UNIT-I:

Security Concepts:-

Introduction -
The need for security -
Security approaches -
principles of security -
Types of security attacks
Security services
Security mechanisms -
A model for Network Security

Cryptography Concepts & Techniques:-

Introduction
plain text & cipher text -
Substitution techniques.
Transposition techniques
Encryption & decryption -
Symmetric & Asymmetric key cryptography
Steganography
key range & key size
possible types of attacks.

* Security Concepts

Security Concepts are the fundamental principles used to protect information and systems from threats, primarily focusing on confidentiality, integrity & availability.

→ These principles ensure that information is protected from unauthorized access, is accurate & unaltered & is accessible when needed.

Core Security Concepts:-

- Confidentiality:- Info is acc only to authorized people.
- Integrity:- Ensures data is accurate, consistent
- Availability:- Ensures systems & data are acc whenever needed
- Authentication:- Verifying the identity of a user(or) device
- Authorization:- Determines what an authenticated user can access or do
- Accounting:- Recording & tracking user activities
- Risk management:- Identifying, evaluating & mitigating risks.

* The Need for Security :-

→ Modern communication systems like the Internet, wireless network, & mobile devices - transmit huge amounts of data every second.

→ The data is often sensitive, such as passwords, bank information, personal messages, business transactions. because this data travels through open networks, it becomes vulnerable to attackers.

→ Therefore, security is essential to protect data & systems.

Key needs for security :-

• Confidentiality :- Cryptography, through techniques like encryption, keeps sensitive data private from unauthorized viewers.

• Integrity : Both fields ensure that a data has not been altered during transmission or storage.

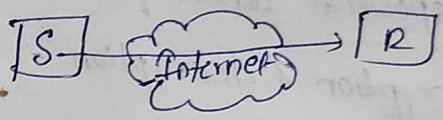
• Availability : Network security measures like firewalls & intrusion prevention systems work to ensure that systems & n/w are available

• Authentication : CNs provide mechanism to verify the identity of users & systems, ensuring that you are communicating with the intended party.

• Secure communication :- They enable secure channels for communication such as email, online purchases

* It is about how to secure our data from third party

* we should make sure that the information is delivered to the reciever without modifications.



* The communication blw sender & Reciever will obviously take place through internet.

* whenever we are sending information to reciever, we should make sure that no third party will be having access to this information.

* If any third party is having access the info that you are sending to the reciever then the data is corrupted.

* The corrupted data is nothing but the data may be change (or) confidentiality of the data may be lost.

* whenever we are sending info from sender to reciever, two process will takes place 1) encryption
2) decryption

Enc: converting plain text (Hello) to cipher text (#@?12)

Dec: It converts cipher text to plain text.

---

* Security Approaches:-

-) It involves technical methods like encryption, digital signatures & authentication to protect data & systems, alongside strategic organizational approaches like a top-down strategy that establishes policies & allocates resources from leadership.

There are three ways that we can approach the security

1) prevention
2) protection
3) Resilrence

① prevention: It will prevent the threats by identifying the underlying causes before they occur

* It happens before the occurance of threats.

2) protection:- It takes place, when the threats are ready to occur.

3) Resilrence: Here, the threat will already occur.. when we are not in a position to control a threat then we have to adopt a mechanism (or) method (or) write a program through which the threat can be solved.

The most effective security approach involves a defence-in-depth model, combining these methods across physical, technical & administrative layers.

for example, a VPN uses cryptographic encryption (confidentiality, integrity) while a firewall provide access control.

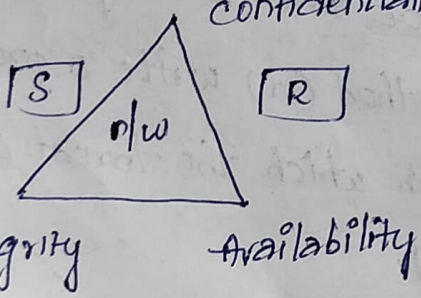
---

* Principles of Security:-

→ The fundamental principles of security revolve around protecting information and systems.

→ The core framework is the CIA triad (confidentiality, Integrity & Availability).

* whenever we are sending info from sender to reciever, we have to maintain this CIA Triad for a proper and reliable communication



* Confidentiality:- It is nothing but confidential data (or) confidential message should be kept in secret.

• It protects data from unauthorized disclosure.

• Encryption is a key mechanism for achieving confidentiality, ensuring that even if data is intercepted.

* Integrity: Integrity guarantees the accuracy, consistency of data.

