CNS Assignments

1. Define the three security goals ? and explain each one with suitable examples.

The three security goals often refferred as the CIA triad. The NIST standards FIPS 199 lists confidentiality, integrity and availability as the three ~~seq~~ security objectives for information & information systems.

a) Confidentiality :- It is preserving authorized restrictions on information access and disclosure including means for protecting personal privacy.

Ex:- When we log into the bank account, our password and personal details are encrypted. Only you and the bank can access this information. If a hacker intercepts it and reads it, confidentiality is broken.

b) Integrity :- It ensures that data remains accurate and unalted during storage, transmission and processing except by authorized person. A loss of integrity is the unauthorized modification or destruction of information.

Ex:- If A is giving a cheque to B and another person C alters the amount in the check then there is a threat to integrity.

c) Availability :- Ensuring timely and reliable access to use of info. It assures that system work promptly and service is not denied to authorized users.

Ex:- If a website becomes unavailable because attackers flood it with traffic, disrupting access for legitimate users.

2. Distinguish between active attacks & passive attacks. Name some active attacks & also some passive attacks.

An attack is a deliberate attempt by an individual or group to breach security policies (confidentiality, integrity and availability) of a system or network. These are broadly categorised into

1. Active attacks
2. Passive attacks

- Active attacks :- It involves some modification of the data stream or the creation of a false stream and can be subdivided into four categories:-

→ Replay :- It involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

→ Masquerade :- It takes place when one entity pretends to be a different entity. This attack usually includes one of the other forms of active attack.

→ Denial of Services:- Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is disruption of entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

→ Data Modification:- It may involve a middle-man-in-the-middle attack in which the attacker selectively modifies communicated data between a client and server.

- Passive attacks :- These are nature of eaves dropping on, or monitoring of transmissions. The goal of the attacker is to obtain information that is being transmitted. Two types of passive attacks are the release of message contents & traffic analysis.

→ Release of message:- A telephone conversation an electronic mail message and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

→ Traffic analysis :- In this the opponent could determine the location and identity of communicating hosts & could observe the frequency and length of messages being exchanged.

Active attack	Passive attack
→ Modification in info takes place.	→ Modification of info doesn't take place.
→ Active attack is a danger to integrity as well as availability of data	→ Passive attack is a danger to confidentiality of the data.
→ In active attack attention is on prevention.	→ In passive attack attention is on detection
→ Execution system is damaged due to this	→ There is no havoc to the system due to this
→ Victim is informed about this attack	→ victim doesn't get informed about the attack
→ The duration of this attack is short	→ The duration of passive attack is long.

3. Define the type of security attack in each of the following cases:

a) A student breaks into professor's office to obtain a copy of next day's test.

It is an 'interception' which is a type of passive attack which damages the confidentiality of the information.

b) A student gives a cheque for $10 to buy a used book. Later she found the cheque was cashed for $100.

→ It a 'modification' attack which is a active attack

It is an attack to integrity of the data.

c) A student sends hundreds of e-mails per day to another student using a phone return e-mail address

This is 'Denial of Services (DOS)' due to flooding emails affects the availability of information it is an active attack.

And 'Spoofing' - using a fake return address (false identity) It is also an active attack

4. What is 'masquerade'? Which principle of security is breached because of that

A masquerade attack is a type of cyber attack where an attacker impersonates a legitimate user on system to gain unauthorized access to resources on information. This breach primarily violates the principle of authentication and non-repudation.

5. Why is confidentiality an important principle of security? Think about ways of acheiving the same.

Confidentiality is a crucial security principle because it ensures sensitive information is only accessible to authorized individuals, preventing unauthorized disclosure & potential harm. It is important because it helps in protecting sensitive

information and maintains trust and compliance also prevents data breaches and frauds, ensures data integrity.

In order to achieve confidentiality:-

1. Encryption:-

A method of converting data into coded format (ciphertext) so that only authorized parties with a secret key can decode and access the original data.

2. Access control:-

Techniques used to regulate who can view or use resources in a computing environment

3. Data classification and labeling:-

Organizing data into categories to determine appropriate security measures based on its sensitivity.

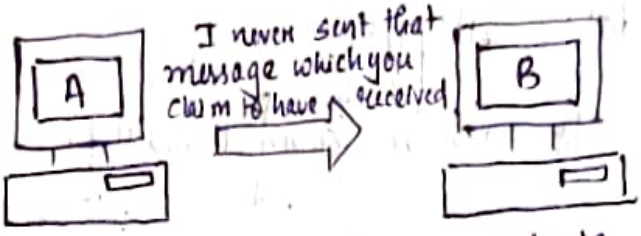
4. Proper Disposal of Data:-

The process of securely deleting or physically destroying data and storage devices to prevent data recovery or leaks

6. What is repudiation? How can it be prevented in real life?

There are situations where a user sends a message & later denies or refuses that she had sent the message. Non-repudiation doesn't allow the sender

of a message to refute the claim of not sending that message.



This principle of non-repudiation defeats such possibilities of denying something after having done it.

In real life it can be prevented using

→ Digital Signatures

- Provides proof that a particular person (via private key) signed or authorized a document or transaction. Ex:- in emails, contracts etc.

