Research on Computer Network Information Security Technology

Yan Yang

Officers College of PAP, Chengdu, Sichuan, 6102132, China

Keywords: Network Information Security, Information Attack, Risk and Its Management

Abstract: This paper starts with the basic concepts of network information security and existing security problems, and briefly analyzes digital security technologies such as information encryption technology, digital abstract, digital signature, digital envelope, digital certificate, etc., focusing on the application of firewall technology in network information security. The function, type, architecture and development history of firewall technology are analyzed. The development and application of the new generation firewall technology are discussed. A hybrid firewall system is designed in combination with the work of the unit information transformation.

1. Introduction

With the continuous development of computer network technology, global informationization has become a major trend of human development. Computer networks have been widely used in the defense and military fields, finance, telecommunications, securities, commerce and daily life, especially in the United States not long ago. The establishment of the cyber warfare command and the idea of network-centric warfare, especially the importance of network technology. However, due to the diversity of connection forms, the uneven distribution of terminals, the openness and interconnectivity of the network, the network is vulnerable to hackers, geeks, malware and other unscrupulous attacks. Therefore, the security and confidentiality of online information is a crucial issue. Therefore, the network must have sufficient security measures, otherwise the network will be useless. On the contrary, it will bring various harms to the users, and even serious national security. Vulnerabilities and potential threats, such as natural and man-made, exist in both local area networks and wide area networks. Therefore, the security measures of the network should be able to comprehensively address different threats and vulnerabilities, so as to ensure the confidentiality, integrity and availability of network information.

2. Risk sources of computer network information security

In daily work, life and study, most computer network users have changed the settings that were originally used to protect the confidence and security of the computer network for easy operation. For example, the protection level of the firewall, the real-time monitoring function of the anti-virus software, and the operation. System patches, etc. Once the computer network encounters network risks such as viruses and Trojans, it cannot effectively defend, and ultimately the computer network information security is seriously threatened.

At present, most computer network information security protection systems are still based on software protection. Because software protection has a certain lag, it needs to be updated in time to achieve protection. Therefore, simply using soft protection does not work. More obvious effect. Although the construction of computer network information security protection system with soft protection as the core saves costs, the losses caused by external security risk factors will be irreparable. Hackers have become well-known words for computer network users. They use the vulnerabilities in the computer operating system to take special intrusion methods to control the computers of computer network users. The purpose of hacking is to destroy operating systems, files, etc., and even steal internal computer files by invading other computer network users. For computer network information in the era of big data, hacking is a factor that reduces the security of computer network information. The so-called hacking is a kind of behavior of human beings to maliciously

DOI: 10.25236/scmc.2019.007

destroy network information, including active attacks and passive attacks. For active attacks, there are certain characteristics. The attack information targets destroy the integrity of network information, which in turn affects the normal use of network information. For passive attacks, it is a means for network information to be cracked and intercepted. Under normal circumstances, it will not hinder the smooth use of the network. These two hacking behaviors will have certain impact on the network information data, resulting in the lack or distortion of the network information, which will threaten the security of the computer network, and even cause the network system to paralyze, causing security risks on the computer network.

In the process of using the Internet, the criminals invade the user system, mainly by acquiring viruses from the computer and breaking the computer firewall to obtain other people's information. With the development of computer network technology, computer education has also received attention. Some computer professionals provide information security for enterprises and institutions after they work, but some computer professionals use computer technology to influence public information security. Such practices have violated the laws of our country, and must be strictly handled by those who have malicious acts such as malicious intrusion into other people's computers and dissemination of other people's information. Computer-implanted virus is a relatively common method of information acquisition and destruction. Viruses are often downloaded and installed in small programs. Once a virus is implanted in a computer, it will spread rapidly, destroying the normal operation of the computer, even to Later, it will cause the entire system of the computer to crash. The types of implanted viruses have evolved to a large extent. For computer destroyers with a large variety of viruses and fast transmission speeds, in order to completely eradicate, it is necessary to establish a complete computer control system. However, after analyzing the current computer control system, it is found that the management method cannot cope with the existing viruses and hackers, and the chaos of the control system is the key to frequent problems in information processing and security. If we continue to let development go, it will only affect the development of China's information technology and make our national information in an insecure state. Therefore, it is necessary to improve the computer control system, give better development of information technology in China, and ensure the national information of our country.

