COMPUTER NETWORK SECURITY

Marijan **MIJATOVIĆ** [1], Marko **MIJATOVIĆ**[2]

[1] *Nezavisni Univerzitet Banja Luka*, [2]*Sveučilište Hercegovina*

photo.by.mile@gmail.com, marko.mijatovic@hercegovina.edu.ba

Keywords: networks, protocols, packets, LAN, cryptography.

Abstract*:* *Computers that we connect to a network serve to exchange data, which is located in the computer's working memory. Data transmission can also be done through electronic signals, and these connections can be wireless networks or wired networks. The bits that are sent one after another simultaneously correspond at an appropriate speed, converting digital signals into analog signals and vice versa, which is a modern process. Computers can also be connected to a local network and a branched network. Each computer connected to the network has its own unique number (address) from which it can be recognized on which continent it is, in which country, and to which server address it is connected. Data is sent according to a pre-agreed protocol, in the form of packets. Security measures for protecting sensitive data and documents have existed for a long time in the world. Throughout history, many methods have been developed regarding data protection and internet security. Methods of providing protection on the internet were sometimes not effective and did not provide the necessary level of protection. With the development of cryptography and technology, very good methods of encryption and document protection have been discovered. Information systems are the foundation of basic and modern business operations. Their fundamental task is to be based on network systems, as well as their operation and security. That's why it's extremely important to familiarize ourselves with the security issues of computer networks and the ways in which these problems are resolved.*

1. INTRODUCTION

Computer networks were initially designed to connect computers situated in locations enabling them to exchange and share data simultaneously essentially allowing communication. In the past the majority of data transmitted through these networks was, in form. However with the advancements in multimedia and network technologies today multimedia content has become a part of the internets evolution.

Various products like internet telephony, internet television, video conferences and others have emerged on the market as a result. In scenarios people will increasingly rely on services such as distance learning and distributed simulations that won't necessitate team members being physically present within the building or even country. The economic advantages of arrangements are quite evident.

To facilitate better quality communication for business purposes network services need to develop hardware and software infrastructure along with tools that support the transmission of multimedia services within computer networks.

The utilization of computers as communication tools will contribute significantly to enhancing network services. There is a belief that in course multimedia networks will replace phones, televisions and other inventions that have played pivotal roles in reshaping our lives in the past.

Fast forward sixty years later; information systems have permeated every aspect of activity. In todays world existence, without computer networks and their associated security measures is simply unimaginable.

2. HISTORY OF COMPUTER NETWORKS

Computer networks emerged as a result of applications developed for large corporate companies. Companies recognized the efficiency problem of their employees who had to transfer the written material to disk units in order to print it. They had to copy certain types of data to a computer with a connected printer before being able to print a specific document.

To simplify and, above all, reduce costs in business operations, companies began to invest in network technology and their security for better and more secure business practices. In the early 1980s, computer networks experienced tremendous growth, although the early networks were quite insecure.

Due to the rapid expansion of computer networks and their security, there was a period of incompatibility among network systems funded by different companies. The solution to this problem was the LAN (Local Area Network). Perhaps the most important moment was in 1983 when the network, using NCP-A (Network Control Protocol), transitioned to TCP/IP (Transmission Control Protocol / Internet Protocol), a newer technology that is widely used in the world today.

Packet-Switched technology describes the sending of specific data in small packaged units called packets. They are routed through the network using the targeted IP address contained in the packet. The packet traveling this way will reach its destination, and it is crucial that all other packets also reach their destinations.

Sharing data for packet transmission allows the same communication network to be shared among a larger number of users in the network. Each computer connected to the network also has its own unique number (address) from which it can be identified in which part of the world, in which country, and through which server it is connected. Data in the network is sent according to agreed-upon protocols and in the form of packets.

3. NETWORKS AND THEIR DIVISION

The division and types of services that an information network should provide are as follows:

- In speech and communication, in digital form, through channel or packet procedures, text communication, data communication through real-time or delayed procedures, access to banking and computer data services, and their processing.
- Image communication, videophone, telefax, multimedia communication, and remote control.

In addition to the physical format for network connections, computer networks can also be distinguished by size:

- Local Area Network (LAN): Simple networks where two computers are connected via cable.
- Home Area Network (HAN): These are computers within a single household that connect personal electronic devices such as mobile phones, laptops, and HDTVs.
- Wide Area Network (WAN): These are computers spread worldwide and connected through telephone lines, satellite links, and radio links.
- Metropolitan Area Network (MAN): Data network in larger cities that connects large companies.

4. TYPES OF NETWORK MEDIA

Media used for transmission, also known as physical media, are used to connect computer devices in a network and consist of:

- Electrical cables (ETHERNET, Home PNA, network communication).
- Optical cables (fiber-optic communication).
- Radio waves (wireless communication).

In the OSI model, they are defined in layers 1 and 2, the physical layer and the data link layer.

The widely adopted family of transmission media used in LAN technology is known as the ETHERNET cable. Data transmission is carried out over copper and optical cables.

