جامعة المستقبل
كلية التقنيات الصحية والطبية
قسم تقنيات البصريات

Principles of computers

First stage

Lecture

NETWORK SECURITY

By

Asst. lecturer Mohammed Qasim Obayes

mohammed.qasim.obayes@uomus.edu.iq

2024-2025

WHAT IS NETWORK SECURITY?

- Every company or organization that handles a large amount of data, has a degree of solutions against many cyber threats.This is a broad, all-encompassing phrase that covers software and hardware solutions, as well as procedures, guidelines, and setups for network usage, accessibility, and general threat protection.

- The most basic example of Network Security is password protection which the user of the network chooses. In recent times, Network Security has become the central topic of cyber security with many organizations inviting applications from people who have skills in this area. The network security solutions protect various vulnerabilities of the computer systems such as users, location, data, devices, and applications

- Any action intended to safeguard the integrity and usefulness of your data and network is known as network security. In other words, Network security is defined as the activity created to protect the integrity of your network and data.

- Network security is the practice of protecting a computer network from unauthorized access, misuse, or attacks. It involves using tools, technologies, and policies to ensure that data traveling over the network is safe and secure, keeping sensitive information away from hackers and other threats.

HOW DOES NETWORK SECURITY WORK?

■ Network security uses several layers of protection, both at the edge of the network

and within it.

Each layer has rules and controls that determine who can access network resources. People who are allowed access can

use the network safely, but those who try to harm it with attacks or other threats are stopped from doing .

■ The basic principle of network security is protecting huge stored data and networks in layers that ensure the bedding of rules and regulations that have to be acknowledged before performing any activity on the data.These levels are:

• Physical Network Security: This is the most basic level that includes protecting the data and network through unauthorized personnel from acquiring control over the confidentiality of the network.The same can be achieved by using devices like biometric systems.

• Technical Network Security: It primarily focuses on protecting the data stored in the network or data involved in transitions through the network.This type serves two purposes. One is protected from unauthorized users, and the other is protected from malicious activities.

• Administrative Network Security: This level of network security protects user behavior like how the permission has been granted and how the authorization process takes place.This also ensures the level of sophistication the network might need for protecting it through all the attacks.This level also suggests necessary amendments that have to be done to the infrastructure.

TYPES OF NETWORK SECURITY

■ There are several types of network security through which we can make our network more secure,Your network and data are shielded from breaches, invasions, and other dangers by network security. Here below are some important types of network security:

■ Email Security, Network Segmentation,Access Control, Sandboxing, Cloud Network Security,Web Security, Intrusion Prevention System(IPS), Antivirus and Anti-malware Software, Firewalls Security, Application Security,Wireless Security,Web Security, Mobile Device Security, Industrial Network Security,VPN Security

BENEFITS OF NETWORK SECURITY

■ Network Security has several benefits, some of which are mentioned below:

• Network Security helps in protecting clients' information and data which ensures reliable access and helps in protecting the data from cyber threats.

• Network Security protects the organization from heavy losses that may have

occurred from data loss or any security incident.

• It overall protects the reputation of the organization as it protects the data and confidential items

ADVANTAGES OF NETWORK SECURITY

- Protection from Unauthorized Access: Network security measures such as firewalls and authentication systems prevent unauthorized users from accessing sensitive information or disrupting network operations.
- Data Confidentiality: Encryption technologies ensure that data transmitted over the network remains confidential and cannot be intercepted by unauthorized parties.
- Prevention of Malware and Viruses: Network security solutions like antivirus software and intrusion detection systems (IDS) detect and block malware, viruses, and other malicious threats before they can infect systems.
- Secure Remote Access:Virtual private networks (VPNs) and other secure remote access methods enable employees to work remotely without compromising the security of the organization's network and data.

DISADVANTAGES OF NETWORK SECURITY

- Complexity and Management Overhead: Implementing and managing network security measures such as firewalls, encryption, and intrusion detection systems (IDS) can be complex and require specialized knowledge and resources.
- Cost: Effective network security often requires investment in hardware, software, and skilled personnel, which can be expensive for organizations, especially smaller ones.
- Privacy Concerns: Some network security measures, such as deep packet inspection and monitoring, may raise privacy concerns among users and stakeholders, requiring careful balancing of security needs with individual privacy rights.