Network Security

Chapter No.	30
Status	Completed

- Network security is any activity designed to protect the usability and integrity of your network and data
  - Includes both hardware and software technologies and measures
  - Effective network security manages access to the network, targets a variety of threats and stops them from entering or spreading on a network

- Threats to Computer Systems
  - Malware
    - Malware is any software intentionally designed to cause damage to a computer, server, client or computer network
    - A virus is the most common type of malware that can execute itself and spread by infecting other programs or files
    - A worm can self-replicate without a host program and typically spreads without any human interaction or directives from the malware authors
    - Malware can enter a computer system in one of three ways
      - As a download from a web page
      - As an email attachment
      - As a file on infected removable media
    - Examples of Damage Caused By Malware
      - Loss of files or data
      - Unauthorised access to files or data
      - Reduction in system performance
      - Unauthorised access to webcams or microphones

        - Loss of control to attacker

- ▼ Denial of Service (DoS) Attacks
    - A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning
    - DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to users
    - A DoS attack is characterised by using a single computer to launch the attack.

▼ Restricting Access to Networks

- ▼ Firewalls
    - A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules
    - A firewall functions as a gatekeeper between a network and the wider internet through filtering incoming traffic, thereby preventing threats from accessing the network
    - ▼ Limitations of Firewalls
        - Firewalls cannot protect against what has been authorized
        - Firewalls cannot stop social engineering attacks or an authorised user intentionally using their access for unwanted purposes
        - Firewalls cannot fix poor administrative practices or poorly designed security policies
        - Firewalls cannot stop attacks if the traffic does not pass through them
        - Firewalls are only as effective as the rules they are configured to enforce.
- ▼ Intrusion Detection System (IDS)

- An intrusion detection system (IDS) is a device or software application that monitors a network for malicious activity or policy violations
- Any malicious activity or violation is typically reported or collected centrally using a security information and event management system
- An IDS acts as a secondary network security measure in the event that other network security measures fail to stop a threat from gaining access to a system

▼ Limitations of IDS

- An IDS cannot block or prevent attacks as they can only help to uncover them

▼ An IDS requires a capable network administrator in order for it to be configured properly

- An IDS has to be configured to reduce the number of false alerts while still maintaining adequate network security

▼ Intrusion Prevention System (IPS)

- An intrusion prevention system (IPS) is an automated network security device used to monitor and respond to potential threats
- Like an intrusion detection system (IDS), an IPS determines possible threats by examining network traffic
- Because an exploit may be carried out very quickly after an attacker gains access, an IPS administer an automated response to a threat, based on rules established by the network administrator
- The main functions of an IPS are to identify suspicious activity, log relevant information, attempt to block the activity, and finally to report it

▼ Limitations of IPS

▼ An IDS requires a capable network administrator in order for it to be configured properly

- An IDS has to be configured to reduce the number of false alerts while still maintaining adequate network security

- ▼ Ensuring Security of Network Applications
    - ▼ Encryption
        - Encryption is a way of scrambling data so that only authorized parties can understand the information
        - Encryption involves converting human-readable plaintext to incomprehensible text, known as ciphertext
        - Encryption takes readable data and alters it so that it appears random
        - ▼ Encryption requires the use of a cryptographic key
            - A cryptographic key is a set of mathematical values that both the sender and the recipient of an encrypted message agree on
        - Although encrypted data appears random, encryption proceeds in a logical, predictable way, allowing a party that receives the encrypted data and possesses the right key to decrypt the data, turning it back into plaintext
        - ▼ Encryption helps prevent data breaches, whether the data is in transit or at rest
            - If a corporate device is lost or stolen and its hard drive is properly encrypted, the data on that device will still be secure
            - Encrypted communications enable communicating parties to exchange sensitive data without leaking the data
    - ▼ Digital Signature
        - A digital signature is a technique which is used to validate the authenticity and integrity of the message
        - A valid digital signature, where the prerequisites are satisfied, gives a recipient very strong reason to believe that the message was created by a known sender, and that the message was not altered in transit
        - ▼ A digital signature can allow a network application to determine whether an incoming data packet should be accepted

    - If the incoming data packet has a valid digital signature, the data packet will be accepted by the network application

▼ Authentication

- Authentication is the process of verifying the identity of a user or process
- Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource

▼ Three Main Types of MFA

    - Things you know (knowledge), such as a password or PIN
    - Things you have (possession), such as a badge or smartphone
    - Things you are (inherence), such as a biometric like fingerprints or voice recognition

- Authentication is important because it enables organizations to keep their networks secure by permitting only authenticated users or processes to access its protected resources