Standard wireless LAN networks also use radio waves and other frequencies as means of transmission. Communication through electrical lines utilizes a network cable for data transmission.

5. DEVICES AND NETWORK NODES

In addition to any physical media transmission that exists, networks comprise additional and fundamental system blocks, such as Network Interface Controller (NIC), repeaters, HUBs, bridges, switches, routers, modems, and other protective barriers (FIREWALL)."

5.1. Network User Interface

Network Interface Control is a computer hardware component that enables a computer to access and transmit data, and has the capability to process network information at a lower level. NIC can have a connector for accepting a cable or an antenna for wireless data transmission. NIC responds to traffic directed to either the NIC itself or to the computer alone.

In Internet networks, each controller has its unique MAC (Media Access Control) address, which is 6 octets long (e.g., 00-0a-83-B1-c0-b8) and is typically stored in the controller's permanent memory. To avoid address conflicts between network devices, the Institute of Electrical and Electronics Engineers (IEEE) maintains and administers the uniqueness of MAC addresses.

5.2. Repeaters and Hubs

A repeater is a network device that receives a network signal, cleans it from unnecessary noise, and regenerates (amplifies) it. The signal is then retransmitted at a higher power level or on the other side of an obstacle, allowing it to cover greater distances without degradation.

In Internet configurations, repeaters are necessary for cables longer than 100 meters, while with optical fibers, they can be located tens, or even hundreds of kilometers apart. Repeaters with multiple ports are more commonly known as hubs, and they operate at the physical layer of the OSI model.

5.3. Bridge

A network bridge connects and filters traffic between two network segments at the data link layer of the OSI model to form a single network. This breaks up the network domain while maintaining the broadcast domain. Network segmentation divides a large congested network into smaller, more efficient networks, and there are three basic types:

- Local bridges: connect LANs.
- Remote bridges: can be used to create a WAN between LANs. Remote bridges, where the connection is slower than the end networks, have mostly been replaced by routers.
- Wireless bridges: can be used to connect LANs or link remote devices to LANs.

5.4. Switch

A network switch is a device that manages the flow of data between parts of a local area network (LAN). Unlike a hub, a switch divides network traffic and sends it to specific locations, while a hub sends data to all devices on the network. They are used for medium-sized networks because they are more efficient and effective than hubs. A switch provides a computer with the full network speed, while other computers connected to a hub only receive a portion of the connection.

5.5. Routers

A router, or network router, is a device used to interconnect computer networks. It has the function of determining the exact path each data packet should take and forwarding that same packet to the next device in the sequence. In local networks, a router is usually set up as the link between the network and the internet, i.e., it is assumed to be the network exit point (GATEWAY).

5.6. Wireless Access Point (WAP)

A WAP is a network hardware device that allows a device compatible with a WiFi network to connect to a wired network. A WAP is usually connected to a router (via a wired network) as a standalone device, but it can also be an integral part of the router itself. A WAP differs from a hotspot, which is a physical location where WiFi access to a wide area network (WAN) is available.

5.7. Modem

Modems (modulators-demodulators) are used to connect network nodes using wires originally not designed for digital network traffic or for wireless connections. Modems are commonly used for telephone lines, utilizing digital subscriber line technology. They modulate the digital signal into a form suitable for transmission over communication channels, and subsequently demodulate it back to its original form after transmission.

5.8. Firewall

A firewall is a network device used for security control and access rules in a network. They are typically configured to reject access from unknown sources while allowing actions from known ones. They play a vital role in network security with the constant rise of cyber attacks.

6. PROTECTION AND SECURITY OF COMPUTER NETWORKS

There has always been a need to protect sensitive data, and consequently, documents containing such information. Throughout history, many methods have been developed in attempts to preserve the confidentiality of important data. Many of these methods were simple and did not provide sufficient protection, often resulting in breaches of confidentiality. With the development of cryptography and technology, very effective encryption methods and document protection techniques have been discovered.

Encryption is a good way to prevent unauthorized individuals from accessing the content of a sensitive document. However, once a document is decrypted with a secret key, a malicious authorized person can save, copy, print, or forward the document. Restricting access to a document to a select few individuals is one approach to document protection, but there is always a possibility that one of the trusted individuals may disclose the information.

In such a case, it is necessary to identify the person who leaked the information, which is not always a straightforward task. A solution that ensures the protection of sensitive information cannot rely on a single technology.

6.1. Antivirus Protection

Antivirus programs constitute a specific category of software designed primarily for the identification, neutralization, and elimination of viruses, worms, trojans, and other malicious programs. The fundamental task of an antivirus program is to recognize a virus and protect the system from its effects. If a computer is infected with a virus, the antivirus program must isolate and remove it. Antivirus definitions are used to identify viruses. Each virus is characterized by a specific sequence of octets (character codes), as it is fundamentally a computer program. After detecting a viral sequence in a file, the antivirus program will:

- Attempt to repair the file by removing the virus itself,
- Place the file in quarantine so that no program can access it, preventing the virus from spreading further,
- Delete the infected file.