→ It prevents accidental modification, alteration of information. Hash functions and digital signatures are commonly used to verify that the data has not been tampered with. S 1234 → R 1234 (ex: 1234 → 1234)

* Availability: This principle ensures that systems, applications & data are accessible to authorized users when needed.

* whatever the data we are sending from sender to the Reciever it should be available in all forms.

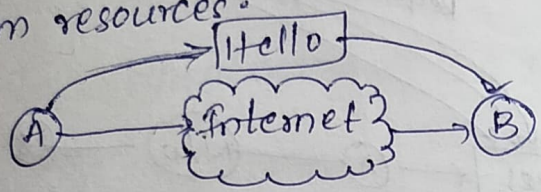
* The Reciever should be able to read the data & write the data, modify the data.

Types of Security Attacks:-

An attack is nothing but any action that compromises the security of information

Types of attack:-

i) passive attack :- It attempts to learn or make use of information from the system but does not affect system resources.



(c) read
Third party.

whenever the data sending from the sender to reciever, the third party can only read the data & observe the data without any modifications.

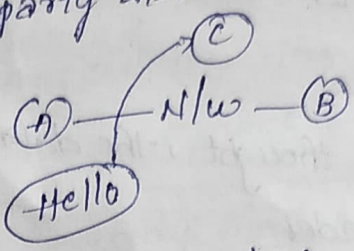
There are divided into two categories:

i) Release of message contents

ii) Traffic analysis.

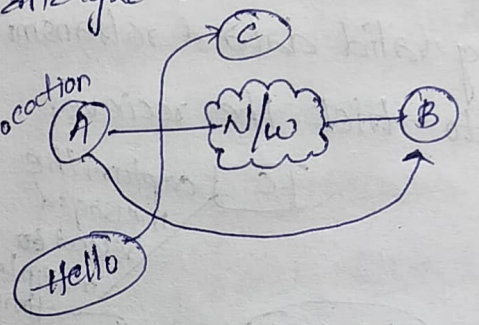
i) Release of message contents:

* whenever the data we are sending from sender to reciever, the data will be released to third party also



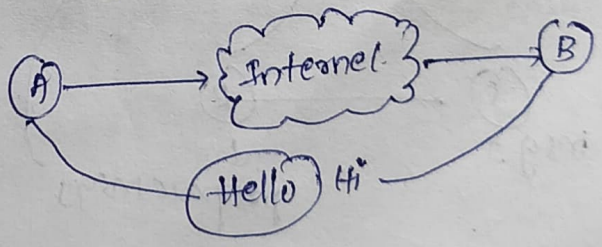
ii) Traffic analysis:-

* whenever the data we are sending from sender to Reciever, third party try to observe and analyze the movement of the data.



I) Active Attacks:-

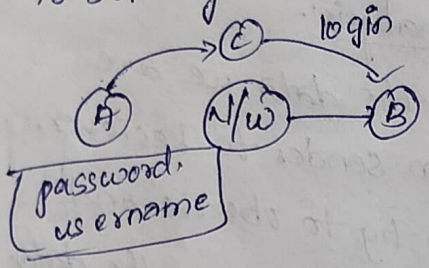
whenever the ~~data~~ we are sending the data from sender to reciever, the third party can read, write modify the data (c) Third party



i) Masquerade Attack.

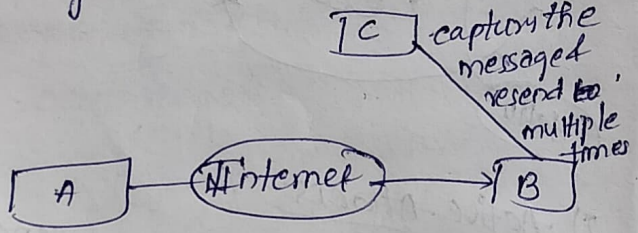
Whenever the data we are sending from sender to reciever, the third party will stolen the data and it modify the data & sends to the Reciever

- But reciever thought, the data is send by sender



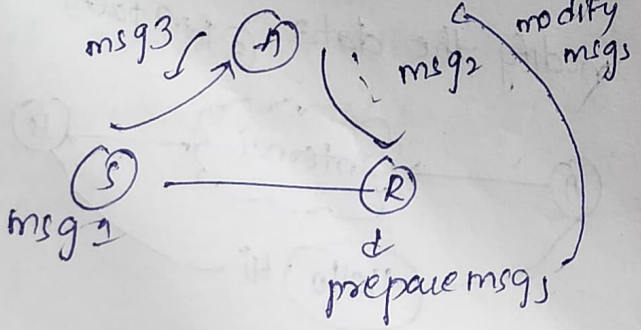
ii) Replay:

- Capturing valid data & retransmitting it to trick the reciever



iii) Modification Attack:

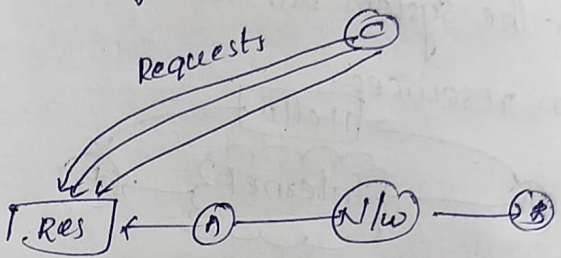
→ Altering or tampering with data in transit



iv) Daniel of Services

whenever sender want to access same resource, third party wantedly send multiple requests to the resource

- In that case, running capacity of Resource will be slow docon
- Then sender has to wait & suffer
- Finally sender will be getting loss



* Security Services:-

Security services include

- ~~confidentiality~~ Authentication
- ~~Integrity~~ Authorization
- ~~Authentication~~ Non-repudation
- ~~Non-repudation~~ ~~Auditiey~~

which protect data and communications from unauthorized access, alteration & denial.

→ These services are implemented using various mechanisms to ensure secure data processing & transmission. & verify the source of information

1) Authentication:

* Getting an official permission to get into the website & get into server to access it.

* There are many ~~users~~ ways to check the authentication by checking whether the username & password which you are giving as an input is correct (or) not.

* If the data is matched then you will be authenticated to use the services.

2) Authorization:

* After you are allowed to ~~the~~ enter into the website, upto some extent you can use this services of the server.

* It is also called as access control

3) Non-repudiation:

* Once the message is transmitted from sender to reciever

* Digital signatures are a primary tool for achieving this service.

4) Audicity:

• It will analyse the data, it will have entire information about the data

• If any unauthorization permissions happens then the audicity will track the hacker.

---

* Security Mechanisms:

Security mechanism include

1) Encipherment(encryption)
2) Digital Signature
3) Access Control
4) Authentication exchange
5) Traffic padding
6) Routing control.

to protect data & ensure confidentiality, authenticity, integrity & non-repudiation

1) Encipherment: The process of transforming data into an unreadable format, which can only be reversed with the correct key to ensure confidentiality

- The sender will convert the data into an unreadable format means sender hides the data.
- When the reciever recieves the data which is unreadable that is converted into readable format

2) Digital Signature:-

* Some special identity which is used for authentication
- These use hash functions & public-key cryptography

3) Access control:

These mechanisms enfore access rights to resources who can view or modify data.

* Restricting the permissions to several levels.

4) Authentication exchange:

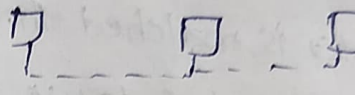
* Declaring the user as an authentcated user by comparing the username & password with the data the we are having in database

Eg: login Instagram.

5) Authentication exchange:-

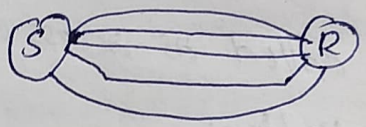
* Declaring the user as an authenticated user by

5) Traffic padding:- we to have to add extra bits in the beginning (or) in the middle (or) in the ending in order to confuse the observer (or) hacker



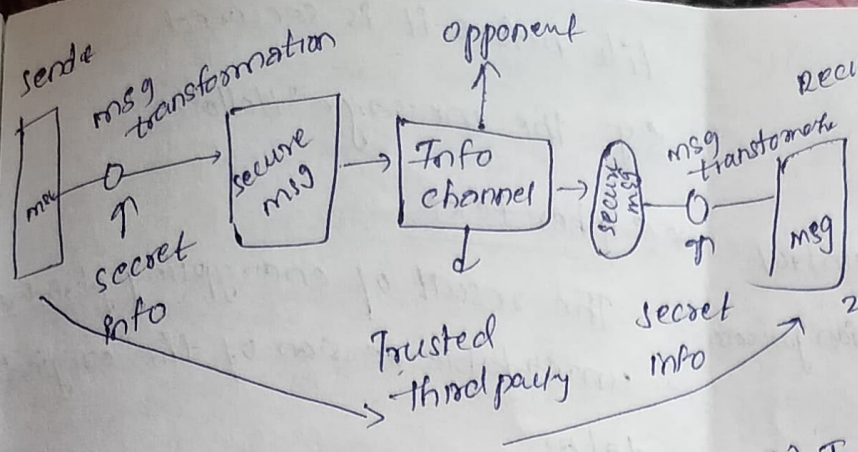
6) Routing control:

" we have 'n' number of paths we can go with any path.
- we can go with mixture of path in order to confuse the hacker



A Model for N/w Security:

=) It involves a layered approach designed to protect data confidentiality integrity & availability across an organization's n/w architecture.



