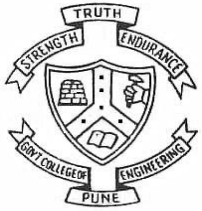
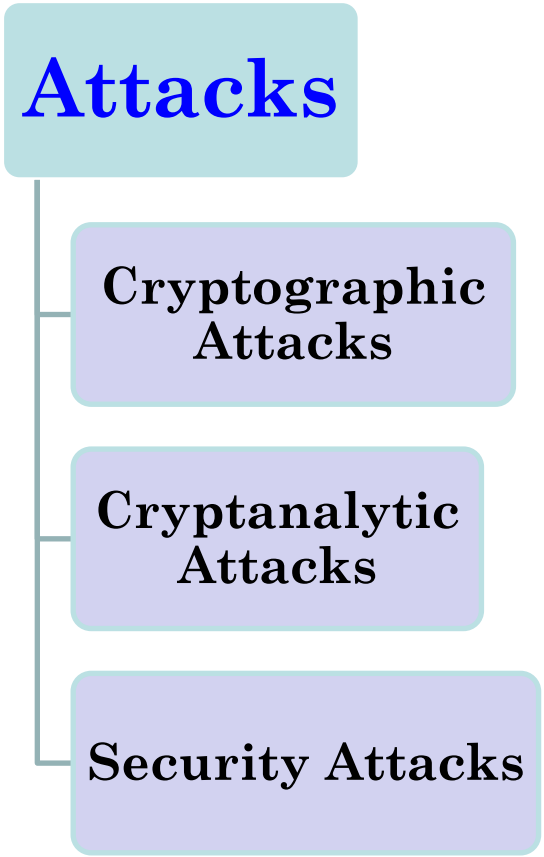
Cryptography and Network Security
Session III

Dr. V. K. Pachghare



Attacks


Attacks
Cryptographic Attacks
Cryptanalytic Attacks
Security Attacks

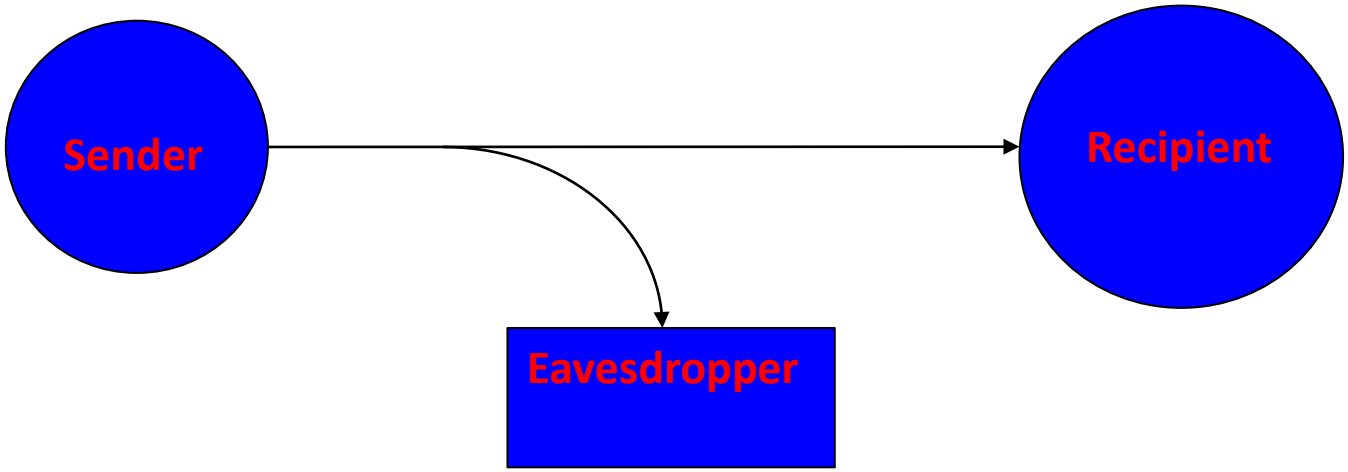
Cryptographic Attacks

- **Passive attacks**
  - Attempts to learn or make use of information from the system but does not affect system resources
  - Ex. Capture the password and use it for login
- **Active attacks**
  - Attempts to alter system resources or affect their operation
  - Ex. Capture the password and modify it

Passive Attacks

Eavesdropping (**Eavesdropping** is the act of secretly listening to the private conversation of others without their consent on), or monitoring of, transmissions to:

- obtain message contents, or
- monitor traffic flows


Sender
Recipient
Eavesdropper

Types of Passive Attacks

1. Release of message contents
2. Traffic analysis

These attacks are very difficult to detect because they do not involve any alteration (modification) of the data.

