OSI Security Architecture

- open systems Interconnections
- The security of an organization is the greatest concern of the people working at the organization
- safety and security are the pillars of cyber technology.
- The OSI security Architecture defines a systematic approach to providing security at each layer.
- OSI security Architecture focuses on these concepts
  - a) security Attack
  - b) security machanism
  - c) security service

1. security Attack

- Action that compromises the security of an individual or an organization
- security Attack has 2 types of attacks

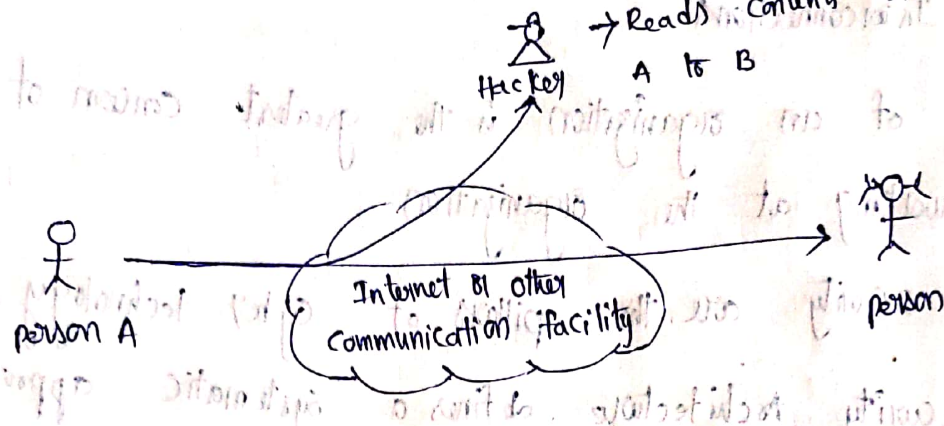
a) passive attack

- attempts to learn or make use of information from the system
- Does not affect system resources
- Eavesdropping or monitoring of transmissions
- The Goal is obtain information that is being transmitted

Types:

1. Release of message contents
2. Traffic Analysis

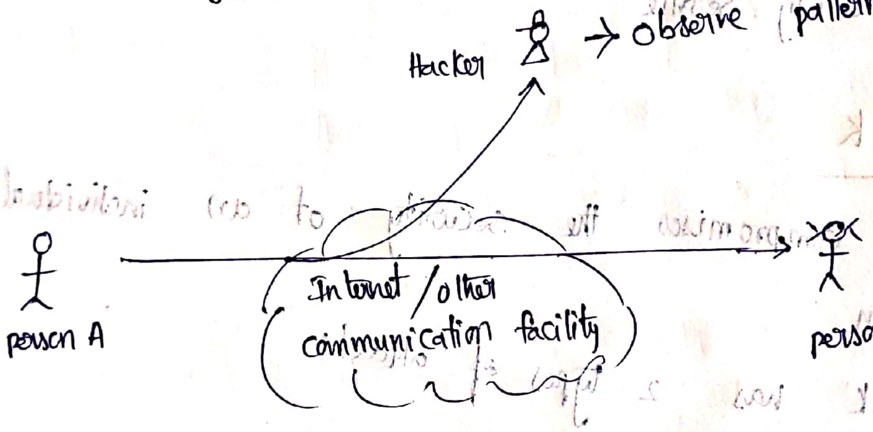
a.1) Release of message contents



→ Reads contents of message from A to B

* To prevent this problem. before Sending the message to Person B person A must Encrypt the message and person B alone Decrypt the message

a.2) Traffic Analysis



→ observe pattern of messages A to B

* After sending Encrypted message, if Hacker reciene that Encrypted message difinitely that hacker not be able to understand the message

* But, he knows the location, user/ Sender Identity ~~of~~ and length of message.

* using that information he knows the nature of the message

b) Active Attack

- Active attacks involve some modification of the data stream or the Creation of a file stream
- it divided into 4 categories

b.1) Masquerade

- Hacker can send the massages to person B using person A Login
- person B thinks that person A is sending messages

b.2) Replay

- person A sends the message to person B, but Hacker will store the all messages
- later Hacker will send all messages to person B

b.3) Modification of message

- Here Hacker modify the message and sends to person B

b.4) Denial of Service

- person A needs to work with Server
- Hacker will overload the Server at the same time
- Then person A will not able to acces the server