Network Security model

* A trusted third party may be needed to achieve secure transmission
* This general model shows that there are four basic tasks in designing a particular security service:-

1) Design an algorithm for performing the security related transformation
2) Generate the secret information to be used with the algorithm.
3) Develop methods for the distribution & sharing of the secret info
4) Specify a protocol to be used by the two principals that makes use of security alg & secret info to achieve a particular security service.

components:-

1) sender - origin of the data
2) Reciever - Intendent recipient of the message
3) Transmission medium - The channel through which data travels
4) opponent (Attacker): unauthorized entity trying to access
5) Security services - confidentiality, Integrity.
6) Security mechanism - Encryption, hashing.

---

* Cryptography Concepts & Techniques:

⇒ cryptography is the practise of security information and communication through the use of codes, using mathematical algorithms to transform readable information into an unreadable format.

key concepts include:

Encryption

Decryption

and the use of keys to control the encryption and decryption process.

Techniques include:

Symmetric key - which uses one secret key

Asymmetric key - which uses a pair of public & private keys

Applications:

Cryptography is essential for securing data in many areas, including secure web browsing (HTTPS), online banking, email & protecting sensitive data.

---

* plain Text

- The original, readable msg or data.
- can be understood by humans without any special process
- Represents the actual content of a message, document or file before it is secured.

Eg: The message "Hello".

* Cipher-text:

The result of encrypting plaintext, unreadable version of the original data.

- can only be understood after being decrypted
- used for secure transmission and storage of data, making it unintelligible to unauthorized individuals.

Eg: msg "Hello" could become "jlnnq".

Substitution Techniques:

- Replace characters in a plaintext msg with other characters, numbers or symbols based on a key.

key Techniques include:-

1) caeser cipher
2) Monoalphabetic cipher
3) play fire cipher
4) hill cipher

1) Caesar cipher.

- It is one of the simplest & oldest encryption technique.

→ It is a substitution cipher where each letter in the plain text is shifted by a fixed number of positions down the alphabets.

Enc: $C = (p+k) \bmod 26$

Dec: $p = (C-k) \bmod 26$

Eg: HELLO key = 3

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

H ⇒ (7+3) mod 26
10 mod 26 = 10 ⇒ K

E ⇒ (4+3) mod 26
7 mod 26 = 7 ⇒ H

L ⇒ (11+3) mod 26
14 mod 26 = 14 ⇒ O

L ⇒ (11+3) mod 26
14 mod 26 = 14 ⇒ O

O ⇒ (14+3) mod 26
17 mod 26 = 17 ⇒ R

2) Monoalphabetic cipher

→ It is a type of substitution cipher in which each letter of plaintext is replaced with fixed letter.

PT: ATTACK CT: PWWDFN

Adv: easy to understand

Dis: weak security.

* playfire cipher:

→ • generate the key square (5×5) grid of alphabets that acts as the key for encrypting the plain text

• Each of the 25 alphabets must be unique and one letter of the alphabet is (ij) omitted from the table

• If the plaintext contains J, then it is replaced by I.

• The plaintext is split into pairs of two letters

• If there is an odd numbers of letters, 'Z' is added to the last letter

PT: instruments:

Aftersplit: 'in' 'st' 'ru' 'me' 'nt' 'sz'

- pair cannot be made with same letter, Break the letter in single & add a bogus letter to the previous letter

PT: hello 'he' 'lx' 'lo'.

↓ bogus letter

Rules

1) If the both the letters are in same rows then Row → Right.

2) If two alphabets are in same columns then immediately goto column → down.

3) If two alphabets are not in same row (or) column then draw a imaginary rectangle. then we have to take corresponding horizontal alphabet.

PT: instruments :- in st ru me nt sz

I	N	S	T	R
U	M	E	Z	A
B	C	D	F	G
H	K	L	O	P
Q	V	W	X	Y

hello
helxlo

M	S	T	R
m	E	Z	A
C	D	F	G
K	L	O	P
V	W	X	Y

key = monarchy

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

in =)

=) qa et zm cl rq tx

---

hill cipher:

$C = KP \bmod 26$

→ square matrix

→ Assign PT numbers to PT alphabets.

eg: key = VIEW

message = ATTACK

key matrix $\begin{bmatrix} V & E \\ I & W \end{bmatrix}_{2\times2} \Rightarrow \begin{bmatrix} 21 & 4 \\ 8 & 22 \end{bmatrix}$

plaintext : $\begin{bmatrix} A \\ T \end{bmatrix} \begin{bmatrix} T \\ A \end{bmatrix} \begin{bmatrix} C \\ K \end{bmatrix}$

$\Rightarrow \begin{bmatrix} 0 \\ 19 \end{bmatrix}, \begin{bmatrix} 19 \\ 0 \end{bmatrix}, \begin{bmatrix} 2 \\ 10 \end{bmatrix}$.

kp mod 26 = c.

