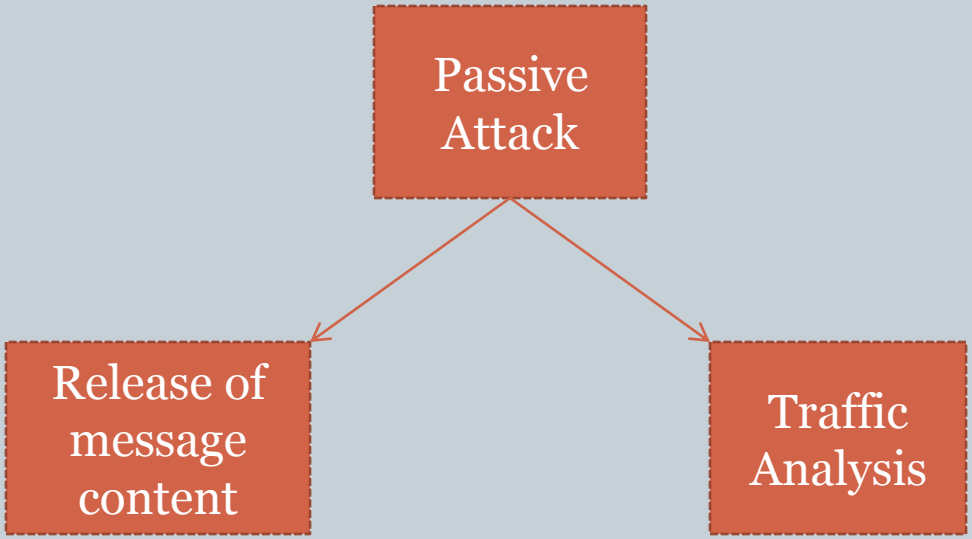
- Any action that compromises the security of information owned by organization is termed as security attacks.

Types of Security Attacks

- Passive Attack
- Active Attack

Passive Attack

- Passive attack do not involve any modification to the content of an original message.



Release of Message Content

- It is quite simple to understand when we send a confidential email message to our friend ,we desire that only he or she be able to access it , otherwise the content of the message are released against our wishes to someone else.
- Using certain security mechanism we can prevent this technique with the encode of message or change the language which is not understand by third party.

Example

- When two people talk together and third person come together then two person change their topic or change their talking language.

Traffic Analysis

- In this technique if there are so many messages are passing through a passive attacker could try to figure out similarities between them to come up with some sort of pattern that provides his some clues regarding the communication that is taking place. Such attempts of analyzing message is called traffic analysis.

Example

- When two people talk to each other and third person only see their lips to talk and guess what type of information sharing there.

Active Attacks

- In active attacks the content of the original message are modified in the some way.
- Active attacks are based on modification of the original message in some manner or the creation of a false message.

Types of Active Attacks

- Masquerade or interruption
- Modification
- Fabrication or denial of service

Masquerade or Interruption

- Masquerade is caused when an unauthorized entity pretends to be an other entity.
- For example like authentication, user c might pose as user A and send a message to user B. So in this attack an entity poses as another entity.

Modification

- Reply Attacks
- Alterations

Replay Attacks

- In replay attacks a user captures a sequence of message or some data units and resends them.
- For example suppose user A wants to transfer some amount to user C's bank account. Both user A and C have accounts with bank B.
- User A might send an electronic message to bank B requesting for the funds transfer, user C could capture this message and send a second copy of the same to bank B.

Cont…

- Bank B would have no idea that this is an unauthorized message and would treat this is as a second and different funds transfer request from user A.
- Therefore user C would get the benefit of the funds transfer twice, once authorized and once unauthrized.

Alterations

- This is involves some change to the original message for example suppose user A sends an electronic message transfer 1000 rs to D's account to bank B, user C might capture this and change it to transfer 10000 rs to C's accounts.

Fabrication or DOS

- This attacks make an attempt to prevent legitimate users from accessing some services which they are eligible.
- For example an unauthorized user might sends too many login request to a server using random user ids one after the an other in quick session so as to flood the network and deny other legitimate users from using the network facilities.