2. Security mechanisms

* security mechanisms divides into 2 mechanisms

a) specific security mechanisms

a.1) Encipherment : it is ciphering techinique, converting plan text data into Intent to cipher text before sending the

a.2) Digital signature : it is a piece of code, it gives the Currect Identity of actual sender.

a.3) Access control : it gives access rights to the user.

a.4) Data Integrity : what sender is sending, the Data that Data alone will receive by reciever

a.5) Authentication Exchange : small piece of Information will exchange b/t 2 persons/ entities by Authentication

a.6) Traffic padding : it create dummy data stream to avoide Hacker messages

a.7) Routing control : it secures the Data from Hackers

a.8) Notarization : we are doing to deploy some 3rd party

b) Pervasive Security Mechanisms

b.1) Trusted functionality

b.2) Security Label

b.3) Event Detection

b.4) security Audit Trail

b.5) Security Recovery

3. Security Services

- The processing or communication service that is provided by a system to give a specific kind of protection to system resources
- security services implement security policies and are implemented by security mechanisms.

a. Authention

a.1) peer entity authentication

- reciever confirms ~~that~~ the Data sent by valid sender or not with the help of peer entity authentication / node will confirm

a.2) Data origin authentication

- same as peer entity authentication but Here reciver directly verify the valid sender

b) Access control

- control the Access

b) Data Confidentiality

- Data will protected

c) Data Integrity

- Reciver directly recive the Data from sender

Unit - I

Hill Cipher

- Hill Cipher is substitution technique
- Multi-letter cipher
- Encrypts a group of letters : digraph, trigraph or polygraph
- Concepts to be known
  1. Matrix arithmetic Modulo 26
  2. square matrix
  3. Determinant
  4. Multiplicative inverse

Algorithm

Encryption

$C = E(K, P)$

$= P * K$ mode 26

C - Cipher text

E - Encryption

K - Key Matrix /value

P - plan text matrix /value

$\boxed{\text{Suppose}}$

$$(C_1\ C_2\ C_3) = (P_1\ P_2\ P_3)\begin{pmatrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{pmatrix} \bmod 26$$

$\boxed{\text{based on question}}$

$C_1 = (P_1 K_{11} + P_2 K_{21} + P_3 K_{31}) \bmod 26$

$C_2 = (P_1 K_{12} + P_2 K_{22} + P_3 K_{32}) \bmod 26$

$C_3 = (P_1 K_{31} + P_2 K_{23} + P_2 K_{33}) \bmod 26$

Decryption

$P = D(K, C)$

$= C K^{-1} \bmod 26$

$= P * K * K^{-1} \bmod 26$

D - Decryption

Q. Encrypt "pay more money" using Hill cipher with key

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}_{3 \times 3}$$

Sol

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

s	t	u	v	w	x	y	z
18	19	20	21	22	23	24	25

→ using above formate we can write the numbers for given plaintext

p	a	y	m	o	r	e	m	o	n	e	y
15	0	24	12	14	17	4	12	14	13	4	24

→ given key matrix is 3 x 3 so we can Encrypt the plaintext as 3 letters

- Key = 3 x 3 matrix

PT = pay mor emo ney

1. Encrypting : pay

$$(c_1\ c_2\ c_3) = (15\ \ 0\ \ 24)\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$= (15 \times 17 + 0 \times 21 + 24 \times 2 \quad 15 \times 17 + 0 \times 18 + 24 \times 2 \quad 15 \times 5 + 0 \times 21 + 24 \times 19) \bmod 26$$

$$= (303 \quad 303 \quad 531) \bmod 26$$

$= (17 \quad 17 \quad 11)$

$= (r \quad r \quad l)$

2. Encrypting : mor

$$(c_1 \quad c_2 \quad c_3) = (12 \quad 14 \quad 17) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$= (552 \quad 490 \quad 677) \bmod 26$

$= (12 \quad 22 \quad 1)$

$= (m \quad w \quad b)$

3. Encrypting : emo

$$(c_1 \quad c_2 \quad c_3) = (4 \quad 12 \quad 14) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$= (348 \quad 312 \quad 538) \bmod 26$

$= (10 \quad 0 \quad 18)$

$= (k \quad a \quad s)$

4. Encrypting : ney

$$(c_1 \quad c_2 \quad c_3) = (13 \quad 4 \quad 24) \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$= (353 \quad 341 \quad 538) \bmod 26$

