Computer Network Engineering Security Problems and Countermeasure Analysis based on Network Security Maintenance

Yutong Chen [a], Baolin Li [b, *]

School of Computer Science, China West Normal University, Sichuan, Nanchong, 637009, China

[a] qqjiangphys@yeah.net, [b, *] jiangqingqua@126.com

Abstract. With the continuous development of the information age, computer information and network technology has been more and more widely used in people's life and production. People get the desired information through the computer network, and realize the purpose of information sharing through the transmission of network information. The application of computer network technology breaks the limitation of information transmission time and space to a certain extent, and is conducive to people's production and life activities. But with it comes the issue of network security. The article mainly analyzes and discusses the current security problems of computer network engineering, and proposes some solutions to how to solve these security problems, hoping to promote the healthy development of computer network engineering science.

Keywords: Computer Network Engineering, Security Problems, Countermeasure.

1. Introduction

With the rapid development of the economy, computer technology is increasingly developed, and network technology is widely circulated in people's lives and work, playing an increasingly important role in promoting social progress and development. Computer network security has a very broad meaning, and this meaning can change due to changes in the application [1]. The general Internet users of our ordinary Internet users usually only pay attention to whether the personal computer will be invaded by the Trojan virus, whether the computer system will collapse, whether the personal privacy of the computer will be leaked, etc., and the network provider pays attention. Not only these [2]. Computer network engineering security issues threaten national security and social order in the broad direction, and are closely related to the daily life of each of us in the small direction. Therefore, the study of computer network security issues, to find solutions to computer network engineering security issues [3]. Once these potential safety hazards break out, they will have a more adverse impact on people's production and life. At this stage, how to maintain network security has become a widespread concern of all sectors of society [4]. Therefore, as computer network technicians, we should enhance the awareness of maintaining network security, strengthen scientific research, enhance the security of computer network technology, and ensure that the network can be carried out safely. In this paper, the author mainly analyses the computer network security problems and preventive countermeasures.

2. Safety and Security of Computer Network Engineering

2.1 Physical Security in Computer Network Engineering

Computer network engineering is a data communication and resource sharing system with functions such as remote communication and remote data transmission, which are composed of communication lines, communication devices, and computers. In the current network situation, everyone can successfully achieve network sharing and network transmission. It is precisely because the computer network has the characteristics of openness, so its security problem has been challenged and threatened. When the computer network completes data communication and resource sharing, the hardware device may cause normal failure due to natural factors or human factors [5]. Therefore, in order to ensure the security of computer network, the integrity of computer network system should be considered first. The integrity of computer network system can be divided into two aspects:

program and data. Only when both aspects are guaranteed at the same time, can the internal program of the system be protected. Generally speaking, any unit first connects to form a network through an internal network, and then accesses the Internet through an external wide area network [6]. Most of the privileges and information secrets of the members of the internal network cannot be accessed directly by the external network. For example, when sending packets with huge traffic leads to the exhaustion of network traffic, the network cannot provide data transmission services for normal users with the attack target of multiple computers and network connectivity, which ultimately leads to the system paralysis.

2.2 Security of Computer Network Engineering System

Computer networks are open, so this can cause a lot of problems for computer networks. It can be said that in the current network environment, anyone can achieve network transmission and network sharing. At present, computer systems are not secure. Common computer system vulnerabilities include: RDP vulnerabilities, VM vulnerabilities and UPNP service vulnerabilities, and computer system vulnerabilities are constantly being exploited, which leads to serious threats to our computer application security [7]. Because of the strong expansibility of computer network, developers can constantly update and upgrade the system. This expansibility provides convenience for hacker attacks and brings hidden dangers to computer network. Therefore, the channel of information acquisition is required to adapt to the development of the times. Information managers need to actively broaden the channel of information collection so as to obtain information resources with high quality and authenticity.

2.3 Security of Computer Network Data Storage

The database storage function of computer network is the function that people use all the time in the process of surfing the Internet. The content that users browse on the Web will be automatically stored in the computer by the computer browser. It also contains personal information such as user's account and account password. Therefore, once the computer operating system has problems, it will inevitably cause some impact on network security. The computer operating system provides many functions for the computer to manage. The two main parts are the software part and the hardware part. When we open a personal mailbox, we will always find that the mailbox is filled with inexplicable emails of various departments, occupying memory and network bandwidth, seriously affecting network quality and obtaining various ways of mail addresses. The criminals attacked the user's computer through a script virus, and tampered or hijacked the web page, causing the web page of the web page to appear pop-ups, causing the user's computer system to collapse. Therefore, the information manager of the enterprise should update the inventory information in the accumulated database in time to prevent the occurrence of a large amount of information that cannot be accessed due to the unsatisfactory update information, which may affect the normal operation of the enterprise.

