

Analysis of Computer Communication Network and Its Security Technology Architecture

Ye Shao^{1, a}, Jing Liu^{1, b}, Wenbo Jiang^{1*, c}

¹ Haikou College of Economics, Haikou, Hainan, 571127

^a email, ^b email, ^c email

Keywords: Computer Communication Network, Security Technology

Abstract. With the development of scientific and technological information, computer technology has been widely used in various industries, the computer as the core of the communication network is to penetrate into people's production and life. In today's Internet age, computer communication network has been inseparable from people's lives, the progress of society and the promotion of life has played a huge role. The global computer communication network are faced with the frequent attacks of hackers, computer communication network security has become the focus of widespread concern. Therefore, it is of great significance to strengthen the research on the security of computer communication network, study its related technology and improve its safe and stable operation performance. This paper analyzes the problems and causes of computer communication network, and discusses the related core technology.

Introduction

Today, the global computer communications network security are facing enormous challenges, hackers, viruses and other frequent father, to the computer communications network security caused a great threat. In order to meet the global computer communications network security development needs, related technology has been rapid development and promotion. Computer communication network security technology is through the use of professional technology, the computer communication network system hardware facilities, software applications, data, etc. to maintain, shielding unauthorized users access. In other words, in order to reduce the computer communications network technology security risks, to take a series of related technical protection.

Computer Communication Network Security Factors

At present, the popularity of computer communication network is getting higher and higher, the openness of communication network is more and more obvious. The openness of the network, while improving its convenience, also increases the threat to network security. Moreover, many computer communication network software system is not perfect, there are some loopholes in their own, in addition, the Internet TCP / IP protocol also exists more security issues. Therefore, in an open network environment, if there is no higher level of security index and strong protective measures, the communication network is very vulnerable to hackers, illegal users and other attacks and violations.

In the process of computer development, the emergence of computer viruses also poses a great threat to the security of communication networks. Computer viruses through the computer program to insert a certain instruction, code, procedures, etc. to destroy the computer system, with a strong communication and destructive. At present, the rapid development of computer viruses, and the increasing number of species, more and more harmful, is one of the major threats of computer communication network.

In the information age, the value of information, whether for individuals or enterprises, and even a country and the development of society are essential, the security of information is today's society are very concerned about the issue. In the computer communication network, only the realization of the transmission of information in order to really play its effectiveness, and the transmission of information requires a certain transmission channel to achieve. At present, the design of computer

communication network transmission channel is not perfect, the signal shielding technology can play a more limited role, the relevant shielding measures are not enough advanced, therefore, the transmission of information protection is not enough, it is easy Will be intercepted, the emergence of information leaked, tampered with, lost and other events, resulting in adverse effects.

In computer communication network security, human factors also have a significant impact, which usually shows the relevant management of network security awareness and network maintenance technology is not strong enough. For example, in the network security awareness, some staff confidential awareness is not strong, will intentionally or unintentionally password, password and other security key leaked out, and the password is not enough to set the science, the encryption is not encrypted, and some password Information is not long-term change, a code and more; in network maintenance technology, some staff of the technical level is not high enough, the operation is not standardized, skilled, safe maintenance and protection efficiency is not high enough. These are the computer communication network there are a lot of security risks.

Computer Communication Network Security Problems and Its Causes

First, the openness of the network. Computer communication network is an open platform, people can freely transfer data through the platform, for information exchange and sharing. In the process of free transmission summary, it is inevitable that the data leakage, the data confidential work caused great trouble. In addition, the complexity of the network, from the wiring network to the communication transmission, any one part of the quality problems, will cause the computer communication network security. Second, the software defects. Computer communication network system contains a large number of software, a lot of software in the design of some flaws, and the application of the communication protocol there are some loopholes, which have become a computer communications network security risks. Computer communication network system using the basic protocol is TCP / TP protocol, but also the basis of the entire computer communication network, but its design process there are more defects, focusing on the effect and ignore the security performance, which resulted in a lot of software Application of this agreement under the operating safety performance will be greatly reduced. The software itself, the existence of defects and vulnerabilities, it is easy to be exploited by hackers, directly into the computer communications network, resulting in security damage.

First, people leaked. Many people engaged in computer communication network work of the overall quality of the lower, the lack of a certain degree of professional ethics, intentionally or unintentionally will leak the relevant secret information. Then there are some staff in order to obtain personal interests, the use of their own occupation will steal the secret information within the network, and even set the Trojan virus, disrupt the security of the communication network. Second, the network hackers. Internet hackers have a high level of professional computer, and hands-on operation ability, for different purposes, the computer communication network to attack. Some Internet hackers in order to obtain high economic benefits for illegal companies to steal business secrets or important data information; some network hackers in order to show off their skills, in the network to create a variety of mischief, damage the computer communication network security and stability ; And some Internet hackers through the preparation of the virus program, directly to the Internet, greatly damaged the communications network security.