$= (15 \quad 3 \quad 7)$

$= (p \quad d \quad h)$

PT = p a y m o r e m o n e y

CT = r r l m w b k a s p d h

Decryption

$$P = C\,K^{-1} \bmod 26$$

$$= P * K * K^{-1} \bmod 26$$

$$K^{-1} = \frac{1}{\text{Det } K} \times \text{Adj } K$$

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$

1. Det K mod 26

$$\text{Det } K = \text{Det} \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \bmod 26$$

$$= \left(17\,(18*19 - 2*21) - 17\,(21*19 - 2*21) + 5\,(21*2 - 2*18)\right) \bmod 2$$

$$= \left(17\,(300) - 17\,(357) + 5\,(6)\right) \bmod 26$$

$$= (5100 - 6069 + 30) \bmod 26$$

$$= -939 \bmod 26$$

$$= -3 \bmod 26$$

↳ if we get -ve number just add -ve number and mod value

$$\boxed{\text{Det } K = 23}$$

2. Adj K

$$\text{Adj } K = \begin{vmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{vmatrix} \bmod 26$$

→ take 1st 2 columns and repeat again

$$\text{Adj } K = \begin{vmatrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \\ 2 & 4 & 19 & 2 & 4 \end{vmatrix} \bmod 26$$

→ take 1st 2 rows and repeat again

$$\text{Adj } K = \begin{vmatrix} 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \\ 2 & 4 & 19 & 2 & 4 \\ 17 & 17 & 5 & 17 & 17 \\ 21 & 18 & 21 & 21 & 18 \end{vmatrix} \bmod 26$$

→ Ignore the 1st column and 1st row

$$\text{Adj } K = \begin{vmatrix} \cancel{17} & \cancel{17} & \cancel{5} & \cancel{17} & \cancel{17} \\ \cancel{21} & 18 & 21 & 21 & 18 \\ \cancel{2} & 4 & 19 & 2 & 4 \\ \cancel{17} & 17 & 5 & 17 & 17 \\ \cancel{21} & 18 & 21 & 21 & 18 \end{vmatrix} \bmod 26$$

⇒ performing the operation - column wise

Entering the matrix - Row wise

$$\text{Adj}\,K = \begin{vmatrix} 18 & 21 & 21 & 18 \\ 2 & 19 & 2 & 2 \\ 17 & 5 & 17 & 17 \\ 18 & 21 & 21 & 18 \end{vmatrix} \bmod 26$$

$$= \begin{vmatrix} \textcircled{1}\,18(19) - 2(21) & \textcircled{2}\,2(5) - 17(19) & \textcircled{3}\,17(21) - 18(5) \\ \textcircled{4}\,21(2) - 19(21) & \textcircled{5}\,19(17) - 5(2) & \textcircled{6}\,5(21) - 21(17) \\ \textcircled{7}\,21(2) - 2(18) & \textcircled{8}\,2(17) - 17(2) & \textcircled{9}\,17(18) - 17(21) \end{vmatrix} \bmod 26$$

$$= \begin{vmatrix} 300 & -313 & 267 \\ -357 & 313 & -252 \\ 6 & 0 & -51 \end{vmatrix} \bmod 26$$

⟶ do mod operation on Every Element

$$= \begin{vmatrix} 14 & -1 & 7 \\ -19 & 1 & -18 \\ 6 & 0 & -25 \end{vmatrix} \bmod 26$$

$$\text{Adj}\,K = \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \bmod 26$$

3. $$K^{-1} = \frac{1}{23} \times \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \text{mod } 26$$

$$= 23^{-1} \times \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \text{mod } 26$$

$23^{-1} \times 23 = 1 \mod 26$

$\underline{17} \times 23 = 1 \mod 26$

$$= 17 \times \begin{pmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{pmatrix} \text{mod } 26$$

$$= \begin{pmatrix} 238 & 425 & 119 \\ 119 & 17 & 136 \\ 102 & 0 & 17 \end{pmatrix} \text{mod } 26$$

$$K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

- How to check K^{-1} matrix is correct
- do $K \times K^{-1}$ mod26, if we get any Identity matrix then K^{-1} is correct

$$K K^{-1} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \text{mode } 26$$

$$= \begin{pmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} \text{mod } 26$$

$$= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

PT = pay more money }
CT = rrl mwbk aspdh } Encryption

$P = C K^{-1} \bmod 26$

r	r	l	m	w	b	k	a	s	p	d	h
17	17	11	12	22	1	10	0	18	15	3	7

a Decrypting : rrl

$$(P_1 \ P_2 \ P_3) = (17 \ 17 \ 11) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$= (587 \ 442 \ 544) \bmod 26$