① $\begin{bmatrix} A \\ T \end{bmatrix} = \begin{bmatrix} 21 & 4 \\ 8 & 22 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 21(0) + 4(19) \\ 8(0) + 22(19) \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 0 + 76 \\ 0 + 418 \end{bmatrix} = \begin{bmatrix} 76 \\ 418 \end{bmatrix} \bmod 26$

$= \begin{bmatrix} 24 \\ 2 \end{bmatrix} = \begin{bmatrix} Y \\ C \end{bmatrix}$

Transposition techniques:

→ Also called as rearrangement.

• Rearrange the plain text alphabet (or) digits with the same plain text.

Four techniques:-

1) Rail Fence Transposition
2) Columnar Transposition / row
3) Improved Transposition
4) Book cipher

① Rail fence:- In this the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

eg: welcome to my session

w l o e o y e s o
e e m t m s s i n

ct: wtoeoyesoeemtmssin

2) columnar transposition:

5×5

1	2	3	4	5
w	E	L	C	O
m	E	T	O	m
y	S	E	S	S
I	O	N	-	.
-				

key = 43512

C = COSLTENOMSwOmyIEESO

* Encryption and Decryption.

• Encryption is the process of converting data into secret code (cipher text) to prevent unauthorized access.

• Decryption is the process of converting that cipher text back into the original, readable form.

Symmetric key & Assymetric key

- Symmetric cryptography uses a single secret key for both encd decryption.
- It is faster and more efficient for large amount of data, but requires secure key distribution
- Less secure if the key is exposed
- It is best for encrypting large amount of data, such as file encryption, database protection

Eg: AES, DES, Blowfish

- Asymmetric key.

uses two keys: a public key (for anyone to encrypt) and a private key (for the owner to decrypt).

- Slower than symmetric
- more secure for key exchange & management since the private key is never shared
- No need to securely share a secret key. the public key can be shared openely.
- Best for Digital signatures, secure key exchange

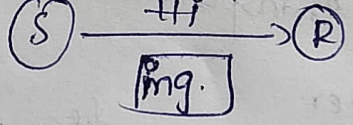
Eg: RSA, DSA, Diffie-Hellman

---

* Steganography

It is the art of concealing the existence of a message within other data.

→ It aims to hide the fact that communication is occuring, often by embedding a secret message in an image, audio or video files without changing the file's structure significantly



Different Types

1) Text steganography:- It is defined as a type which involves caching dispatches or secret information within a textbook document or other textual data.

2) Image steganography:- It involves caching dispatches or secret information within digital images. It is generally used for watermarking, brand protection etc.

3) Audio steganography:- within audio lines. It is generally used for digital rights operation in audio files.

4) video steganography:- within digital videotape lines. The ideal way to use video steganography is to detect secret information in a videotape in such a way that normal people won't notice it.

Adv
- It offers better security for data sharing & communication.
- It can apply through colorful means like images, audio etc.

* Key Range & Key Size:-

⇒ key range is the total number of all possible keys that a specific algorithm can generate.

⇒ key size is the number of bits in a cryptographic key, which determines how many possible keys exist

key size:

→ It is the length of a cryptographic key, measured in bits.

- A larger key size provides greater security.

eg: a 256-bit AES key is more secure than a 128 bit AES key.

key range

→ The total number of possible keys that can be used for a given algorithm.

- A larger key range increases the difficulty for attackers to guess the correct.
- key range is determined by the key size for a key of n bits, there are 2^n possible keys

Possible types of Attacks

1) passive
2) Active.

3) Network-Based Attacks

These specifically target n/w protocols and connections

a) Man-in-the middle

- Attacker intercepts & possibly modifies communication b/w two parties

b) IP Spoofing

- Attacker sends packets using a fake IP address.

4) Host-Based Attacks

These target individual computers or servers.

a) malware

- Virus, worm

b) Rootkits

- Hide malicious processes in a system.

5) Web-Based Attacks

Modern web vulnerabilities

a) SQL Injection

- Injecting SQL code into i/p fields

Brute-force Attacks :- public & private keys play a significant role in encrypting & decrypting the data in a cryptographic system

- Dictionary Attack :- A targeted form of a brute-force attack that uses a precompiled list of the most common passwords or keys.