2.4 Network Virus Security

Nowadays, the humanized design of programming tools and software makes it easier for people to learn to program, and the means of those network hackers are even more first-class, producing a computer virus almost every second in the world. Computer viruses are codes that are inserted by programmers into software or data to destroy computer systems and data. Such codes are parasitic, hidden, infectious and latent. Common computer viruses include boot zone viruses, file parasitic viruses, macro viruses, script viruses, worms and Trolls. Imma, etc. The computer network has a strong virus destructive power and a strong reproductive capacity. In severe cases, it will lead to the paralysis of the entire network system. Therefore, the virus has a great destructive power and spreads extremely fast, which brings great harm to our work and life.

2.5 Hacker Attack Security Problem

At present, there are two kinds of criminals who specialize in computer network attacks. One is to attack and destroy other people's network systems and computers, steal other people's confidential

data for profit, the other is to destroy the network system for fun and prove their destructive ability. These two kinds of criminals are unified. It's called "hacker". In the classification of means of hacker attack, most of the vulnerable hackers are servers, which are attacked by torrents. Hackers control dozens, hundreds or even thousands of computers through Trojan Horse virus, and then control the computer remotely to send connection requests to the same server at the same time, occupying public ports [8]. Usually, some people illegally act against the government and the unit for the benefit. Network attacks are mainly carried out through various means such as registration password, Trojan virus, and listener. Inflict harm on the interests of the country and seriously damage the property of the people. Different software facilities and hardware facilities constitute a computer network. Certain natural conditions provide support for the normal operation of the computer network. In a sense, the security of the computer network depends to some extent on the natural environment.

3. Research on the Countermeasure of Computer Network Engineering

3.1 Improving Technical Preventive Measures

To establish a more secure technology management system, it is necessary to improve the quality of relevant management personnel, and also to improve the security of the network system, strengthen the professional quality of technical personnel, and set every level of technical prevention. Strengthening the management of the network system can restrict the entry of bad network information through legally binding behavior or moral education for netizens [9]. Continuously improve the network security awareness of computer network information technology personnel. Do a good job of controlling network access, control access personnel, and set access rights, so as to effectively protect the network system from unauthorized access and intrusion. At the same time, it is necessary to strengthen the management of user rights. Users should be screened strictly before entering the network. A mechanism must be installed at the interface between the system and the external network to detect the security of external users. Solve the legitimacy of requests, whether internal users transfer confidential non-co-prosperous files to illegal external users, and other issues. Therefore, for networked users, appropriate anti-virus software should be purchased and installed according to the security level. Because the virus library of anti-virus software is always lagging behind the virus, it is also a content that computer network managers must attach great importance to updating the virus library of anti-virus software at any time.

3.2 Strengthen Management Level

Data generated in the process of computer network operation often exists in a dynamic form. Encryption technology is to use the key to control and transform the data, avoiding unauthorized users to modify the relevant data information. Safety management of computer network engineering has always been the top priority, because it plays a very important role in network protection. If only relying on technical prevention to ensure the safety of computer network engineering, it is far from enough. Because more security measures are needed to maintain the security of computer network engineering. For example, to maintain the information security of computer users, to legislate to protect computer network security and strictly enforce the law. Therefore, for networked users, you should purchase and install appropriate anti-virus software according to the security level. Because the virus database of anti-virus software is always lagging behind the virus, the virus database that updates the anti-virus software at any time is also a content that computer network managers must attach great importance to. The security management mechanism of network management is a problem that network users, especially key units, must attach great importance to. For LAN information security, it is especially important to do a good network defense mechanism. Therefore, the specific operation will face difficulties from many aspects. Therefore, it is necessary to further strengthen the network security management of the computer, and only by raising the security awareness of the relevant personnel, can the maintenance of the computer network engineering be more effectively maintained.

3.3 Safeguards at the Security Level

The basic premise of ensuring computer network engineering security is to create a relatively secure physical environment, such as a computer room or a physical space similar to a computer room. Care must be taken when selecting addresses, and it is necessary to prevent physical damage to the computer system due to natural environmental factors. It is important to choose the address. It is necessary to prevent attacks from physical disasters such as the environment, and to prevent human damage. Establish a complete information security hardening system to ensure the safe and stable operation of the system. Second, we must establish a sound network information security management system and clarify security responsibilities. Therefore, improving the self-prevention awareness of computer users is an important part of the computer vulnerability handling measures. Users should be vigilant in the process of downloading or installing software. During the installation of software, some optional plug-ins need not be checked. The anti-virus software in the computer will periodically inform the user to update the virus library. The user should update the virus library on the basis of regularly killing the virus in the computer. In the actual operation process, we also need to control the access of virtual addresses and restrict the access rights of users, such as identity recognition, so that we can avoid the damage to computer network security caused by illegal intrusion to a certain extent.