$= (15 \ 0 \ 24)$

$= (p \ a \ y)$

b Decrypting : m w b

$$(P_1 \ P_2 \ P_3) = (12 \ 22 \ 1) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$= (402 \ 482 \ 329) \bmod 26$

$= (12 \ 14 \ 17)$

$= (m \ o \ r)$

c. Decrypting : kas

$$(P_1 \quad P_2 \quad P_3) = (10 \quad 0 \quad 18) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$= (472 \quad 90 \quad 456) \bmod 26$$

$$= (4 \quad 12 \quad 14)$$

$$= (e \quad m \quad o)$$

d. Decrypting : pdh

$$(P_1 \quad P_2 \quad P_3) = (15 \quad 3 \quad 7) \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} \bmod 26$$

$$= (273 \quad 186 \quad 362) \bmod 26$$

$$= (13 \quad 4 \quad 24)$$

$$= (n \quad e \quad y)$$

CT	=	r	r	L	m	w	b	k	a	s	p	d	h
PT	=	p	a	y	m	o	r	e	m	o	n	e	y

* Model for Network Security

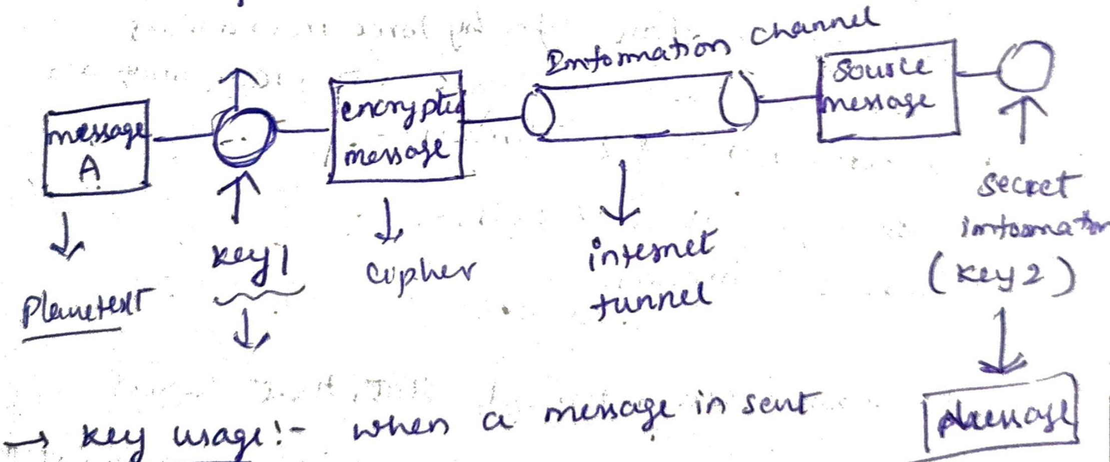
→ A model for which creates authentication and security mechanism to transfer a message from user A to user B in internet

→ while processesing and sending message in internet we need to take care about the security mechanism

→ The security of the message without attacking from third party people by encrypting the message by using some physical quantity

→ Now, we need to create some quantity of values (or) algorithem to encrypt and decrypt

→ There are many algorithems for encrypting and decryption but all the algorithems uses 2 keys public key and private key



→ Key usage:- when a message in sent in any social media acount the message first gets encrypted to some form of some n-bit length to Reduce the load of model

→ encrypt message storage is a online created buffer with limited time of accessing and that encrypted message is stored in that buffer

→ Internet tunnel is the place when the network signals processing units are present like internet prividers, service providers, Network towers etc)

→ Now, the message is sent to the other person, by using TCP/IP server mechanism the data gets authenticated and verified at the buffer storage

→ The encrypted message gets decrypted and send the message to the user B.

→ By the above example we can say that the security is done by ~~by~~ three mechanisms

The threads which are there in predictiting service models:-

→ Information access threads:-

→ ~~do~~ login access threads:-

→ Service threads.

Information access thread states that when the message is sent from one person to other person wrt to security attack model the data gets encrypted, so we should not allow third party people to access our data elements

→ login access controle:- login access controle states that when our message data is safely encrypted but our social media login creditionals can be stoled if they were not secured, then our data gets hacked easily.

→ service access controle!- service access controle states that while encrypting we use some algorithem and if the hacker can decode that encryption technique then the data cannot be safely authenticated

→ By the following risks we can authenticate easily.