Release of message contents

A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information.

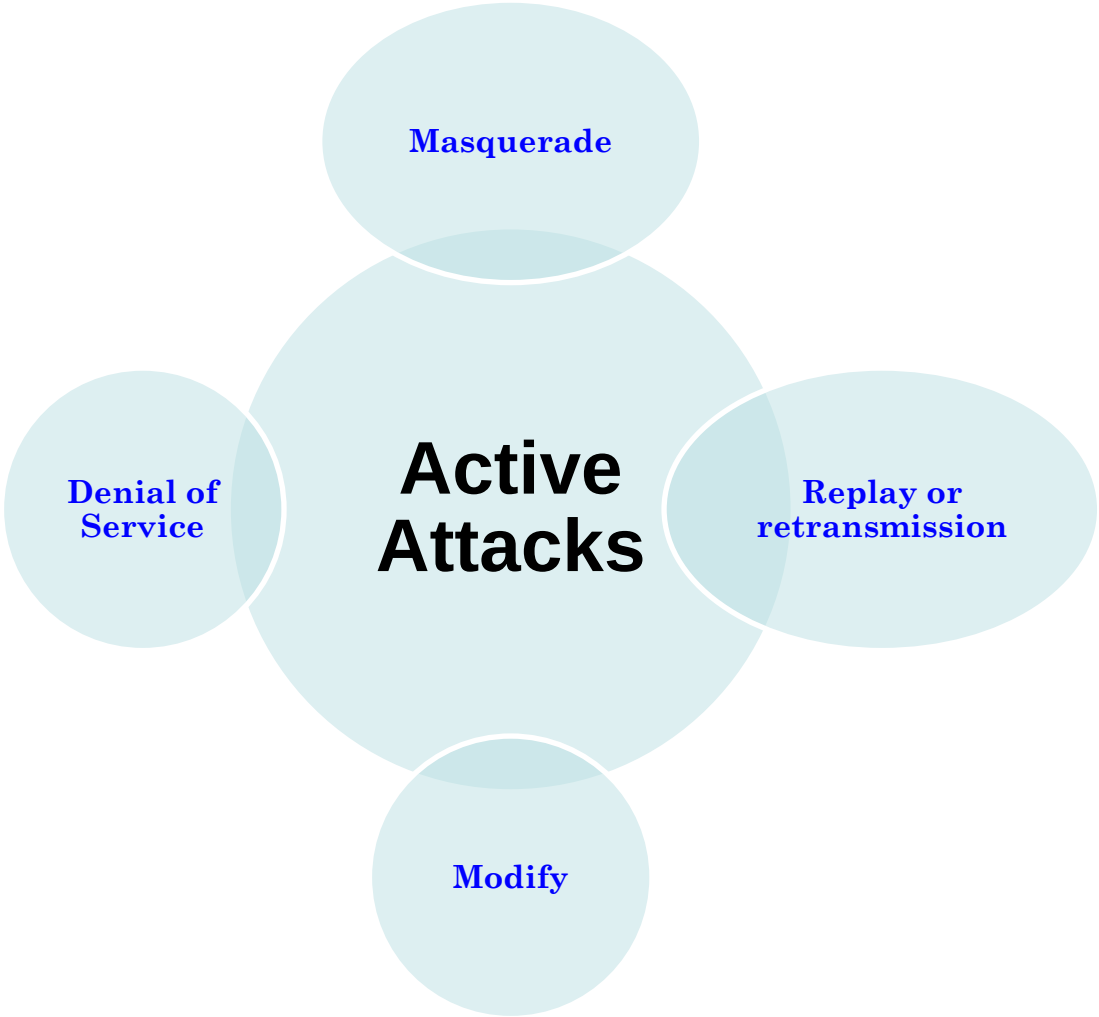
We would like to prevent the attackers from learning the contents of these transmissions.

Traffic analysis

- An attacker might be able to observe the pattern of the encrypted message.
- An attacker could determine the location and identity of hosts and could observe the frequency and length of messages being exchanged.
- This information might be useful in guessing the nature of communication that was taking place.

