Research on Computer Network Security and Network Technology

Jiyong Li

Applied Technology College of Soochow University, Suzhou, Jiangsu, 215000, China

lijiyong@suda.edu.cn

Keywords: Computer Network, Network Security, Security Issues, Network Technology

Abstract: Since the 21st century, computer and network technology have developed rapidly. The information age has gradually penetrated into all aspects of human existence and life, the development of the network has had an unprecedented impact on human life, and has gradually become a necessary part of people's life. At the same time, the security problems of computer network are gradually revealed, which has caused a series of troubles to human use of computer network, which makes human sometimes can not use the network technology normally and smoothly. Most of these problems are caused by the problems of computer network itself, which leads to the computer network extremely vulnerable to various attacks. This paper discusses various problems existing in computer network security, and makes more in-depth research and analysis on some common network security technologies, so as to provide the necessary guarantee for computer network security.

1. The Importance of Computer Network Information Security

In general, the 21st century is the information age of computer network, and the popularization of information network has already gradually occupied all levels of human social life. But according to previous data reports, hacker attacks and the wanton spread of network viruses have caused economic losses of at least $170 billion a year worldwide [], which is only a direct economic loss to major companies and groups, but the indirect economic losses caused by them can not be estimated. However, the network information security awareness of ordinary people is more weak, its network security prevention ability is also weaker, which gives some people with ulterior motives a chance. Therefore, if the computer network problems, it causes not only economic losses, more likely to endanger some of the country's information security. Moreover, the current problem of network information security in our country is especially serious, so the problem of computer network information security is the top priority for the whole world. Therefore the computer network security question has the extremely important theory research necessity.[1]

In the rapid development of information age, the application of computer network has been widely popularized, but followed by the rapid growth of network information transmission, some departments and institutions benefit from the network to speed up the operation of business, while its data left on the Internet has also been leaked and attacked to varying degrees.The attacker can not only eavesdrop on all kinds of related information content on the network, steal the password of the user and the relevant information content in their database, but also tamper with the content in the user database and forge the identity of the real user. What's more, these attackers are also able to arbitrarily delete content from user databases, destroy their network nodes, and spread computer viruses indiscriminately. However, both in the wide area network and in the specific local area network, the security measures of the computer network should be able to be targeted to various different vulnerabilities and threats, only in order to ensure the integrity, confidentiality and availability of network information content.[2]

2. Current Situation of Computer Network Security

2.1. Hardware Equipment for Computer Networks

  DOI: 10.25236/cseem.2020.057

In the whole computer network, the hardware equipment is the basic condition foundation of its operation, but the computer hardware itself will also have the security hidden trouble problem to a certain extent. One of the leakage of electronic radiation, this problem can not be ignored, but also the most important security risks in the hardware. The most simple is that the computer and the network contains electromagnetic information leakage, which leads to the information inside the leak, leak, theft of the possibility of higher. In addition, the security risks of network hardware are also reflected in the communication part of information resources, which is also extremely fragile, because the computer will continue to carry out data transmission and interaction in operation, this operation process will be achieved through the hardware equipment of the network. Such routes as special lines, optical cables, telephone lines and microwaves, especially the telephone lines and microwaves.

2.2. Secure Kernel Technology for Computer System Operation

As we all know, today is the era of network information, the specific visible figure 1, and the security of network systems and computers and as well as operating systems have an inseparable close relationship. Because the operating system of the computer is a few main factors used to build the connection between users, the hardware equipment and software of the computer. However, if the computer's operating system wants to run stably and safely in the extremely complex information network environment, there will inevitably be a variety of vulnerabilities, especially security vulnerabilities. System vulnerability and backdoor are the most important security factors in computer operating system.