Since viruses are constantly evolving, the database of virus definitions and their codes needs to be constantly updated, often multiple times a day. This is typically done by the antivirus programs themselves. If the definitions were not updated, the antivirus program would not be able to recognize new viruses.

The failure to update virus definitions is the main reason for the continued spread of some long-known viruses. To outsmart virus detection mechanisms, virus developers often create so-called oligomorphic, polymorphic, or metamorphic viruses. These viruses change their form and source code, aiming to go unnoticed in each subsequent "incarnation."

Another way antivirus programs operate is by monitoring the behavior of all programs. If a program attempts to write data into the executable code of another program, access the network, or try to send data to a specific port, the antivirus program will signal and notify the user.

6.2. Encryption

An important part of protecting documents stored on computer hard drives, especially laptops, is encryption. Through this relatively simple process, it is possible to prevent the exposure of confidential information in the event of a lost laptop, as well as attacks by malicious users who gain physical access to the computer. Most modern operating systems have built-in mechanisms that allow for the encryption of stored data.

The encryption process involves transforming open or clear text into text that is unintelligible to unauthorized individuals. The individuals for whom the document is intended and who are allowed to read it must possess a special key to convert the document back into clear text, or decrypt it. There are symmetric and asymmetric cryptographic systems.

In a symmetric cryptographic system, the key for encrypting or transforming the document into unintelligible text is the same as the key for decrypting it, while in an asymmetric cryptographic system, this is not the case. In communication through messages, there is usually a sender and a recipient of the message.

Asymmetric cryptographic systems are based on certain properties of numbers explored in number theory. The idea is explained by the following example. Ana creates her own pair of keys: one for encryption and one for decryption. Assuming that asymmetric encryption is a form of computer encryption, Ana's encryption key is one number, and the decryption key is another number. Ana keeps her decryption key secret, which is why it is usually referred to as the private key. However, she publicly publishes her encryption key, making it available to everyone.

An example of the most commonly used asymmetric cryptographic system is RSA, authored by Ron Rivest, Adi Shamir, and Len Adleman. Other examples of such algorithms include ElGamal, NTRUEncrypt, LUC, and others. The security of encrypted documents depends on which algorithm is used for encryption and the length of cryptographic keys. Attackers may conduct cryptanalysis on the text they want to decrypt.

6.3. The IPSec protocol

(IP Security) is a set of extensions to the IPv4 protocol that ensures basic security aspects of network communication, including confidentiality, integrity, authentication, and non-repudiation. It's worth noting that IPSec, in addition to extending the currently used IPv4, also comes as an integral part of the IPv6 protocol. As it integrates with the IP protocol, IPSec implements secure network communication at the third, or network layer, of the ISO OSI model of this protocol, i.e., the internet layer when considering the TCP/IP stack. Of course, security can also be implemented in other layers, from the physical to the application layer (such as SSH, SSL/TLS). Each implementation has its own advantages and disadvantages.

REFERENCES

[1] B. Djordjevic, D. Pleskonjic, N. Macek, *Operating Systems: UNIX and Linux, Higher*.

[2] M. Cagalj, *Security in Wireless Computer Networks*, Faculty of Electrical Engineering, Mechanical Engineering and Naval Architecture, Split, 2006.

[3] A. Darko; *Basic Network Terminology*, Electrical Engineering School, Belgrade, 2004.

[4] B. Eugene; *Introduction to Data Communications*, 1999.

[5] S. Ilisevic, *Quick Guide to Home Networks*, BUG & SysPrint, Zagreb, 2003.

[6] S. Jusic, *Security of Web Applications*. Communication Technologies and Standards in Computer Science, 2003.

[7] M. Bojovic, *Squid Proxy Server*, diploma thesis, Higher Electrical Engineering School, Belgrade, 2005.

[8] M. Zivkovic, *Algorithms*, Faculty of Mathematics, Belgrade, 2000.

[9] K. Milan and C. Dario, *Introduction to Computer Networks*, Zagreb, 2014.

[10] V. Muzic, *Methodology of Pedagogical Research*, Svjetlost, Sarajevo, 1982.

[11] B. Olivier *Computer Networking: Principles, Protocols, and Practice*, 2011.

[12] T. Pralas, *Computer Networks - Passive and Active Equipment*, Sys portal, Zagreb, 2004.

[13] M. Randic, *Network and Service Management*, Faculty of Electrical Engineering and Computing, Zagreb, 2004.

[14] V. Sinkovic, *Information Networks*, School Book, Zagreb, 1994.

[15] Srdic, Ida, Hrpka, Branko, K; Goran, *Textbook of Computer Science*, ALFA d.d., Zagreb, 2007.

[16] S. Skundric, A. Sok, *Analysis of Computer Network* at the Technical Faculty in Rijeka, Technical Faculty, Rijeka, 2007.

[17] P. Toni; *Computer Networks* - OSI Reference Model, 2008.

[18] V. Vasiljevic, P. Gavrilovic, B. Krneta, M. Krstanovic, N. Macek, B. Bogojevic, *Manual for Computer Network Administration*, Higher Electrical Engineering School, Belgrade, 2004.