29/09/2024

UNIT-1

→ CIA TRIAD:

* Computer security is defined and given by confidentiality, integrity and availability of system resources and protecting them from attackers.

* Confidentiality: protecting the data from attackers through encryption.
Ex: Account info

* Integrity: avoiding modification, data sent from the sender to receiver.
Ex: Patient's info

* Availability: Ensure timely and reliable access to the resources.
Ex: Authentication service.

→ Levels of impact of security breach.

(1) Low: limited/minor attack on the system.

(2) Medium: serious effect on the system (or) individual.

(3) High: very serious effect (or) loss of money (or) life threat.

→ Additional features of CIA triad:

- authenticity: genuine & verifiable / legal
- accountability: responsible towards the data & privacy.

→ OSI Security Architecture:

* Potential violation of ~~threat~~ security is known as threat.
* Potential vulnerability to enter into system (or house is known as attack.

→ Attack: an assault on ~~an~~ system security that derives from an intelligent threat; (or) a deliberate attempt to evade security ~~attacks~~ services & violate security policy.

→ Security attacks: action that compromises security
→ Security mechanism: detect, prevent or recover from attack.
→ Security service: enhances security, counter security attacks and provide the service.

* Security Attacks: (Hard (to detect)).
Action that compromises the security of an individual (or) an organization.

Types:

1) Passive Attacks (hard to detect): Attempts to learn (or) make use of info from the system.

→ Does not affect system resources
→ Monitoring of transmission.

* Types: *

1) Release of message contents.
2) Traffic analysis → analyses the patterns of messages.

reading the messages b/w 2 users; encryption helps to avoid this.

getting the info regarding frequency of data; format of data etc.

2) Active Attacks:

involve some modification of data stream or creation of a false stream.

* Types:

1) Masquerade: Stealing somebody's credentials for login
2) Replay: Capturing msgs & replaying causing confusion
3) Modification of messages:
4) Denial of Service (DoS): disrupting the service given by provider.

Ex: No. of TCP requests from single system by overloading

* Both the attacks are equally dangerous.

Passive	Active
→ Hard to detect	→ Hard to prevent
→ Neither sender nor receiver is aware of the attack	→ The sender (or) receiver will be aware of the attack.
→ Difficult to detect hence concentrate on prevention	→ difficult to prevent – physical, software & network vulnerabilities
→ Encryption prevents the attack.	→ Prevention is possible if detection has less effect.

* Security Services:

Service that is provided by a system to give a specific kind of protection to system resources; implement security policies and are implemented by security mechanisms.

→ Authentication:

Proving the identity of the user

- Peer-entity authentication: confirming from neighbours
- Data-origin authentication: confirming from the source.

→ Access Control:

- Controlling the levels of privileges given to any user.

→ Data confidentiality: hiding the data from threats.

→ Data integrity : sent = receive.

→ Non-repudiation: avoiding any conflict regarding deny of sending (or) receiving with the help of security

Ex: proving that msg is sent by sender and received by receiver.

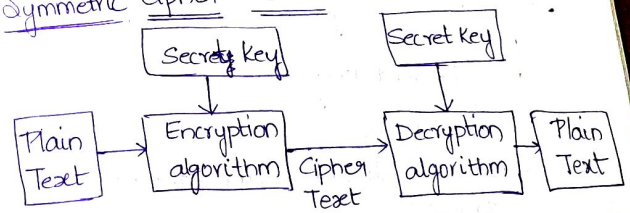
* Security Mechanisms: → Specific
→ pervasive.

→ Specific security mechanisms: implementing security services at various protocol level.

(1) Encipherment: cipher text generation. (key).
(2) Digital Signature: piece of code used to prove identity.
→ provides both authentication & integrity.
(3) Access control
(4) Data integrity
(5) Authentication Exchange: exchange code to prove identity
(6) Traffic padding: data sent while there is no comm. b/w 2 connected routers.
dummy traffic helps to avoid this by confusing the attacker.
(7) Routing control: If any path data is sent along the routers is attacked, we can physically secure the routers.
(8) Notarization: using a secured 3rd party to communicate b/w 2 users.

