2100031921
E.Kowshik
sec-54

1. Security Goals:
Security goals represent the fundamental objectives that any secure system or network should strive to achieve. The three commonly recognized security goals are:

Confidentiality:
Confidentiality ensures that sensitive information remains hidden from unauthorized individuals or entities. It involves protecting data from being accessed, read, or understood by anyone who doesn't have the necessary permissions. Encryption and access control mechanisms are used to maintain confidentiality.

Integrity: Integrity focuses on the accuracy and reliability of data. It ensures that data remains unaltered and trustworthy throughout its lifecycle. Security measures, such as checksums, digital signatures, and access controls, are employed to prevent

3. Security Mechanisms to Provide Security Services:
Security mechanisms are the tools or techniques used to implement security services. Here are some examples:

Encryption: Encryption transforms data into an unreadable format, ensuring confidentiality. Only authorized parties with the appropriate decryption key can access the original data.

Firewalls: Firewalls are network security devices that filter incoming and outgoing traffic based on predefined rules. They help control access and protect against unauthorized access, contributing to both confidentiality and availability.

Digital Signatures: Digital signatures provide authentication and data integrity by attaching a unique digital identifier to a message or document. This helps achieve the goals of integrity and non-repudiation.

Access Control Lists ACLs:
ACLs specify who is allowed to access certain resources or perform specific actions. They enforce access control policies, supporting confidentiality and availability goals.

Intrusion Detection Systems (IDS): IDS monitor network traffic for signs of unauthorized or malicious activities. They help maintain the integrity and availability of systems by detecting and responding to potential threats.

Hash Functions: Hash functions generate fixed-size values (hashes) from input data. These hashes are used for data integrity verification, ensuring that the data hasn't been tampered with.

These mechanisms, among others, work together to implement security services and achieve the overarching security goals within a system or network.