EXCELLENCIA
INTERNATIONAL MULTI-DISCIPLINARY JOURNAL OF EDUCATION
Volume 02, Issue 05, 2024 ISSN (E): 2994-9521

Threats to Computer Networks and Methods of Protection against Them

Do‘schanov Bekzod Davronbek o‘g‘li [1], Shamuratov Ulug‘bek Alisher uli [2], Ismonaliyev Sanjarbek Qambaraliyevich [3]

[1, 2, 3] Tashkent University of Information Technologies named after Muhammad al-Khwarizmi

Abstract:

Today, while every aspect of our lives is developing at a rapid pace, modern technologies, electronic devices, and computer networks are becoming an integral part of our daily lives. This article examines the threats to computer networks and how to properly protect against them.

Keywords: Computer networks, processor, Windows, API, information, Firewall, attack, virus, security, password, FTP, DoS, DDoS.

Currently, a new stage of development associated with fundamental changes in the field of telecommunications is being implemented around the world. Issues of innovative development have always been an urgent task for the field of telecommunications, which requires deep knowledge. At the same time, innovative development of the field, considering the achievements of developed countries, and training of specialists are important. Implementation of innovative development in the telecommunications sector requires a systematic approach, that is, the provision of legal, technological, organizational, and qualified personnel. In modern conditions, a complex approach aimed at solving the issues of innovative development in the telecommunications sector requires knowledgeable and experienced specialists. The transition to innovative development of the industry forces new approaches to the training of specialists. For the innovative development of the telecommunications network, it is necessary to train many specialists in network technologies, network solutions, and network integrators.

A network is a set of computers, terminals and other devices interconnected by communication channels that provide information exchange. Such networks that provide data exchange between computers are called computer networks. It became possible to transmit information over long distances through the network. The network provides opportunities to transfer information, to

organize the joint operation of computers that are used separately, to solve one problem with the help of several computers. In addition, it is possible to specialize each computer to perform a certain task and to use the resources of computers (data, memory) together, and to connect to the Internet network, which unites the computers of the whole world.

A network always connects several computers, and each of them has the ability to transmit and receive information. Information transmission and reception is carried out alternately between computers. Therefore, information exchange is managed in any network. This, in turn, prevents or eliminates the collision and corruption of information between computers. After the establishment of computer networks, the addresses of all computers in it are determined. Because the transfer of information from one computer to another through the network is carried out through computer addresses. The sender and receiver addresses are indicated on the information being sent and transmitted to the network, just like the process of sending a letter in our ordinary life. Each computer compares the address of the recipient in the incoming information with its own address, if the addresses match, then it receives the information and sends a confirmation of receipt to the sender. Information is exchanged between computers in the same way.

A threat is an event, impact, or process that may harm someone's interests. An event or process that has the potential to negatively affect computer networks or elements of the network system is considered a threat to the interests of the subjects of network relations.

Today, wired and wireless computer networks are essential for everyday activities. Individuals and organizations depend on their computers and networks for business. Unauthorized network access can lead to data theft and performance disruption. Network attacks can be devastating and cause loss of time and money due to damage or theft of critical data or assets.

Vulnerability is the degree to which a network or device is susceptible to threats. Some level of vulnerability is inherent in routers, switches, computers, servers, and even security devices. There are three main weaknesses:

1. Technological weaknesses.
2. Configuration.
3. Security Policy.

All three of these sources of vulnerability can leave a network or device open to a variety of attacks, including malicious code attacks and network attacks.