Active Attacks

Modification of data stream or the creation of false stream


Masquerade
Denial of Service
Active Attacks
Replay or retransmission
Modify

Types of Active Attacks

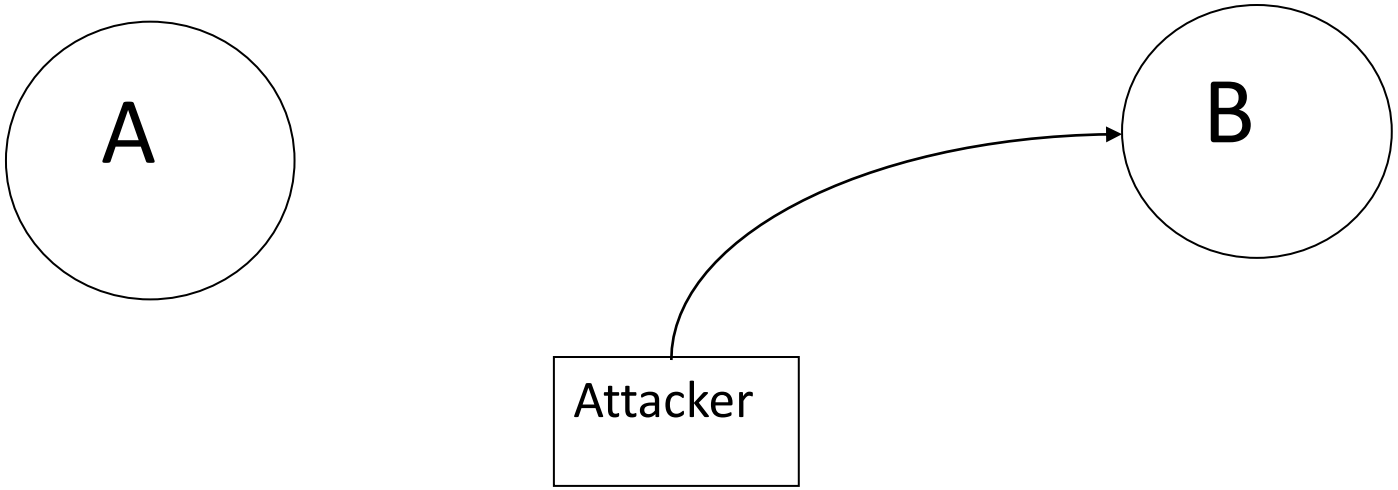
Masquerade of one entity pretends to be a different entity

Replay or retransmission of previous messages

Modify messages in transit

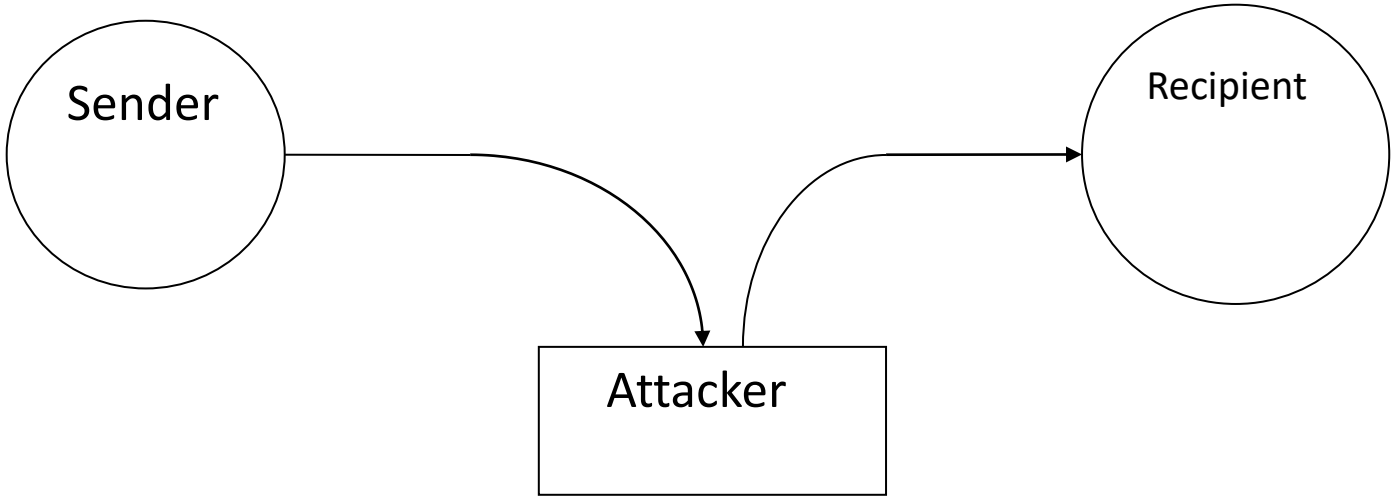
Denial of Service (DoS) Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance.