3.4 Comprehensive Preventive Measures for Computer Network Engineering Safety

It is necessary to strengthen the education of network security so that both managers and users can realize the importance of computer network security. Increase network management, so that the safety awareness and professional technology of relevant personnel have been improved. Therefore, it is particularly important and key to maintain network security when authenticating user identity information. Users should use passwords and passwords to achieve the privilege classification of network system. Due to the unreliable transmission of network links, data is easily intercepted in the process of transmission. In order to avoid the leakage of confidential data, it is necessary to encrypt the transmitted data according to encryption technology, which can be divided into symmetric and asymmetric encryption symmetric encryption. The cryptographic technology includes confidential technologies and digital signatures of different networks. There are three ways to encrypt the network. The first is the node-to-node encryption, the second is the end-to-end encryption, and the third is the link encryption. In addition, it is necessary to improve the protection function of the computer system firewall. The firewall technology is also divided into three types, one is packet filtering technology, one is proxy technology, and the other is application gateway technology. Therefore, on the one hand, we must strengthen the research and development of computer network engineering hardware and software security, ensure the computer network application system that provides consumers with more perfect and safe, and on the other hand strengthen the security management of the computer building application, and install the latest computer system in time. Security patch. At the same time, the firewall technology and the intrusion detection system are linked together to complement each other, which can provide a reliable guarantee for the security of the computer network.

4. Summary

In the current era of rapid progress, the process of informationization is being accepted by all mankind. Gradually, human beings have become dependent on the network. The computer network system itself also has certain loopholes, which makes the computer network run more and more hidden dangers, which has a negative effect on social development. To a certain extent, it also restricts the healthy development of computer networks, and the use of computer network crimes is a serious phenomenon. Therefore, according to the direction of the development of modern network and the future trend of development, it is the best guarantee for maintaining network security and national diplomacy to do a good job of network security protection and enhance network defense ability. In order to maximize the security of information, we should strengthen the education of computer network security while improving the technology of computer network security protection strategy.

Only by improving the quality of citizens and two-way combination can we maximize the security of information.

References

[1]. Davis J J, Foo E. Automated feature engineering for HTTP tunnel detection[J]. Computers & Security, Vol. 59 (2016) p. 166-185.

[2]. Feng J, Lu G, Wang H, et al. Supporting secure spectrum sensing data transmission against SSDH attack in cognitive radio ad hoc networks[J]. Journal of Network and Computer Applications, Vol. 72 (2016,) p. 140-149.

[3]. Freitas B, Matrawy A, Biddle R. Online Neighborhood Watch: The Impact of Social Network Advice on Software Security Decisions[J]. Canadian Journal of Electrical and Computer Engineering, Vol. 39 (2016) No. 4, p. 322-332.

[4]. Jayaraman B. Special Issue on Security and Performance of Networks and Clouds: Guest Editor's Introduction[J]. The Computer Journal, Vol. 55 (2018) No. 8, p. 907-908.

[5]. Puthal D, Mohanty S P, Nanda P, et al. Building Security Perimeters to Protect Network Systems Against Cyber Threats [Future Directions] [J]. IEEE Consumer Electronics Magazine, Vol. 6 (2017) No. 4, p. 24-27.

[6]. Li T, Jung T, Qiu Z, et al. Scalable Privacy-Preserving Participant Selection for Mobile Crowdsensing Systems: Participant Grouping and Secure Group Bidding[J]. IEEE Transactions on Network Science and Engineering, (2018) p. 1-1.

[7]. Li A, Pan Y. A Theory of Network Security: Principles of Natural Selection and Combinatorics[J]. Internet Mathematics, (2015) p. 1-60.

[8]. Moyano F, Fernandez-Gago C, Lopez J. A model-driven approach for engineering trust and reputation into software services[J]. Journal of Network and Computer Applications, Vol. 69 (2016) p. 134-151.

[9]. Jiang Y P, Cao C C, Mei X, et al. A Quantitative Risk Evaluation Model for Network Security Based on Body Temperature[J]. Journal of Computer Networks & Communications, Vol. 2016 (2016) No. 4, p. 3.