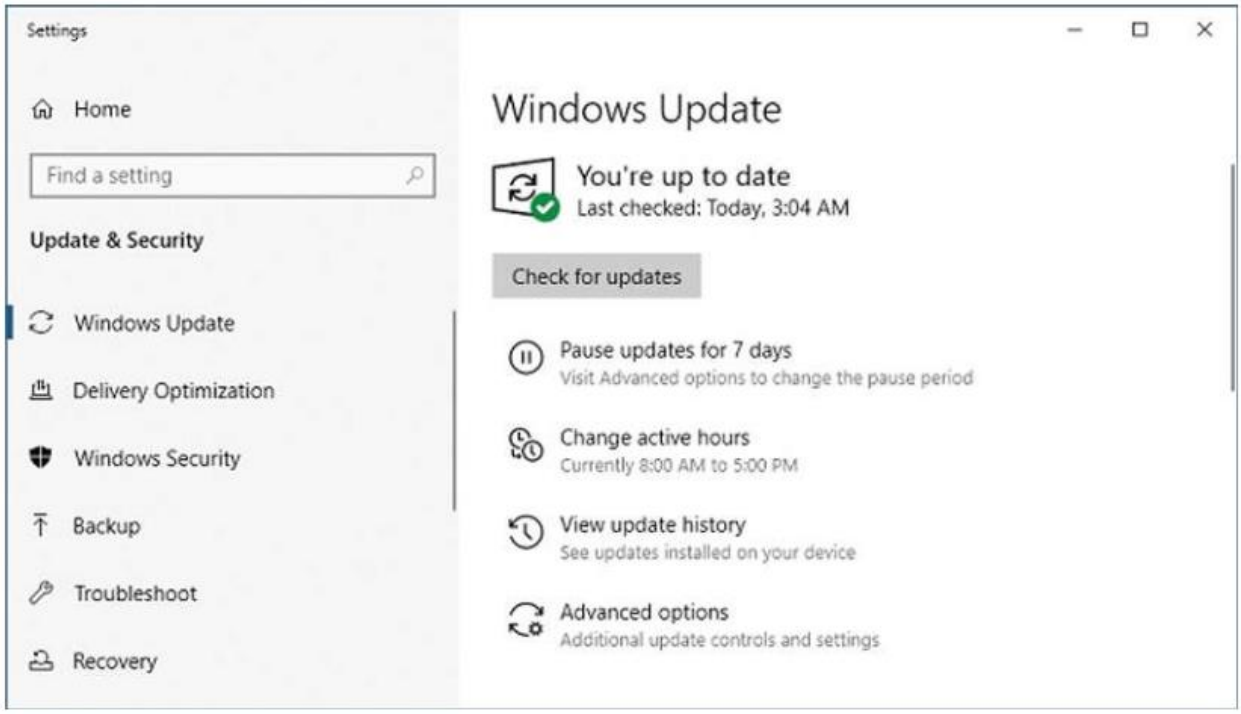
Attacks on computer networks can be different. Today, network protection is very important in the activities of any organization. Computer networks are still a valuable resource that is important for the organization's activity and competitiveness. There are many threats to the security of information systems and information resources of organizations: computer viruses that can destroy important data and industrial espionage of competitors; authentication access attacks; DoS and DDoS attacks; SQL attacks; their own trade secrets obtaining illegal access to information; and other similar threats. Therefore, protecting the network and ensuring information security are urgent problems.

Access attacks use known vulnerabilities in authentication services, FTP services, and web services to gain access to web accounts, confidential databases, and other sensitive information. An access attack allows individuals to gain unauthorized access to information they do not have access to. Access attacks can be divided into four types: password attacks, trust exploits, port forwarding, and man-in-the-middle attacks.

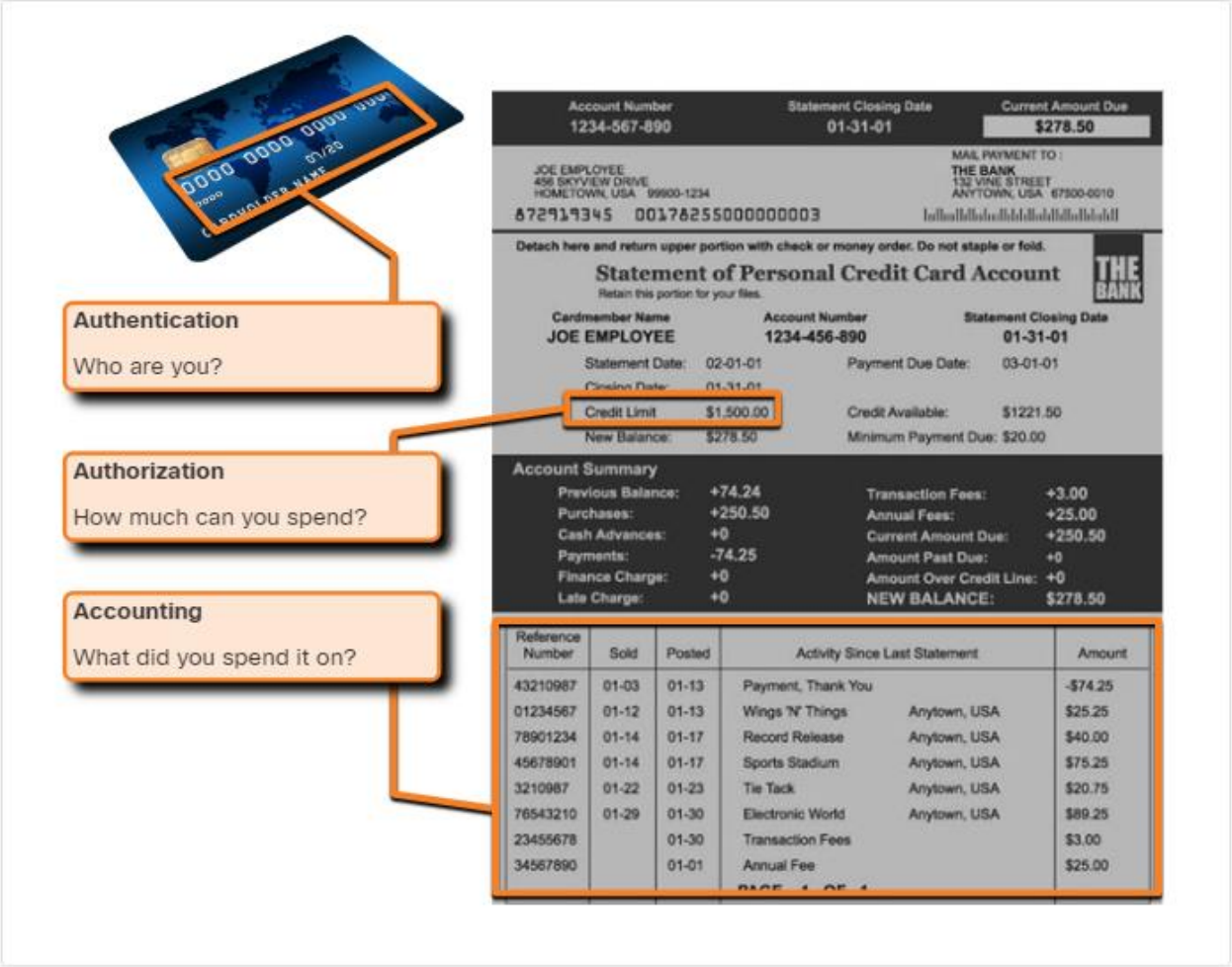
Computer viruses are malicious programs that cause some sort of damage to a computer system, usually without permission.