Ex:- A customer tries to deny they authorized large payment. But the system shows a time stamped digital signature, IP address, & OTP used - making repudation invalid.

7. Why are some attacks called passive? Why other attacks are called active?

⇒ Passive attacks are those wherein the attacker indulges in eavesdropping or monitoring of data transmission. In other words, the attacker aims to obtain information that is in transit. The term passive indicates that the attacker does not attempt to perform any modifications to the data. This is also why passive attacks are harder to detect. Thus, the

general approach to deal with passive attacks is to think about prevention, rather than detection or corrective actions.

Passive attacks do not involve any modification to the contents of an original message.

Passive attacks have more two sub-categories:-

→ Release of message contents

→ Traffic Analysis

Release of message means when the content of a message is seen by some else except the receiver against our wishes.

Attempts of analyzing (encoded) messages to come up with likely patterns are the work of the traffic-analysis attack.

Active attacks unlike passive attacks are based on the modification of original message in some manner or in the creation of a false message. These attacks cannot be prevented easily. However they can be detected with some effort, and attempts can be made to recover from them.

In active attacks the contents of the original message are modified in some way.

- Trying to pose an another entity involves masquerade attacks.
- Modification attacks can be classified further into replay attacks and alteration of message
- Fabrication causes Denial of services (DOS) attacks

8. Using the Euclidean algorithm, find the greatest common divisor of the following pairs of integers.

a. 88 and 220

u_1	u_2	q	r
220	88	2	44
88	44	2	0
44	0	-	-

$\gcd(220, 88) = r_1 = 44$

b. 300 and 42

u_1	u_2	q	r
300	42	7	6
42	6	7	0
6	0	-	-

$\gcd(300, 42) = 6$

c. 24 and 320

u_1	u_2	q	r
320	24	13	8
24	8	3	0
8	0	-	-

$\gcd(320, 24) = 8$

d) 700 and 401

u_1	u_2	q	r
700	401	1	299
401	299	1	102
299	102	2	95
102	95	1	7
95	7	13	4
7	4	1	3
4	3	1	1
3	1	3	0
1	0	-	-

9. Using the extended Euclidean algorithm, find the greatest common divisor of the following pairs and the value of s and t.

a) 4 and 7

u_1	u_2	r	s_1	s_2	s	t_1	t_2	t
1	7	4	3	1	0	1	0	1	-1
1	4	3	1	0	1	-1	1	-1	2
3	3	1	0	1	-1	4	-1	2	-7
-	1	0	-	-1	4	-	2	-7	-

$s = s_1 = -1 \quad t = t_1 = 2 \quad \gcd = (7, 4) = r_1 = 1$

$-1 \times 7 + 2 \times 4 = 8 - 7 = 1 = \gcd(7, 4)$

by 291 and 42

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
6	291	42	39	1	0	1	0	1	-6
1	42	39	3	0	1	-1	1	-6	7
13	39	3	0	1	-1	14	-6	7	-97
-	3	0	-	-1	14	-	7	-97	-

$s = s_1 = -1$ $t = t_1 = 7$

$\gcd(291, 42) = r_1 = 3$

$-1 \times 291 + 42 \times 7 = 294 - 291 = 3 = \gcd(291$

$s \times a + t \times b = \gcd(291, 42)$

c) 24 and 320

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
13	320	24	8	1	0	1	0	1	-13
3	24	8	0	0	1	-3	1	-13	40
-	8	0	-	1	-3	-	-13	40	-

$\gcd(24, 320) = r_1 = 8$

$s = s_1 = 1$ $t = t_1 = -13$

$s \times a + t \times b$

$320 \times 1 + (-13) \times 24 = 320 - 312 = 8 =$ gcd(

d) 400 & 60

q	r_1	r_2	r	s_1	s_2	s	t_1	t_2	t
6	400	60	40	1	0	1	0	1	-6
1	60	40	20	0	1	-1	1	-6	7
2	40	20	0	1	-1	3	-6	7	-20
-	20	0	-	-1	3	-	7	-20	-

$\gcd(400, 60) = r_1 = 20$

$s = s_1 = -1$ $t = t_1 = 7$

$s \times a + t \times b = 400 \times (-1) + 7 \times 60$

$= -400 + 420$

$= 20 = \gcd(400, 60)$

10. Perform the following operation using reduction first

a. $(273 + 147) \bmod 10$

i) $273 \bmod 10 = 3$

$147 \bmod 10 = 7$

ii) $3 + 7 = 10$

iii) $10 \bmod 10 = 0$

$(273 + 147) \bmod 10 = 0$

b. $(4223 + 17323) \bmod 10$

i) $4223 \bmod 10 = 3$

$17323 \bmod 10 = 3$

ii) $3 + 3 = 6$

iii) $6 \bmod 10 = 6$

$(4223 + 17323) \bmod 10 = 6$

c. $(148 + 14432) \bmod 12$

i) $148 \bmod 12 = 4$

$14432 \bmod 12 = 8$

ii) $4 + 8 = 12$

iii) $12 \bmod 12 = 0$ $(148 + 14432) \bmod 12 = 0$

d) $(2467 + 461) \bmod 12$

i) $2467 \bmod 12 = 7$

$461 \bmod 12 = 5$

ii) $7 + 5 = 12$ $(2467 + 461) \bmod 12 = 0$