Masquerade

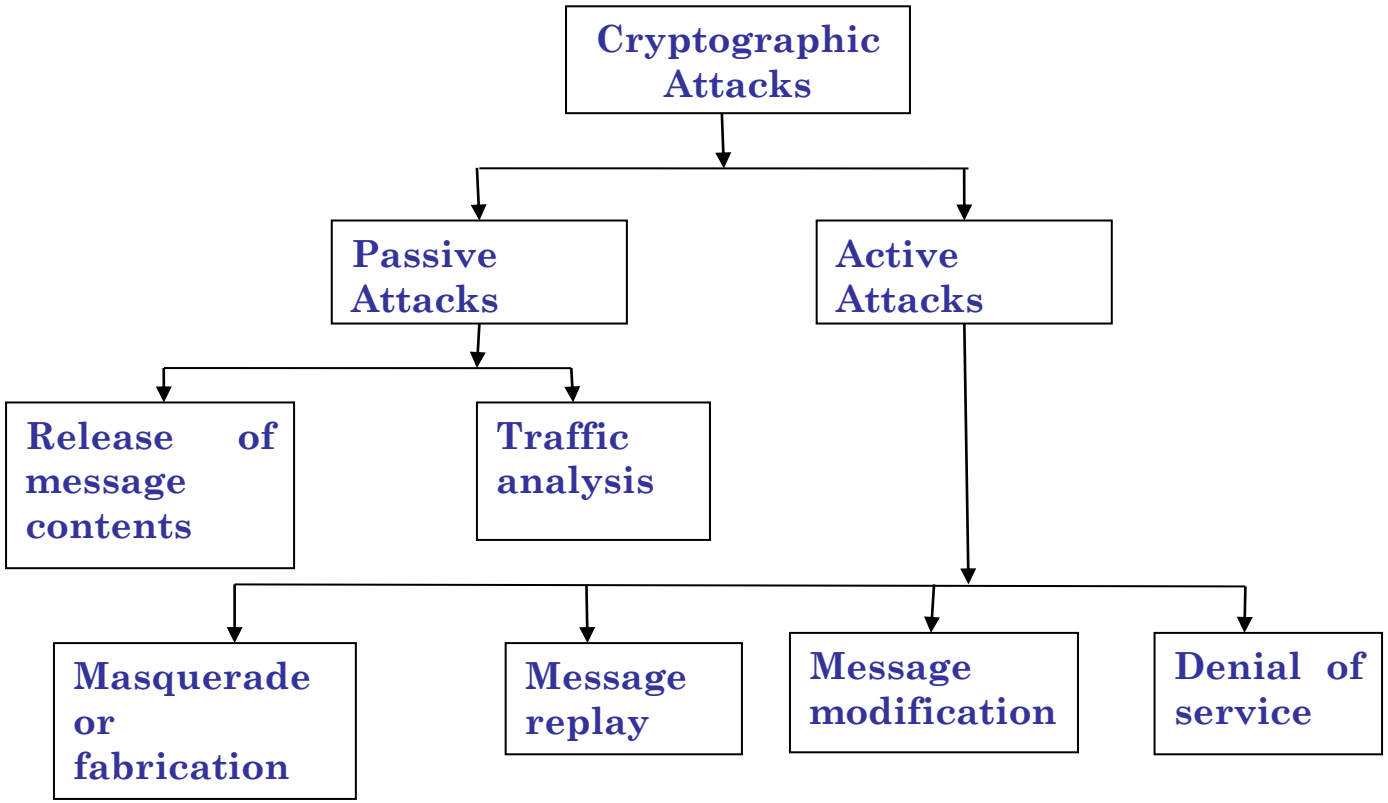


Active Attack- **Masquerade**

Replay Attack



Active Attack - Message Replay


Cryptographic Attacks
Passive Attacks
Active Attacks
Release of message contents
Traffic analysis
Masquerade or fabrication
Message replay
Message modification
Denial of service

Cryptanalysis

- The process of attempting to discover plaintext or key or both is known as cryptanalysis.
- The strategy used by the cryptanalysis depends on the nature of the encryption scheme and the information available to the cryptanalyst.

Cryptanalytic Attacks

Cryptanalytic attacks are perform on the encrypted messages

- Ciphertext Only
- Known Plaintext
- Chosen Plaintext
- Chosen Ciphertext

- **Ciphertext only –** The encryption algorithm and the cipher text are known to the cryptanalyst.
- **Known plaintext –** The encryption algorithm, the cipher text and corresponding plaintext are known to the cryptanalyst.
- **Chosen plaintext –** The encryption algorithm and the cipher text are known to the cryptanalyst. Cryptanalyst chooses the plaintext. They can encrypt a large number of suitably chosen plaintexts and try to use the resulting cipher texts to deduce the key.