Key Technologies of Computer Communication Network Security

In the process of designing a computer communication network, from hardware facilities to software programs, we must fully consider the performance of its play, as well as the protection of security. In the initial design of the network system, it is necessary to include software applications, data confidentiality, communication protocols and other basic software to enhance the protection of security. And in the use of the process, the more specific requirements of the communication network, the development of different security level authentication system, and the corresponding security measures, and constantly optimize the repair system vulnerabilities, reduce or prevent the

illegal analysis of intrusion network system, stealing important information The

Computer communication network system security, can not be separated from the internal staff to fulfill their duties, to enhance the professional ethics of practitioners, and strengthen the management of employees. Through the introduction of knowledge lectures, technical training, etc., to promote the importance of computer communication network, its safety management of great significance. In addition, we must organize network security technology research households, the organization of experienced technical experts, to the enterprise lectures, to answer technical staff doubts, improve the technical level of employees, so as to better serve the computer communications network security.

Set up a firewall. Firewall as the first barrier to access to the network through the data filtering technology, application network management and proxy technology, users can access the network set permissions, and the user all the connection operations to track the inspection, so as to achieve the purpose of identifying foreign data, and Can effectively limit the illegal data and access to the entry, in order to achieve the security of the internal network security. Password technology. The basic nature of cryptography is camouflage information, the password is divided into symmetric encryption and asymmetric encryption in two ways. In the actual application, the specific performance for the three types, that is, instead of the password, product password and shift password. Which replace the password of the highest frequency of application, by using code or characters instead of plain code character of a password, with high security. Identification technology. In order to prevent the illegal use of information, duplication or tampering, need to use identification technology to be kept confidential, so as to ensure that important information in a safe environment, be legally applied. In the actual use of the process, identification technology, including identification, digital signature and face recognition technology. Only information obtained through the authentication technique is consistent with the original information retained to ensure that the information is used and transmitted. Encryption protocol technology. The network protocol is the basic protocol of the computer communication network, and its security is directly related to the information security on the communication network platform. Therefore, to strengthen the security of network protocols, can fundamentally guarantee the security of information, in the actual application process, mainly through the authentication data and authentication technology, to achieve the network protocol reorganization and variation. In the process of designing a network protocol, the important protocol can be encrypted. If the intrusion is encountered in the transmission process, the protocol will issue an alarm. On the one hand, it can guarantee the security of the protocol through encryption. On the other hand, Out of the protective response.

In the computer communication network security protection, can not ignore the impact of human factors, should improve the network security-related management, technical and other personnel requirements, to strengthen the relevant personnel communications network security training and education, enhance their awareness of security, Their network security knowledge and skills. At the same time, more exchanges and seminars will be carried out to promote network security personnel in the communication and interaction can be more advanced security information, skills and rich practical experience to better improve their work to ensure the safety of communication networks, reliable.

Computer communication network security and protection of the strengthening, the need for a certain management system as a guarantee, so that the relevant work can be more standardized. Therefore, we should strengthen the internal management, the development of computer communications network security management system, set up specialized departments and positions for network security management, but also the establishment of accountability system, designated relevant person in charge, through continuous improvement, to establish a scientific, Standardized, operable computer communication network security and protection management system.

The operation of the computer communication network mainly depends on its system to complete, if the security of its operating system can not be fully guaranteed, then the computer communications network security performance will be threatened. Therefore, in the computer

communication network security protection, should pay attention to the computer system related work performance optimization, can not only focus on its effectiveness and ignore the security issues, to continuously improve its security level, for different data attributes to specify the appropriate security measures , To improve its security protection of the integrity, relevance and effectiveness.

Conclusion

In the information age, to improve the security of network information on social progress and development has a significant impact, so to strengthen the computer communication network security and protection of great significance. We should improve the security awareness of computer communication network, actively analyze and study the factors that affect the network security, and constantly regulate the network security management, improve the computer system and network security technology. At the same time, we should also improve the overall quality of the relevant personnel of the communication network, take various means to improve the security technology and level of the computer communication network, form an efficient security protection system, and effectively improve the security of the communication network.

Acknowledgements

Fund Project: Hainan Province, higher education and teaching reform research key project "Internet of Things construction and wisdom of Hainan research and practice"

Project No.: Hnjg2016ZD-22

References

- [1] Zhao Yuan. Special communication network security problem analysis and maintenance measures [J]. Digital Technology and Application. 2017 (07)
- [2] Fu Manyao. New situation of computer communication network security and protection [J]. China's new communication. 2017 (16)
- [3] Zhao Cigang. Computer communication network security and protection strategy [J]. Electronic Technology and Software Engineering. 2017 (18)
- [4] Wang Yan, Su Guozhong. Key Technologies of Communication Network Security [J]. Digital World. 2017 (08)
- [5] Zhang Li. Communication network security status and countermeasures [J]. Information Systems Engineering. 2017 (07)
- [6] Zhu Chenggang. Computer data communication network security maintenance points analysis [J]. Computer fans. 2017 (11)