To mitigate network attacks, you must first secure devices such as routers, switches, servers, and hosts. Most organizations use a defense-in-depth approach to security (also known as a layered approach). Backing up your device configuration and data is one of the most effective ways to protect against data loss. Data backup saves a copy of the data on your computer to a removable backup medium that can be stored in a secure location. Infrastructure devices should have backup copies of their configuration files and IOS images on an FTP or similar file server. Backups should be performed regularly, as defined in the security policy. Data backups are typically stored off-site to protect the backup environment in case something happens to the primary facility.

The most effective way to mitigate a virus attack is for the operating system to download security updates and patch all vulnerable systems. Managing large numbers of systems involves creating a standard software image (operating system and accredited applications authorized for use on client systems) that are installed on new or upgraded systems.



All network devices must be configured securely to ensure access to authorized persons only. Authentication, Authorization, and Accounting (AAA or "triple A") network security services provide the basic framework for establishing access control on network devices.



A firewall is one of the most effective security tools available to protect users from external threats. A firewall protects computers and networks by preventing traffic from entering internal networks.

A firewall sits between two or more networks, controls the traffic between them, and helps prevent unauthorized access.

It is important to use strong passwords to protect network devices. Here are the standard guidelines to follow:

- Use a password that is at least eight characters long, preferably 10 or more characters. A longer password is a more secure password.
- Make passwords more complex. If allowed, include a mix of upper and lower case letters, numbers, symbols, and spaces.
- Based on repetition, common vocabulary words, sequences of letters or numbers, usernames, relative or pet names, biographical information such as date of birth, ID numbers, and other easily identifiable information not using passwords.
- Deliberately typing the wrong password. For example, Smith = Smyth = 5mYth or Security = 5ecur1ty.
- Passwords should be changed frequently. If the password is unknowingly compromised, the attacker has limited access to the password.
- Do not write passwords on paper, and do not leave them in open places such as desks or monitors.

Conclusion

Computer network attacks and how to protect them are important in computer engineering, cyber security, and network administration. In order to prevent threats to network security or to eliminate threats that have arisen, the existence of a regulatory legal base and the availability of knowledge and skills of specialists in the field of network security are of great importance.

References

1. Велихов А.В. и др. Компьютерные сети. Учебное пособие по администрированию локальных и объеденeнных сетей. 3-е изд. доп. и исп. - М.: Нов. Изд. дом. 2005 г.304 с.
2. Бройдо В.Л. "Вычислительные системы, сети и телекоммуникации" - СПб.:Питер. 2003.
3. Solidjonov, R. (2012). Problems and Contradictions of Sociocultural Transformations of the Tajik Society. *Dushanbe: Knowledge*.
4. Farkhod, M. (2020). Econometric Modelling of the Innovation Process in Uzbekistan. *International Journal of Psychosocial Rehabilitation*, *24*(02).
5. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Учебник. - СПб. Питер. 2016 г.