- **Chosen cipher text –** The encryption algorithm and the cipher text are known to the cryptanalyst. The cryptanalyst obtains temporary access to the decryption machine, uses it to decrypt several string of symbols, and tries to use the results to deduce the key.

Security Attacks

Security attacks are

- Interruption
- Interception
- Modification
- Fabrication

Interruption Attack

- An asset of the system is **destroyed or becomes unavailable or unusable**.
- This is an attack on availability

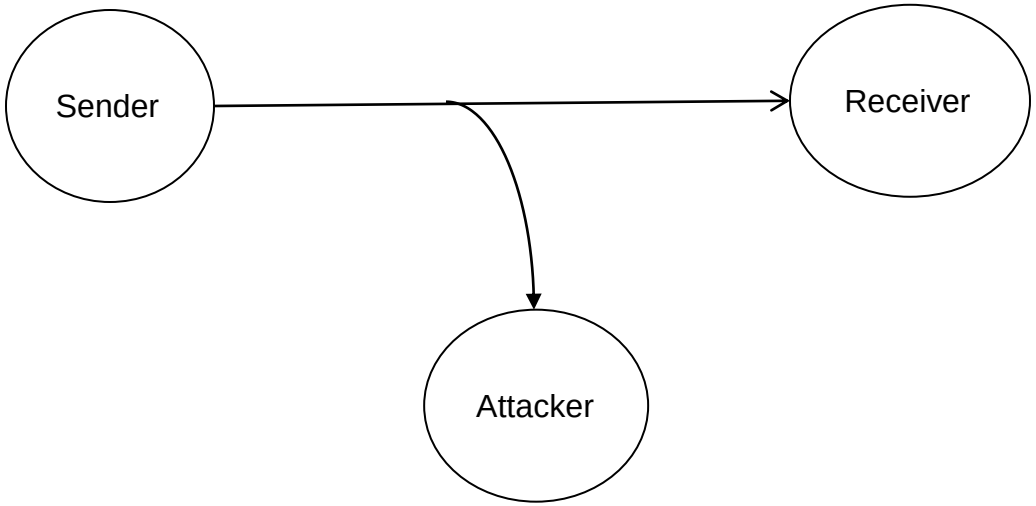
  e.g., destruction of piece of hardware, cutting of a communication line or Disabling of file management system.

Interception Attack

- An unauthorized party **gains access** to an asset.
- This is an attack on confidentiality.
- Unauthorized party could be a person, a program or a computer.

  e.g., wire tapping to capture data in the network, illicit copying of files

Interception Attack

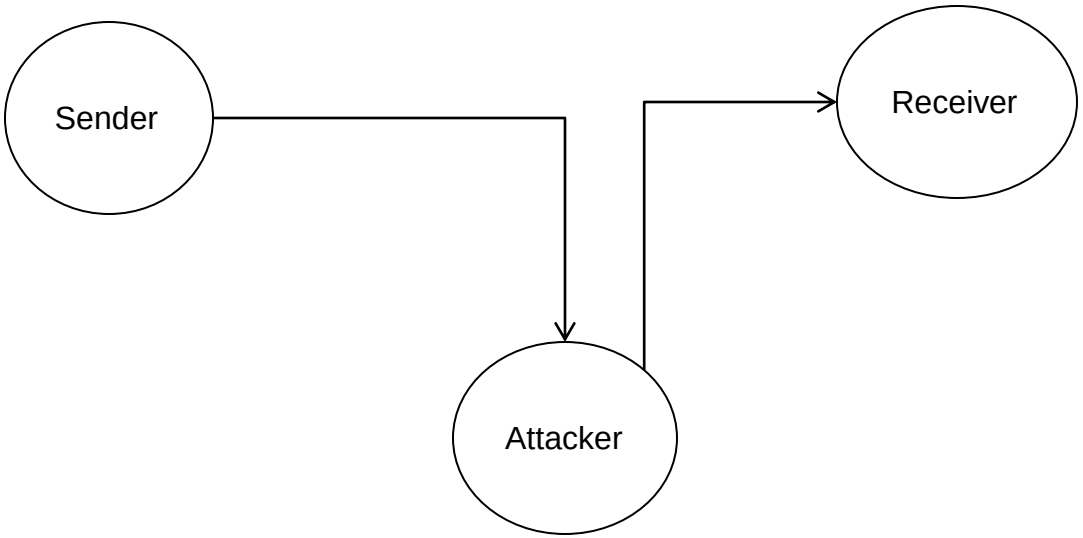


Modification Attack

- An unauthorized party not only gains access to but **tampers with an asset**.
- This is an attack on integrity.

  e.g., changing values in data file, altering a program, modifying the contents of messages being transmitted in a network.