→ Pervasive security mechanisms (criteria)
(1) Trusted functionalities: security policies that help to decide the action perform.
(2) Security labels
(3) Event detection: detecting suspicious events.
(4) Security audit trail: checking the activities
(5) Security recovery: backing up the data / getting back system after attack.

* Symmetric Cipher Model:



→ Secret key decides the type of encryption algorithm and the respective O/P is generated based on the same secret key.

→ Cipher Text: encrypted plaintext.

Ex: $E(x) = (x+3) \bmod 26$ $D(x) = (x-3) \bmod 26$

tutorial (plain text) $\xrightarrow{E(x)}$ wxzwruldo (encrypted text) $\xrightarrow{D(x)}$ tutorial

∵ Sender and receiver use the same key; this encryption is called symmetric encryption.

→ Cryptography is the process of converting plain text into cipher text and cipher text into plain text.

- Symmetric Cryptography (or) Private Key Cryptography:
  - same key is used for both encryption & decryption. (known to sender & receiver)
- Assymmetric Cryptography (or) Public Key Cryptography:
  - different keys are used for encryption & decryption.
  - one key is public and other is private.

* Conditions for:

① Encryption:
- unconditionally secure – generates a unique cipher text.
- computationally secure – if the attacker takes lot of time & efforts to break the text

* Cryptanalysis:
- attacks done based on the info known to cryptanalyst.
- most difficult is when attackers knows only the cipher text (not even encryption algorithm).
  - Ciphertext only – encryption algo, ciphertext
  - Known Plaintext – " , 1/more PT-CT pairs
  - Chosen Plaintext – " , PT msg.
  - Chosen Ciphertext – " , CT msg.
  - Chosen Text – Choosen plaintext (or) ciphertext.

* Brute Force Attack:
- finding every possible keys.
- guessing
- exhaustive key search

Ex: Aircrack-ng, DaveGrohl, Hydra

* Classical Encryption Techniques: Substitution, Transposition
- Not really secured; not used in todays world

→ Substitution Technique:

Letters are replaced by other letters or symbols.

→ Transposition Technique:

Applying some sort of permutation on the plaintext letters.

Ex: Plaintext: NESO

Cipher text: ESON, SONE, ONES, ENOS ...

Transposition technique is ~~used~~ ~~not~~ efficient when the length of the plain text is longer

*→ Substitution Techniques

1. Caesar Cipher
2. Monoalphabetic Cipher
3. Playfair Cipher
4. Hill Cipher
5. Polyalphabetic Cipher
6. One-Time Pad

*→ Transposition Techniques:

1. Rail Fence
2. Row-Column Transposition.

* Caesar Cipher:

Replacing each letter of the alphabet with the letter standing 3 places further down the alphabet.

Algorithm:

for every plain text 'p'; substitute the Cipher text 'C': $C = E(p, K) \bmod 26 = (p+K) \bmod 26$

Decryption algorithm ⇒ $p = D(C, K) \bmod 26 = (C-K) \bmod 26$

Ex: neso ⇒ QHVR

QHVR ⇒ neso

*→ Shift Cipher: If key is other than 3 it is called shift Cipher.

key = 2, 3, 4, 5, ...

- Shift Cipher with key=3 is called Caesar Cipher

Ex: Neso K=4

RIWS

Pros:

1. Simple
2. Easy to implement

Cons:

1. Easy to decode.
2. 25 keys are only possible.
3. Easily recognizable using Brute force attack

* Monoalphabetic Cipher:

→ The cipher line can be any permutation of the 26 alphabetic characters.

Ex: Neso ⇒ ~~DEFD~~ ~~DE~~ DALM

→ randomly assigning any alphabet

→ to break this we need 26! ways.

→ according to the relative frequency of occurrence of english letters:
we try to decode the monoalphabetic cipher; where we calculate the % of any letter in the cipher text.

* according to above analysis
E → most occurring letter in english sentence.
T → 2nd most.

Ex: GZGEWVGRNCP
∵ most appearing is G
E_E___E____
→ using trial and error to get the decrypted word.

