CNS Assignment-I

21001-CS-069

1. Define computer network.

Computer network refers to interconnected computing devices that can exchange data and share resources with each other. These networked devices user a system of rules.

2. Define network security.

Network security consists of all steps taken to protect the integrity of a computer network and the data within it. It is important because it keeps sensitive data safe cyber attack.

3. Define computer security.

Computer security refers to measures and controls that ensure the confidentiality, integrity and availability of the information processed and stored by the computer.

4. List goals of network security.

- Confidentiality
- Integrity
- Availability

5. List services of network security.

- Confidentiality
- Integrity
- Authentication.
- Access control
- Non-repudation.

6. List types of attacks.

- Passive attack
- Active attack.

7. Define confidentiality.

Confidentiality means making sure that information is only available to those who are authorised to have access. Preserving authorised restrictions on access and disclosure, including means for protecting information.

8. Define authentication.

Authentication is used by a server when the server needs to know exatly who is accessing their information. Authentication verifies the identity of a user or service.

9. Define Integrity.

Upholding integrity means that measures are taken to ensure that data is kept accurate and up to date.

10. Define access control.

Access control is a security measure which is put in place to regulate the individuals that can view, use or have access to a restricted environment.

11. Define denial of service.

A dos attack is an attack meant to shut down a machine or network making it inaccessable to ~~ie~~ its inteded users

12. Define plain text.

The ~~it~~ data to be protected during transmission is called plain text.

13. Define cipher text.

The data that is in encrypted foam after transmission is called cipher text.

14. Define key.

Key allows connected devices to encrypt and decrypt the code making it difficult to write or read by other devices/ others.

15. Explain passive attack.

In this, an attacker observes the message, copy them and may use them for malicious purposes. It is an attack in which a system is monitored and sometimes scanned..

There are two types:

1) Monitoring message.

2) Traffic monitoring / analysis.

16. Explain active attack.

In this, the attacker attempts to change or tranform the content of message or information. These attacks are threat to integrity and availability.

1) Masquerade attack.

2) Replay attack.

3) Modification attack.

4) Denial of service.

17. Explain OSI security ~~ARC~~ architecture.

OSI defines a systematic way of defining and providing security requirements.

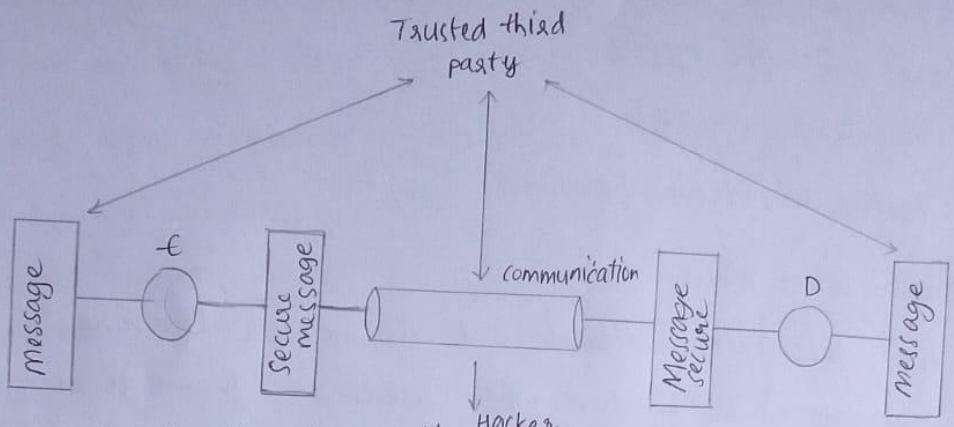
Security attack: Any activity that compromises the security of information.

Security mechanism: A mechanism that is designed to detect, prevent or recover from a security attack.

Security services: A service that enhances the ~~services~~ security of data processing systems and information transfers.

18. Explain model for network security.

This exhibits how the security service has been designed over the networks to prevent the opponent from causing threats.



19. Explain goals of network security.

1) Confidentiality: Protecting precious data from unauthorised people. The privacy or confidentiality of important information is the primary goal of network security.

2) Integrity: The second goal of network security. The data received by recipent must be exactly same as the data sent from the sender, without change in even single bit of data.

3) Availability: Making sure the data is continuously available to the authorised people.

21. Explain network security attacks.

These are two types of attacks;

1) Passive attack.

2) Active attack.

→ Passive attack: In passive attack, only monitoring of data is done. The attacker monitors data but doesn't modify it.

1) Release of message content

2) Traffic analysis.

Active attack: In Active attack, the hacker not only monitors the data but also modifies the data and uses it for malicious purposes.

1) Masquerade attack

2) Replay attack.

3) Modification attack.

4) Denial of service.

22. What is classic cryptography and modern cryptography.

Classic cryptography is a cryptography network provides secret communication. It is of these types:

1) Symmetric key encryption.

2) Assymmetric key encryption.

3) Public - key encryption.

Modern cryptography is security digital information, transactions and distributed computations.

1) Symmetric ~~en~~ encryption.

2) Assymmetric ~~encry~~ encryption.

3) Hashing.

23. Write a short notes on evolution of cryptography.

Cryptography improved coding techniques like vignese coding come into existence, in the 15th century with offered moving letters in the message with a number of variable places instead of moving them the same number of places and cryptography is the study of algorithms and protocols in a formal framework.

24. What is the need of cryptography?

The need of cryptography is providing privacy and security and their conversations and data confidential, in a network security to the people and secure their data.

25. Write short notes on types of networks.

1) LAN (Local area network)
2) PAN (Personal area network)
3) MAN (metropolitan area network)
4) WAN (Wide area Network).

* LAN is a computer network which connects devices in a small area like an office, allowing quick data sharing.
* PAN is a network that connects devices within one persons workspace.
* MAN covers a city-sized area, providing medium scale connectivity, often used by operations
* WAN connects offices, data centres cloud applications all together.