Modification Attack

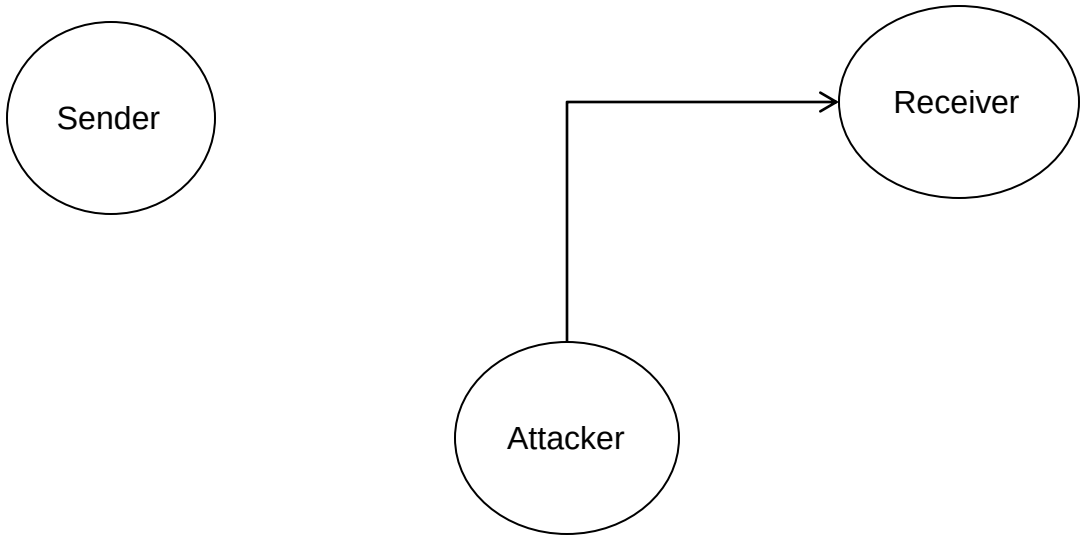


Fabrication Attack

- An unauthorized party **inserts counterfeit** objects into the system.
- This is an attack on authenticity.

  e.g., insertion of spurious message in a network or addition of records to a file.