Pros:
① Better security than caesar cipher.
②

Cons:
① Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet.
② Prone to guessing attack using the english letter frequency of occurrence of letters

* Playfair cipher: also known as Wheatstone-Playfair cipher
→ manual symmetric encryption technique.
→ Multiple letter encryption cipher.
→ 5×5 matrix is constructed using a keyword (Ex: 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

** Rules for Encryption:
1) Repeating letters – filler letters
2) Same column |↓| wrap around.
3) same row |→| wrap around.
4) Rectangle |⇄| Swap.

Ex: ATTACK
RSSRDE

Ex: balloon
to avoid same letter in a pair
ba lx lo on
IB SU PM NA

* Hill Cipher:
→ Multi-letter cipher
→ Encrypts a group of letters: digraph, trigraph (or) polygraph.

Algorithm:

$C = E(K,P) = P \times K \bmod 26$ → Encryption.

Decryption:

$P = D(K,C) = CK^{-1} \bmod 26 = P \times K \times K^{-1} \bmod 26.$

Ex: "pay more money"

$$key = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$

pay more money

15 0 24 12 14 17 4 12 14 13 4 24

dividing the given sentence:

pay mor emo ney.

$$= \begin{bmatrix} 15 \\ 0 \\ 24 \end{bmatrix} \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} =$$

$$= \begin{bmatrix} 15 & 0 & 24 \end{bmatrix} \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \bmod 26.$$

$$= \begin{bmatrix} 303 & 303 & 531 \end{bmatrix} \bmod 26.$$

$$= \begin{bmatrix} 17 & 17 & 11 \end{bmatrix}$$

⇒ RRL

$$= \begin{bmatrix} 12 & 14 & 17 \end{bmatrix} \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix} \bmod 26$$

$$= \begin{bmatrix} MWB \end{bmatrix}$$

$$= \begin{bmatrix} 4 & 12 & 14 \end{bmatrix} \begin{bmatrix} key \end{bmatrix}$$

$$= KAS$$

$$= PDH$$

PRLMWBKASPDH.

→ Decryption:

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

$$Adj K = \text{repeating } 1^{st} \text{ 2 cols twice} \ \& \ \text{2 rows twice}$$

17	17	5	17	17
21	18	21	21	18
2	2	19	2	2
17	17	5	17	17
21	18	21	21	18

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

$$= \begin{bmatrix} 14 & -1 & 7 \\ -19 & 1 & -18 \\ 6 & 0 & -25 \end{bmatrix} = \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix}$$

$$\det K = 17(342-42) - 17(399-42) + 5(42-36) \bmod 26$$

$$= -939 \bmod 26.$$

$$= -3 \bmod 26$$

$$= 23$$

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

$$= 23^{-1} \quad u \quad \Rightarrow 17 \begin{bmatrix} 14 & 25 & 7 \\ 7 & 1 & 8 \\ 6 & 0 & 1 \end{bmatrix} \mod 26$$

$23^{-1} \mod 26 = 17$

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

RRL MWB KAS PDH

* Poly alphabetic Cipher:

Vernam Cipher:

→ Length of keyword = length of the plaintext.

→ works on binary bits rather than letters.

Expression:

$$C_i = P_i \text{ XOR } K_i$$

Where: C ⇒ Cipher text
P ⇒ Plain text
K ⇒ Keyword.

→ uses repeating keywords which makes it easy to decode.

* One Time Pad:

→ Improvement to Vernam Cipher
→ yields the ultimate security
→ Random key is as long as the msg.
→ No repeating keyword
→ the key generated is only used for a single msg.
→ unbreakable in nature
→ generates ≠ random o/p

** Drawbacks:

1) Increased no. of random keys.
2) Key distribution & protection
∵ this is symmetric in nature.

→ used primarily for low-bandwidth channels requiring very high security.

→ exhibits the perfect secrecy (ntg will be revealed about msg).

* Transposition Techniques:

** Rail - Fence technique:

→ simple
→ Plain text is written down as a sequence of diagonals & then read off as a sequence of rows.