3. Computer Network Information Security Technology

In order to be lower than the security risk of computer network information, researchers have designed various types of computer network information security technology, including information encryption technology, firewall technology, intrusion detection technology, and the application of the above technologies to achieve further computer network information security. improve.

The so-called information encryption refers to the effective protection of information stored on a computer or transmitted through a computer network according to a pre-agreed agreement. In the field of computer network information security technology, the use of information transmission encryption is more common. Through the use of link encryption, node encryption, and end-to-end encryption technology, information security problems caused by network information monitoring can be effectively prevented. In the aspect of information encryption technology, the most important one is the encryption algorithm. The more complex the algorithm, the higher the security factor of the information. However, this also increases the decryption burden of the computer network during the information transfer process. Therefore, in the process of computer network information transmission, the encryption algorithm should be selected according to the importance of the information transmitted, so as to improve the information transmission efficiency.

Firewall technology is an important guarantee for computer network information security. A reasonable setting of firewalls can effectively control external information security risks and enter personal computer networks. At present, mainstream firewall technologies include packet filtering firewall technology and proxy firewall technology. Moreover, shielded router technology can be used to filter and judge access IPs, and filter IPs that are at risk to restrict access. In terms of computer network information security, Internet intrusion detection technology is a computer network information security defense measure that integrates hardware protection and software protection. In actual use, the computer intrusion detection software can monitor the network traffic, and judge whether the computer network is invaded by the change of the Internet traffic and the monitoring of the main process of the computer. Once the intrusion condition is met, such as the networked intrusion detection software. The computer will be disconnected from the network and the source IP address of the router will be detected and added to the blacklist.

The scope of big data applications is very broad and has penetrated into the work and life of human beings. With the continuous development of science and technology, big data has gradually entered the era of intelligent informationization, which means that human beings can access events happening in society from any place. For example, human beings can understand the actual trend of logistics through the technology of the era of big data. The level of physical health and the status quo of the use of electrical equipment fully demonstrate that the application of computer networks in the era of big data provides many useful information for human life. Therefore, in order to effectively ensure the security of computer network information, on the one hand, we must improve the relevant legal provisions on the use of information in the era of big data. On the other hand, we must formulate a special information security protection mechanism to reflect the authority and persuasiveness of the law and ensure the information of computer networks. Safety. In addition, relevant national agencies should strive to develop effective computer network security protection laws in the shortest possible time, so that people can ensure the security of personal information during the application of computers. In recent years, the Internet industry has developed rapidly, and the authenticity of data information is increasing and has multiple values. Therefore, more and more companies are developing computer technology to maximize economic benefits, but they ignore the security of computer network information. In response to this situation, China needs to attach great importance to it and systematically manage and constrain computer-related enterprises. In addition, relevant institutions need to establish a specialized management department for computer network information, and require relevant personnel to regularly conduct anti-virus verification on relevant code information of network operation, and ensure the security of computer network system by means of human inspection to ensure the security of network information. Sex

In the design of intelligent network information security defense and self-recovery system, the fuzzy recognition technology used in the intelligent firewall is skillfully integrated, and the external access is intelligently controlled through data identification. Moreover, when the computer network is subjected to an external attack, the intelligent network information security defense and the self-recovery system determine the defense result. In the case of a failure, the system will back up, transfer, and internal all the files. The file is destroyed, and after the attack is completed, the computer system is restored, thereby effectively avoiding a series of problems such as leakage of internal information of the computer caused by external attacks.

4. Conclusion

In the modern information industry, computer network technology is more representative. Computer network technology not only enhances the personal information receiving ability, but also changes the working mode of various enterprises and institutions. Therefore, professional and technical personnel need to continuously improve information security technology. Conduct research to ensure the safety of user information and promote the rapid development of China's social economy.

References

[1] Yang Bin. Analysis on the Research and Development Trend of Computer Network Information Security Technology [J]. Science and Technology, 2009(20):227.

[2] Yao Xinying. Research on Computer Network Information Security Technology in the New Period [J]. Silicon Valley, 2013, 29(22): 166-166.

[3] Wang Jun. Research on Information Security Technology of Computer Network [J]. Silicon

Valley, 2012(16): 120-121.

[4] He Wei. Research on Data Encryption Technology in Computer Network Information Security [J]. Electronic Technology and Software Engineering, 2016(18):231-232.

[5] Tang Huilan. Research on Computer Network Information Security Protection [J]. Wireless Interconnect Technology, 2019(12):31-32.