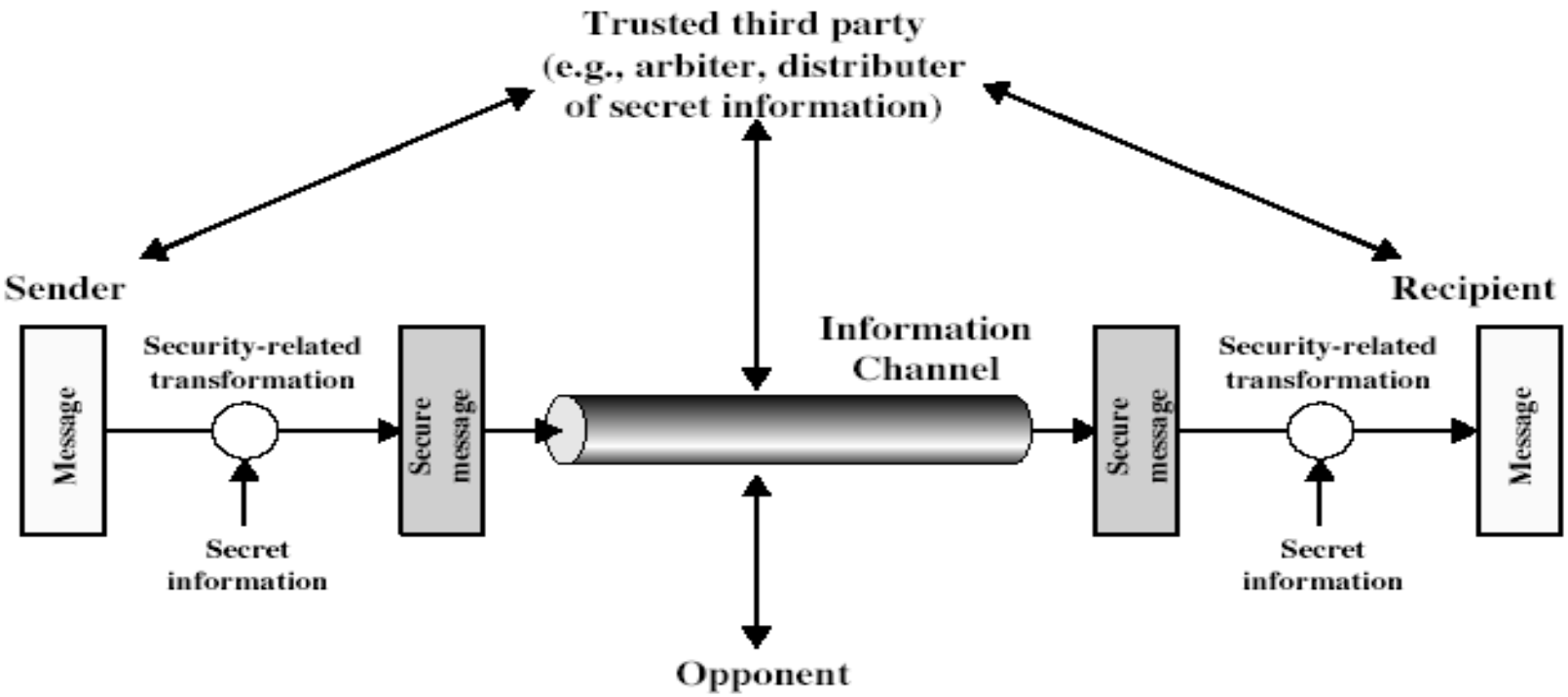
Fabrication Attack



Security Attacks

Attack Type	Attack Against	Affected Security Services
Interruption	Resources are destroyed or becomes unavailable	Availability
Interception	Gains access to an asset	Confidentiality
Modification	Tampers with an asset.	Integrity
Fabrication	Inserts counterfeit objects	Authenticity

Model for Network Security



Model for Network Security

- using this model requires us to:
  - design a suitable algorithm
  - generate the secret information (keys)
  - develop methods to distribute and share the secret information
  - specify a protocol enabling the principals to use the transformation and secret information for a security service

One-Time Pad
or
Vernam Cipher

- Different messages are encrypted by different key streams.

Three essential properties are:

- The number of possible keys is equal to the number of possible plaintexts
- The key is selected at random
- The key should be used only once

$$CT = (PT \oplus K) \bmod 26$$

OR

PT	K	CT = PT ⊕ K
0	0	0
0	1	1
1	0	1
1	1	0

EXAMPLE

Message: WE LIVE IN A WORLD FULL OF BEAUTY

Key: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Encryption

PLAINTEXT	W	E	L	I	V	E	I	N	A	W	O	R	L	D	F	U	L	L	O	F	B	E	A	U	T	Y
	22	04	11	8	21	4	8	13	0	22	14	17	11	3	5	20	11	11	14	5	1	4	0	20	19	24
OTP KEY	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
RESULT	22	5	13	11	25	9	14	20	8	31	24	28	23	16	19	35	27	28	32	24	21	25	22	43	43	49
MOD 26	22	5	13	11	25	9	14	20	8	5	24	2	23	16	19	9	1	2	6	24	21	25	22	17	17	23
CIPHERTEXT	W	F	N	L	Z	J	O	U	I	F	Y	C	X	Q	T	J	B	C	G	Y	V	Z	W	R	R	X

The ciphertext is "WFNLZJOUIFYCXQTJBCGYVZWRRX"

Decryption

CIPHERTEXT	W	F	N	L	Z	J	O	U	I	F	Y	C	X	Q	T	J	B	C	G	Y	V	Z	W	R	R	X
	22	5	13	11	25	9	14	20	8	5	24	2	23	16	19	9	1	2	6	24	21	25	22	17	17	23
OTP KEY	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
RESULT	22	4	11	8	21	4	8	13	0	−4	14	−9	11	3	5	−6	−15	−15	−12	5	1	4	0	−6	−6	−2
MOD 26	22	4	11	8	21	4	8	13	0	22	14	17	11	3	5	20	11	11	14	5	1	4	0	20	20	24
PLAINTEXT	W	E	L	I	V	E	I	N	A	W	O	R	L	D	F	U	L	L	O	F	B	E	A	U	T	Y

Steganography

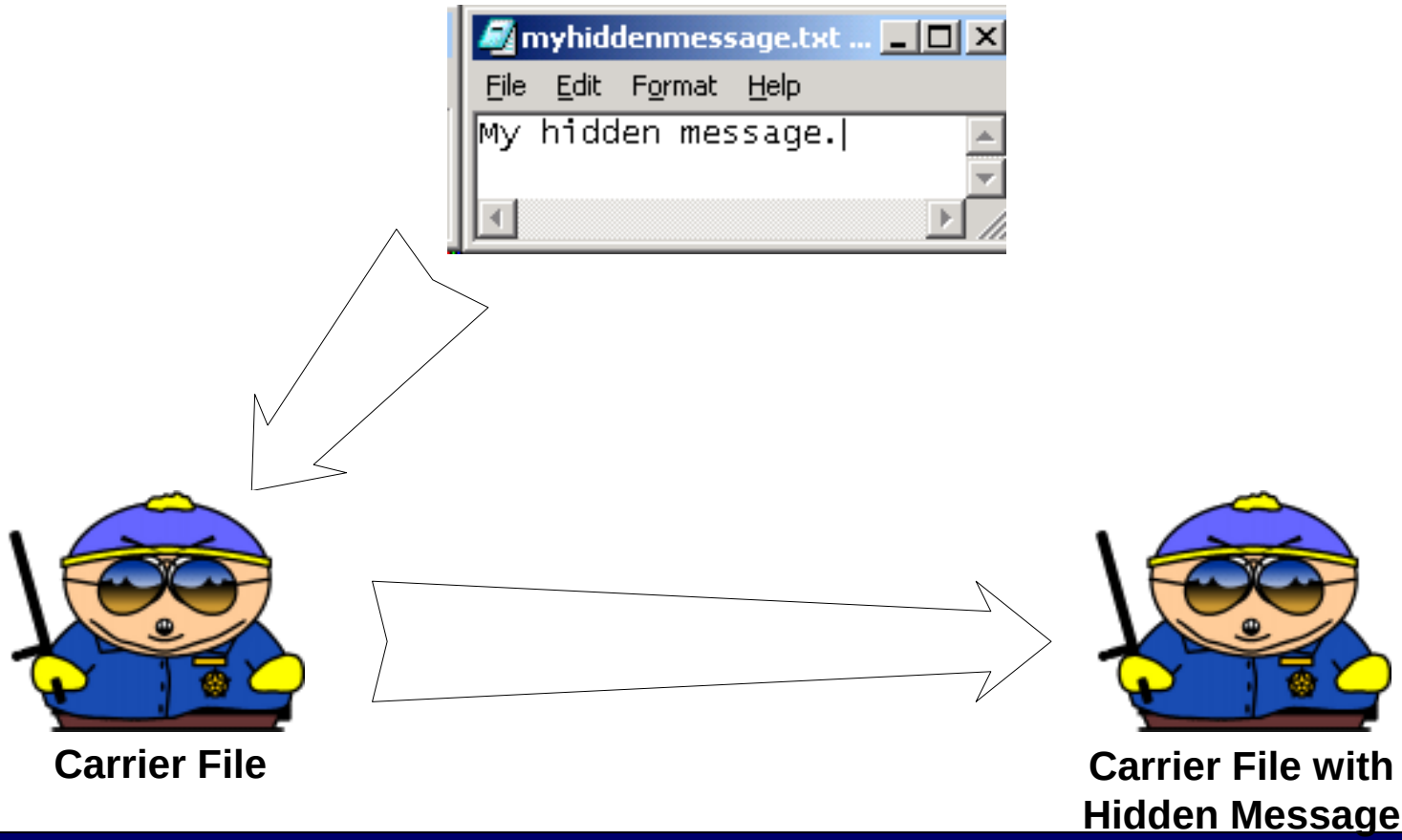
From the Greek word steganos meaning "covered"
and the Greek word graphie meaning "writing"

Steganography is the process of hiding of a secret message within an ordinary message and extracting it at its destination

Anyone else viewing the message will fail to know it contains hidden/encrypted data

- Modern digital steganography
  - data is encrypted
  - then inserted and hidden, using a special algorithm which may add and/or modify the contents of the file
  - This technique may simply append the data to the file, or disperse it throughout
  - Carefully crafted programs apply the encrypted data such that patterns appear normal.

Steganography – Modern Day



Steganography – Carrier Files

Steganography Carrier Files

- bmp
- jpeg
- gif
- wav
- mp3
- Amongst others…

Steganography - Tools

Steganography Tools

- Steganos
- S-Tools (GIF, JPEG)
- StegHide (WAV, BMP)
- Invisible Secrets (JPEG)
- JPHide
- Camouflage
- Hiderman
- Many others…