Ex: "neso academy is the best"

Rail-fence = 2

n s a c a e m y i s t h e b e s t
e o c d

Ciphertext:

nsaaeysbbseocdmiteet

Ex: "Thank You"

depth = 3

t k
h n y u
a o

Cipher text = tkhnyu_ao

* Row-Column Transposition:

→ more complex
→ Rectangle: decision ~~done~~ taken by the sender and receiver.

→ Write: Row by Row
→ Read: Column by Column
→ Key: order of the column.

Ex: "Cryptography"

4	3	1	2
C	R	Y	P
T	O	G	R
A	P	H	Y
B	D	E	F
I	J	K	L

key = 4312

Cipher text: YGHEK PRYFL ROPDJCTABI

Y	G	H	E
K	P	R	Y
F	L	R	O
P	D	J	C
T	A	B	I

→ We can repeat this process any no. of times and this also acts as a key.
→ This generates a complex cipher text.

* CYBER THREATS:

A cyber threat is any malicious act that can negatively impact a computer system, network, (or) data, (or) people and processes that use it.

→ Phishing:

It is form of social engineering where attackers deceive individuals into revealing sensitive info by impersonating legitimate entities usually via email, text, (or) malware.

Phishing Techniques:

→ Spear Phishing: Targetted to particular individual (or) small group. The attacker will research their target & include personalized details that make the attack seem real.

→ Vishing (or) Voice phishing: attack performed over phone. Vishers attempt to talk their targets into handing over sensitive info.

→ Smishing: attack performed using SMS. These msgs include; links which say there is an issue with the target's account & upon clicking the link, the details are hacked by the attacker.

→ Clone Phishing: involves sending a user a phishing mail that is similar to the previous mail they have received and include a malicious link.

→ Spam: unwanted / irrelevant mails that are designed to steal money or sensitive data.

* Defensive Measures:

1. Email filtering & Spam detection
2. Two-factor authentication
3. User education & awareness.
4. Anti-phishing software.
5. Email authentication protocols.

→ Web-based attacks:
Software-based threats that exploit vulnerabilities in web applications.
They can be used to steal user credentials, financial data, spread malware.

Types of web-based attacks:

1. Cross-site scripting (XSS):
   Leads to session hijacking, phishing, info collection.

2. SQL injection:
   Injecting malicious commands into existing SQL.
   → Injecting a always true condition along with our input.

   Ex: select * from users where Id=105 OR 1=1;

* → Defensive Measures:

1. Input validation.
2. Parameterized Queries
3. Stored procedures.
4. Web Application Firewalls (WAF)
5. Error Handling.

* Buffer Overflow and Format String vulnerabilities:

→ Buffer overflow occurs when a program writes more data to a memory buffer than it can hold, leading to corruption of adjacent memory and potential code execution by an attacker.

→ Format String vulnerabilities occurs when the user input is unsafely passed to a fn like printf in C ; which interprets the I/P as a format string. This leads to info disclosure & corruption.

Defensive measures:

1. Bounds checking
2. Safe programming languages: Java/Python.
3. Stack canaries (markers): that detect buffer overflow before program crashes.

(1) Input Sanitization:

* TCP session hijacking:

Occurs when an attacker intercepts & manipulates an ongoing TCP session to gain unauthorized access to the session b/w 2 communicating systems.

Techniques:

1. ARP Spoofing: sending fake ARP messages to associate the attacker's mac address; further redirecting network traffic.
2. Route Table Modification: Manipulates the routing tables in a network to redirect packets to a malicious system.

Defensive measures:

1. Encryption: Transport layer security (TLS)
2. Intrusion Detection System (IDS); detects ARP spoofing (or) unusual routing.
3. Static ARP entries: manually configure ARP entries.
4. Session timeouts: short session time.

* UDP Hijacking (Man in the middle attacks)

∵ UDP is connectionless; it is more vulnerable to man-in-the-middle (MIM) attacks; where an attacker intercepts comm. b/w 2 parties; potentially modifying or injecting packets.

Techniques:

① UDP flooding: attackers flood a network with UDP packets; leading to target system crash.

② MIM attacks: attacker modifies the comm.

Defensive measures:

① Encryption: VPNs, TLS, DTLS.

② Firewall rules

③ UDP flood protection

④ DNS security extensions: