Journal of Electronics and Information Science (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/jeis.2023.080204
ISSN 2371-9524 Vol. 8 Num. 2

Analysis of Computer Network Security and Prevention Technology

Shuai Yang[1,a,*], Xianfang Wang[2,b]

[1]University of Perpetual Help System DALTA, Las Pi ñas Campus, Alabang–Zapote Rd, Las Pi ñas, 1740, Metro Manila, Philippines
[2]Fushun County, Zigong, Sichuan, 643212, China
[a]444288640@qq.com, [b]1025472846@qq.com
**Corresponding author*

Keywords: Computer network security, Firewall, Preventive measures, Group filtering, agent

Abstract: This paper mainly studies computer network security and firewall technology, discussing the functions, main technologies, configurations, security measures, and firewall design ideas of network firewall security technology. With the popularization of computer networks, network security issues are receiving increasing attention from people. We can propose corresponding measures to address the shortcomings and vulnerabilities in current network security and firewall settings, in order to expect our network to be more secure. In terms of ensuring network security and data security, there are data encryption technology, smart card technology, firewall technology, etc. We mainly study firewall technology here. Firewalls can be divided into various types based on their different methods, precautions, and priorities. Afterwards, two basic implementation technologies, firewall packet filtering and application proxy, were introduced. Firewall technology is still in the development stage, and there are still many problems that need to be solved.

1. Introduction

With the widespread use and development of the Internet, especially the widespread application of Internet technology, the application of computers has become more extensive and in-depth. At the same time, we must note that although the network is powerful, it still has vulnerabilities[1]. In China, hackers and computer virus also cause huge economic losses every year.

2. Research objective

In recent years, firewall technology has emerged to address personal network security issues in the Internet era. Firewalls are very practical and highly corresponding. It provides a complete network security solution for individual network users. Can effectively control the sending and receiving of personal computer user information on the Internet. Users can set some parameters as needed to control the information exchange between the local computer and the Internet, and prevent malicious information from attacking the local computer.

3. The Concept of Computer Network Security

The security of computer systems, the reliability of computer hardware, software, and computer data, as well as the causes of malicious damage, have all been changed, and subsequently derived technologies to protect and protect the security and definition of development and management. Therefore, computer network security theories that use different technologies and management methods allow networks, their sources, data integrity, and security to be preserved. Therefore, establish network security measures to prevent data transmitted and exchanged through the network from being added, modified, damaged, or leaked.

4. Current Situation of Computer Network Security

Computer security, hardware, software, and data protection network systems, losses, losses, reliability of continuous systems, or harmful consequences such as failure stops and network service stops. The complexity and diversity of computer and network technology are areas that require continuous updates and improvements in computer and network security. At present, hackers have invaded more computer virus than any other, and many attacks are fatal. Due to the fact that the internet itself is not limited by time, space, or territory, every time a new attack method appears, it will spread throughout the world within a week. These attacks. Utilize vulnerabilities in networks and systems to attack and paralyze computer systems and networks. Worms, backdoors, rootkits, DOS (denial of service), and Sniffer (network monitoring) [2] are familiar with several hacker attacks. However, these attack methods all reflect their astonishing power. Today, they are becoming increasingly powerful. Compared with traditional attack methods, these new varieties of attack methods are more intelligent, and the attack targets directly refer to the basic protocols and operating system level of the Internet. From web program control programs to kernel level rootlets. Hacker attack methods are constantly upgrading and updating, constantly challenging user information security and prevention capabilities.

5. Threat factors to network security

Overall, the threats to network security mainly include software vulnerabilities, deployment errors, insufficient security awareness, viruses, hackers, etc.

Software defects: All OS or network software cannot appear without defects and defects. This means that computers will face danger and once connected to the network, they will become targets of criticism.

Configuration error: If an error in the security configuration leads to a security vulnerability, such as incorrect software configuration in a firewall, then it is useless. For specific network applications, a series of security vulnerabilities can be opened at startup, making many program related applications effective. Unless the user locks or configures the program correctly, there is always a security threat.

Weak security awareness: Users choose their passwords carelessly, while others transfer them to their own accounts or exchange them with others, posing a threat to network security.

Virus: The biggest enemy of current data security is computer virus, which is a set of computer commands or program code that can be self-replicated and disrupt the normal operation of computer software and hardware when inserted into computer programs by production personnel [3]. Computer virus has the characteristics of infectivity, parasitism, concealment, flammability and destructiveness. Therefore, improving virus prevention is currently the most important issue.

Hackers: Another aspect of computer security threats comes from hackers. Hackers can exploit the weaknesses of this system to invade someone else's computer system, which is very dangerous.

In a sense, hackers pose a greater threat to information security than ordinary computer viruses.

6. Firewall technology

Fire Wall is a security system between internal and external networks. It protects the internal network by isolating the network or other external networks, and limits the availability of the internal network. The firewall is usually installed in the connection between the internal and external network. All traffic from the Internet (external network) or Intranet must pass through the firewall

7. Data encryption technology

Data encryption technology is a technology that re encodes information, conceals content, and protects the actual identity of unauthorized users who cannot obtain information. Data encryption technology has improved the security of information systems, and privacy is one of the main tools to prevent the destruction and analysis of external confidential data. According to the different functions of data encryption technology, it can be divided into data collection, data transmission, data integrity identification, and encryption control technology. Storage data encryption technology aims to prevent data from entering the storage network, and these losses are divided into secret memory and two types of access control. Data transmission encryption technology is designed to encode the data stream in transmission. Data authentication technology aims to verify the relevance of data content to meet security requirements. Compare and verify through the system to ensure that the features of the object comply with the initial value parameters for data security.

In many cases, data encryption is the application of keys. Key management technology actually facilitates the use of data[4]. It includes key generation, fragrance and storage of key management technology, replacement and destruction of security measures. Data encryption technology mainly ensures the encryption of internet data, ensuring the security and reliability of the internet, and effectively preventing the leakage of confidential information. It is also widely used in cutting-edge technologies such as information authentication and digital signatures to prevent interference from electronic deception and plays a crucial role in the security of information processing systems.

8. System Disaster Recovery Technology

For a complete Internet Security Systems, only prevention and detection measures are not enough. It must also have disaster tolerance and system recovery capabilities. Because no network security facility can prevent it 100%, once a leak prevention event occurs, its consequences will be catastrophic. In addition, damage caused by natural disasters, natural disasters, and force majeure may also have a devastating impact on information systems. This requirement has not even been discussed, and it is necessary to quickly restore the system and data to ensure the complete security of the network information system. The main existing disaster management technologies are based on reserve and tolerance systems. Backing up data is the last defense barrier that cannot go wrong. However, offline media cannot guarantee security. Data containment capacity ensures data security through IP containment capacity technology. Data disaster recovery uses two rams (offline) in one region and creates a replica relationship. The local backup system uses local storage. Real time replication of key data from remote disaster reconstruction backup storage and local backup storage. By connecting the two through IP, a complete data disaster recovery system can also provide database disaster recovery functionality.

Cluster technology is a system level fault-tolerant technology that solves system crashes and unavailability issues caused by which part of a system failure occurs through redundancy and faulttolerance of the entire system[5]. The cluster system can be implemented by two machine hot backup, local cluster network, and remote cluster network, providing different system availability and capacity. Among them, remote cluster networks have the best disaster tolerance. Data storage systems are a comprehensive combination of storage, backup, and disaster prevention technologies, and are an important stage in the development of data technology. With the development of the storage network era, traditional single function memory has been replaced by integrated multi-functional network memory.

9. Intrusion detection technology

Intrusion detection technology collects information from various systems and network resources (system working status, information flow in the network, etc.)[6], and analyzes and judges them. Intrusion detection systems can detect attacks or abnormal behaviors in network systems in a timely manner by detecting them, and respond with blocking, recording, and alerting, thereby minimizing the threat and impact of impacts. At the same time, intrusion detection systems are the behavior of users and systems, audit system deployment and identification of defects, abnormal behavior, and attack behavior, and monitor and track attack behavior or abnormal behavior responses

10. Vulnerability scanning technology

Vulnerability scanning is a technology that automatically detects the security of remote or local hosts. Query the ports of each TCP/IP service, record target responses, and collect practical information about specific projects. The specific implementation of this technology is a secure scanner. The scanner can quickly check for existing security vulnerabilities. Scanner developers utilize available attack methods to integrate them into the entire scan. After scanning, they output in statistical format for reference and analysis.

11. Physical security

To ensure the physical security of information networks, it is necessary to prevent the spatial diffusion of system information. Physical protection is usually used to reduce or interfere with the transmission of spatial signals[7]. To ensure network operation, the following physical security measures must be taken:

Product assurance: mainly includes safety measures such as procurement, transportation, and installation.

Operational security: Devices in the network, especially security products, need to be able to quickly obtain technical support services from manufacturers and suppliers during use. For some important equipment and systems, backup systems should be set up;

Anti-electromagnetic radiation: All important classified equipment should be equipped with anti-electromagnetic radiation products, such as radiation interference devices;

Safety: mainly anti-theft, fire prevention, etc. Including security protection for all network devices, computers, and network system security devices. Computer network security is a comprehensive and complex issue. Faced with the rapid development of the network security industry and the acceleration of social informatization, various new technologies are constantly emerging and applied. Cybersecurity breeds infinite opportunities and challenges. As a research hotspot and of significant strategic significance, I believe that there will be greater progress in network security technology in the future.

12. Conclusion

With the growth of the Internet, network security has gradually become a huge potential problem. Cybersecurity is a broad issue, including whether it is a crime. Its simplest form is to ensure that it is unrelated to employees and cannot be read, let alone change the information sent to other recipients. Most safety issues are intentionally caused by those who want to harm or harm others. As you can see, protecting a network is not just about protecting it from programming errors. It includes guarding against those who are cunning, professional, time rich, and financially wealthy. At the same time, it must be clarified that the method of preventing enemy arbitrary destruction has little impact on recidivism. We should attach great importance to this issue.

Due to the complexity of transmission control, it is easy to cause transmission errors and give others a chance. The management system is not perfect, and network management and maintenance are implemented by one's own devices. But fundamentally, network security is in a quite primitive stage. Its manifestation is that network security based on cryptography and firewall cannot be perfectly combined to become a more effective security mechanism. It is hoped that a reasonable mathematical model will play an important role in the research of network security and the development of practical Internet Security Systems.

References

[1] Du Weili. On Network Security and Prevention Technology [J]. Silicon Valley 2011(07).

[2] Yuan Jinming. Analysis of Network Information Security and Prevention Technology [J]. Information Security and Technology 2015(11).

[3] Yuan Wenxin. Exploration of hidden dangers and prevention methods in computer network security in universities [J]. Network Security Technology and Applications. 2019 (12).

[4] Wei Changchao, Feng Tao, Li Xingxiang, Yang Fei, Tian Shujin. Research on Network Security Hazards and Network Security Technology Strategies in Computer Rooms [J]. Electronic testing. 2019 (02).

[5] Yan Sida. The influencing factors and preventive measures of computer network security technology [J] .Information and Computers (Theoretical Edition). 2011 (12).

[6] Zou Yang. Application of Computer Network Security Technology in Network Security Maintenance [J]. Shandong Industrial Technology. 2019 (04).

[7] Wang Zhongtang. How to Apply Computer Information Management Technology in Network Security [J]. The Age of Think Tanks 2019(51).