International Journal of Computer Trends and Technology
ISSN: 2231–2803 / https://doi.org/10.14445/22312803/IJCTT-V71I5P113

Volume 71 Issue 5, 80-84, May 2023
© 2023 Seventh Sense Research Group®

Original Article

Computer Network Security and Technology

Narangerel. TS[1], Dolgorsuren. T[2]

University of the Humanities, Mongolia

Received: 30 March 2023 Revised: 05 May 2023 Accepted: 19 May 2023 Published: 30 May 2023

Abstract *- The development of Information technology has granted users the opportunity to work in a network and the Internet. Due to this, risks regarding the safety of computer networks have arisen. These issues generally concern system security and information security. It is a matter of reliability, privacy, integrity, and access to information in the network environment. This research addresses network security technology such as authentication, encryption, firewall technology, intrusion detection system (IDS), antivirus technology and virtual private network (VPN). Issues regarding network security should assess such network issues, prevent various attacks, and ensure network security.*

Keywords *- Internet, Risk, Hacker, Key, External, Attacks, Virus, Protocols, Password, Protected.*

1. Introduction

As the use of computers continues to grow lately, computer network security has become one of the most critical issues. Computer network security plays an important business, economic and financial role for individuals and organizations. Internet-based e-business applications have simplified organizational processes, reduced operational costs, and increased customer satisfaction in recent years. Such applications can be used to transmit audio, video, and embedded information, and as the number of users increases, so do the network resources. As more network applications are developed and attract more users, this poses a risk to network security. Therefore, security technologies must play a central role in today's networks to combat threats and use electronic services without risk.

When the network is running, a large amount of data and information is stored on the external memory of the host or terminal, so how we prevent unauthorized users from accessing it is important to solve network security problems. [1].

Network security must be 100 percent secure since, due to loss of system security, data loss may result in direct and indirect economic losses. The risk of hacker attacks on the network poses a great threat to network security, and it also causes great economic and social damage.

1.1. Requirement

Network security problems are growing rapidly every year, reminding us of the need to take the necessary measures to protect the network and ensure the security of the network environment. As time goes by, new technologies continue to evolve and improve communication efficiency. At the same time, technological advancements have increased network security even more, thus requiring more experience to operate a network in a business environment.

1.2. Goals

Today, network administrators and other data center professionals need to understand security in order to organize and manage networks securely. One of the main goals of computer and network security is to prevent all possible risks, and it is important to develop security protocols and introduce them to your employees, and urge the organization to introduce and use additional services to protect its information resources. Organizations can prevent the latest threats and risks if they use new advanced technologies in their operations and regularly update them.

1.3. Importance of Network Security

Network security is particularly important to organizations operating in the Internet environment, e-commerce services, online learning and all network environments.

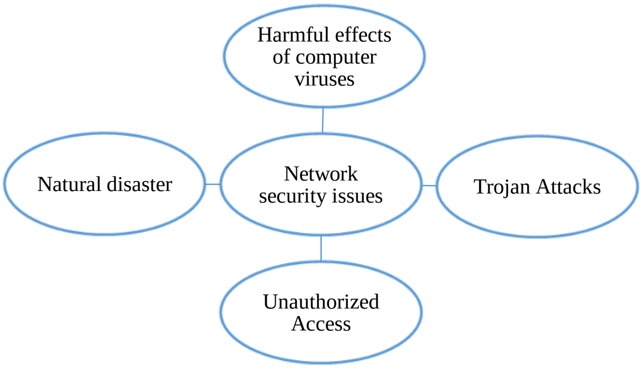

Fig. 1 Computer network security issues

2. Current State of Research

This topic of research is particularly interesting for security practitioners and researchers. Computer network security problems can arise from just one computer and spread to other systems and hosts in the network, affecting the system's normal operation and causing considerable damage.[2]. Risk issues continue to grow due to the lack of security control mechanisms, network security policies and protections. The main problems facing computer network security are defined in the following four basic conditions.

2.1. Harmful Effects of Computer Viruses

A virus is a small program capable of changing the normal operation of a computer. In other words, a virus aims to perform certain functions by entering the computer without the user's knowledge and consent.

2.2. Natural Disaster

Various natural phenomena, electromagnetic radiation, network equipment durability and other natural factors.

2.3. Trojan Horse Attack

A Trojan horse is a fake program designed to imitate widespread programs. It starts to work when the user tries downloading and installing the program from an untrusted site or a third-party website that is not the official website.

2.4. Unauthorized Access

Unauthorized access is when someone gains access to an account or website, application, server, service or other system by using unauthorized access to a network**.**

It is important to analyze the threats and protection protocols of computer network information security and present them as a basis for the development of common procedures for security and protection and to deliver useful and necessary information about it to users in a timely manner.

3. Computer Network Security Analysis

Computer network hardware security is defined by the level of privacy and protection required by the network environment to store data across the network for devices used in the network environment.

In order to build a reliable network security architecture, these 3 factors must be taken into consideration:

1. Natural disasters (earthquake, fire, flood), equipment damage (hard disk damage, equipment expiration period, external influences)
2. Electromagnetic field and radioactivity
3. Operational errors (hard disk formatting, data deletion), random operations.

Computer network software security is not only changing people's daily lives, living environment and learning environment but also affecting people's thinking. (Bec, 2004).

A network security system refers to a network operating system designed to ensure the reliability of network hardware and software. The network operating system regulates the security of the user's Internet network environment, and the organization must assign resources to detect potential errors and violations in accordance with its security regulations. User verification also plays an important par.[2]. Table No.1. Shows computer network threats, their effects, and the factors affecting them.

Table 1. Factors affecting network security

№	Name	Definition	How this issue could affect you
1	Unauthorized access	The act of gaining unauthorized access to computer systems	Access to or theft of information or serious actions that result in restricting or terminating online services.
2	Computer virus	A piece of code that can replicate itself can have harmful effects, such as damaging the system or destroying data.	It could affect the normal functionality of the computer and may lead to the loss of important files.
3	Computer worms	A standalone malware program that replicates itself to spread to other computers	Often harms the host's network by using wide area networks and overloading web servers.
4	Trojan horse	A program designed to breach the security of a computer system.	One of the most common methods is to gain access to a computer or perform nefarious activities such as sending personal information to other computers.
5	Denial of Service Attacks	Attempts to gain unauthorized access to network resources.	A denial of service is the temporary loss of access to a particular network, such as e-mail, or the temporary loss of all network connectivity.
6	Information and program changes	Hacking computers and modifying programs and data.	When you log on to your computer, your data and software could be unorganized and messy.

4. Computer Network Security Requirements

It becomes simpler to implement appropriate security policies and safeguards once the sources of potential threats and the types of potential damage are identified. Organizations have a wide range of options, from antivirus software packages to network firewalls, intrusion detection systems, and network security hardware. Methodological issues in computer network security have their own characteristics, each of which has advantages and disadvantages.

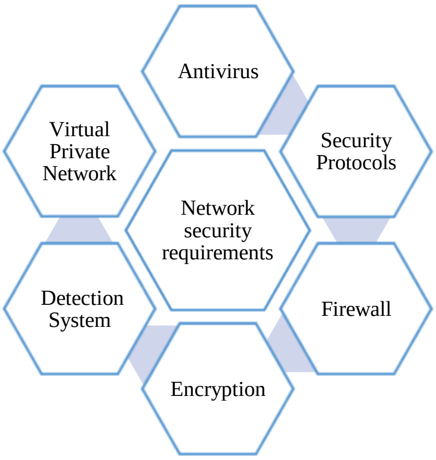

Fig. 2 Computer network security requirements

4.1. *Antivirus*

Antivirus software is installed on most computers and can handle most virus threats if the software is regularly updated and properly maintained. Antivirus software authors rely on large networks to develop and distribute updates containing information about new viruses. As thousands of new viruses are created every month, it is important to keep a virus database up to date. A virus database is a record stored in an antivirus package that helps detect and identify known viruses. Reputable anti-virus software companies will publish changes with the latest virus information on their websites, and the software allows users to download and use new changes.[3]. A network security policy should ensure that all computers on the network are up-to-date and, ideally, protected by an anti-virus package. Also, the software itself needs regular updates.[4].

4.2. *Security Protocols*

When setting up a network, whether it is a Local Area Network (LAN), Virtual LAN (VLAN), or Wide Area Network (WAN), it is important first to establish basic security policies. Security policies are rules that are electronically programmed and used in security equipment to control areas such as access rights.[5]. Policies in place should control who has access to which parts of the network and prevent unauthorized users from accessing restricted data. The individuals responsible for the security of the network and its security must have access to all areas of the network. After defining and configuring security policies, authentication methods and technologies must be used to authenticate users and their access rights. The simplest and most common method is to check whether a certain part of the network is "password protected" and only people with a specific password can access it. The golden rule for passwords is as follows.

- Change passwords regularly
- Make passwords as obscure as possible
- Never share your password with anyone until you leave the company.

Firewall - A firewall is a hardware or software solution implemented within a network infrastructure to enforce an organization's security policies by restricting access to specific network resources. A firewall creates a layer of protection between the network and the outside world. As a result, the firewall replicates the network at the access point so authorized data can be received without significant delay. It has filters that can block unauthorized or potentially dangerous material from entering the actual system. It records intrusion attempts and reports them to network experts.[6].

4.3. *Encryption*

Encryption technology ensures that messages cannot be received or read by anyone other than the authorized recipient. Encryption is often used to protect data transmitted over social networks.

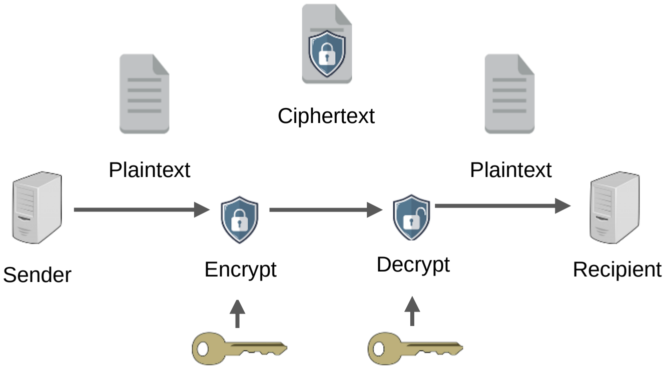

Fig. 3 Encryption

4.4. *Intrusion Detection System (IDS)*

A network-based intrusion detection system is always monitoring the network. IDS allows users to analyze packet traffic on a network, detect unauthorized activity, such as hacker attacks, and respond to security breaches before systems are compromised. When an unauthorized activity is detected, the IDS will send its details to the management and inform other systems and network devices to stop the unauthorized activity. As a physical analog, IDS is the equivalent of a video camera and motion detector and detects unauthorized or suspicious activity and stops the activity by working with an automated response system such as a watchdog.

4.5. *Virtual Private Network*

A VPN is a technology that uses the Internet to create a private, confidential network between hosts regardless of geographic location and allows information to be transmitted securely without being exposed to any external intrusions. The VPN uses automatic encryption for all applications and IP or Ethernet to increase security. The VPN system has powerful features and is very flexible and effective.

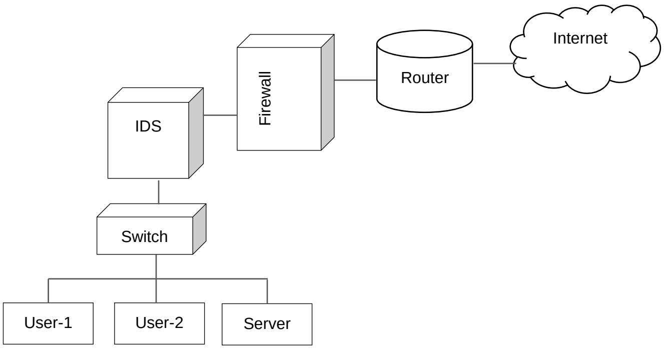

Fig. 4 Intrusion detection system

5. Conclusion

Network security is an important area that is gaining more and more attention as the Internet expands. Advances in technology have made network security more demanding, and more knowledge and experience are needed in this area. Current developments in network security are not very reliable and cannot guarantee data security. Therefore, it is appropriate to use a combination of various dependency methods to create a network security protection system.This research paper examines the problems of network threats and risks and mentions some forms of protection required to protect against them. Network security issues are becoming a part of the daily activities of every organization and user, and following the rules, regulations and standards related to security will significantly reduce hidden threats. In the future, the network security landscape may change even more quickly to cope with threats.

References

[1] A. Hess, and G. Schafter, “Realizing a Flexible Access Control Mechanism for Active Nodes Based on Active Networking Technology,” *IEEE International*, vol. 1, pp. 68-72, 2004. [CrossRef] [Google Scholar] [Publisher Link]

[2] Cristina L. Abad, and Rafael I. Bonilla, “An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks,” *27Th International Conference on Distributed Computing Systems Workshops*, pp. 60, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[3] S. Yongjie, “Research on Communication Encryption Technology of Network Security,” *Telecom Power Technology*, 2014. [Google Scholar]

[4] B. Endicott, “Active Defense to Cyber Attacks,” *Information Assurance and Security*, 2014.

[5] L.D. Peng, “Network Security and Firewall Technology,” *Proceedings of 2010 3rd International Conference on Computer and Electrical Engineering (ICCEE 2010)*, no. 2, 2012.

[6] A. Mayer, A. Wool, and E. Ziskind, “Fang: A Firewall Analysis Engine,” *IEEE Symposium on Security and Privacy*, pp. 177-187, 2000. [CrossRef] [Google Scholar] [Publisher Link]

[7] T.B. Bec, “Remote Control Euphoria,*” Americas Edition: Telecommunications (Americas Edition),* vol. 38, no. 10, pp. 10-11, 2004

[8] James P. Anderson, “Computer Security Threat Monitoring and Surveillance,” *Technical Report, James P. Anderson Company*, 1980. [Google Scholar] [Publisher Link]

[9] W. Xiaolin, “Study on Computer Network Antivirus Mechanism based on Antivirus Software,” *Network Security Technology & Application*, 2014. [Google Scholar]

[10] Narangerel Ts, "E-Commerce Security Issues," *International Journal of Computer Trends and Technology*, vol. 70, no. 4, pp. 25-28, 2022. [CrossRef] [Publisher Link]

[11] J.W.Yang, “A Brief Analysis of Computer Network Security Precautions in the Era of Big Data,” *Science and Technology Communication*, no. 2, pp. 108-109, 2019.

[12] Z.H. Long, “Computer Network Information Security and Protection Strategy in the ERA of Big Data,” *Management Informationization in China*, no.3, pp.161-162, 2019. [Google Scholar]

[13] Q.F. Deng, “Computer Network Information Security Technology and its Development Trend,” *Electronic Technology and Software Engineering*, no. 24, pp. 194-195, 2019. [Google Scholar]

[14] W. Liu, “Research on Optimizing Network Security Strategy Based on Big Data,” *Software*, vol. 39, no. 9, pp. 205-208, 2018.

[15] L. Zhao, “Research on Computer Network Security Protection Strategy under the Background of Big Data,” *Journal of Heihe University*, vol. 10, no. 1, pp. 217-218, 2019.

[16] Q.Wang, and C.Pan, “Analysis of Network Complete Vulnerabilities and Preventive Measures in the Era of Big Data,” *Network Security Technology and Application*, no. 2, pp. 77-79, 2017.

[17] L.J. Bao, “Application of Big Data-based Network Security Situation Awareness Platform in Private Network Field,” *Information Security Research*, vol. 5, no. 2, pp. 168-175, 2019.

[18] B. Wang, “Network Security Fuzzy Risk Assessment Based on Computer Network Technology,” *Foreign Electronic Measurement Technology*, vol. 38, no. 5, pp. 11-16, 2019.

[19] Q. Liu et al., “Research on the Framework and Methods of Network Security Detection,” *Computer Engineering and Science*, vol. 39, no. 12, pp. 2224-2229, 2017.

[20] Biswajit Tripathy, and Jibitesh Mishra, “Protective Measures in e-commerce to deal with Security Threats Arising out of Social Issues – a Framework,” *International Journal of Computer Engineering and Technology (IJCET),* vol. 4, no. 1, pp. 46-53, 2013. [Google Scholar] [Publisher Link]

[21] Pooman Patel, and Kamaljeet I. Lakhtaria “A Study on e-Commerce security Threats” *IJIRSCE*, vol. 5, no. 3, 2017.

[22] W. Xiang, “Research on Hierarchical Structure and Linkage of Network and Information Security Emergency Response System,” *Network Security Technology and Application*, pp. 177-179, 2015.

[23] L. Hailong, “Discussion on Network Security Emergency Response Mechanism in Colleges and Universities,” *Industry and Technology Forum*, vol. 19, no. 15, pp. 277-278, 2020.

[24] H. Daoli, and Y. Hao, “Legal Protection of Network Security Emergency Response of China's key Information Infrastructure,” *China Information Security*, pp. 42-43, 2020.

[25] D. Yuanyuan, “Research on Network Security Incident Emergency Response Linkage System,” *Wireless Internet Technology*, pp. 47-48, 2017.

[26] L. Feng, “Network Security Situation Awareness and Emergency Response Platform Solution,” *Information Technology and Standardization*, pp. 16-18, 2018.