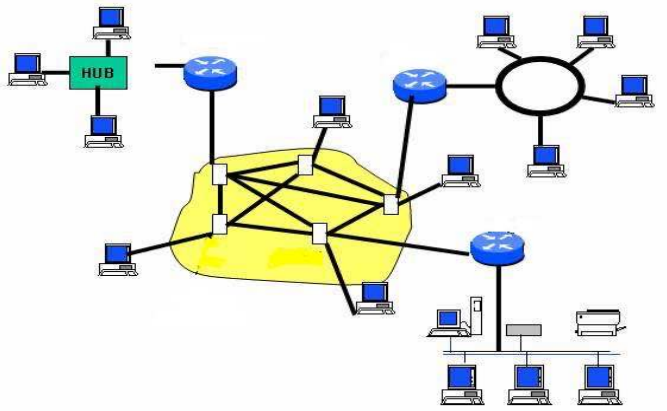

Figure 1 Scope of the situation on the internet today

2.3. Software

Computer is certainly involved in a variety of APP, but because the software itself has a certain degree of software design and application defects. And there are many aspects involved in these defects, not only some Mini Programs, but more importantly, it involves all aspects of some large software, and these defects will inevitably lead to the risk of user property and social stability can cause a relatively large threat. According to the report data, many practical cases of computing network security can be seen that most of the security problems in computers are caused by the existing defects of their software itself. Therefore, we must pay attention to the computer security problems brought by computer software.

3. Four Main Factors Affecting Computer Network Security

3.1. Lack of Awareness of Network Security Among Network Users

In a network that itself is fully secure design, because human factors lead to security vulnerabilities, which is undoubtedly one of the biggest hidden dangers affecting network security. But in reality the network administrator or the network user all has the corresponding some authority, they may use these own authority to destroy the network security, has caused the hidden

danger also to occur endlessly. For example, the user's operation password has been leaked, used temporary files have not been deleted in time, resulting in theft, tampering, and for example, internal management personnel deliberately leak information to hackers, so that hackers can take advantage of the opportunity, these actions may affect the security mechanism of the network.

3.2. Tcp/ip Protocol Lacks Security

So far, there are still a variety of security problems on the network, the main reason is that the structure and system of TCP/IP protocol cluster, the TCP/IP designed at the beginning of the lack of security considerations, resulting in this vulnerability point to "hackers" used to attack computer information networks, resulting in the network upload information is easily intercepted, stolen and tampered with.

3.3. Security in the Operating System of the Computer Itself

At present, many computer operating systems have network security vulnerabilities and various back doors, especially the Windows operating systems that currently occupy most of the market, and the security vulnerabilities of this system appear one after another. And hackers and some viruses rely on this one by one vulnerabilities to the system intrusion, resulting in computer security is threatened and destroyed.

3.4. Lack of Monitoring Tools and Assessment of Network System Security

At present, the evaluation and analysis of network system security is to carry out various checks on the network system to find out whether there are security vulnerabilities that may be hacked.The security status of network system is evaluated and analyzed, and then practical and effective suggestions are put forward to improve the security of network system.

4. Computer Network Security Measures

4.1. Increased Security Awareness Among Network Administrators and Users

Computer network administrators and terminal operators can choose different operation passwords according to their own different responsibilities, and legally operate the data of the application, as shown in figure 2, which can prevent users from exceeding their authority to access some private data and use some specific network resources.In the computer, when the virus attacks the application program on the net, the virus exists on the medium of the network, which must be fortified on the network level, and the antivirus operation must be carried out at the front end.

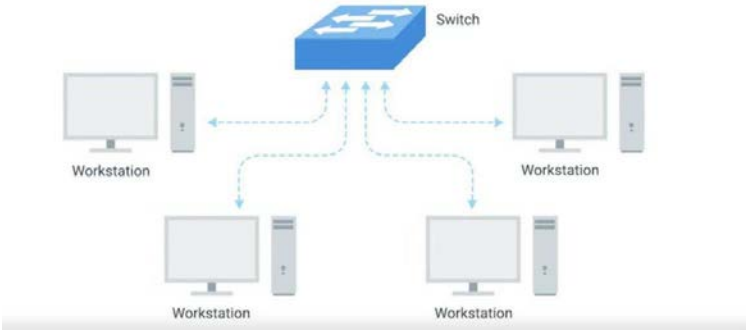

Figure 2 General schematic system for network management

4.2. Network Information Security Encryption Technology

The invention of network information encryption technology provides large or small guarantee for electronic commerce all over the world, so developers to perfect symmetric encryption and asymmetric encryption technology is the focus of the 21st century. Symmetric encryption is a conventional technique based on password, which means that the password of encryption operation and the password of decryption operation need to use the same key. Asymmetric encryption means

that encryption keys are different from decryption keys, such as encryption keys will be made public, but decryption keys will only be known by the decryptor himself.

4.3. Computer Network Firewall Technology

This is a control means to enhance access between network information, see figure 3, in order to prevent users of external networks from entering the internal network by illegal means, and then to access the resource information inside the internal network, to protect the operating environment of internal network users and a specific special network associated device. It can check operations and decide whether the communication rights between network information are allowed and monitor the state of the whole network running.

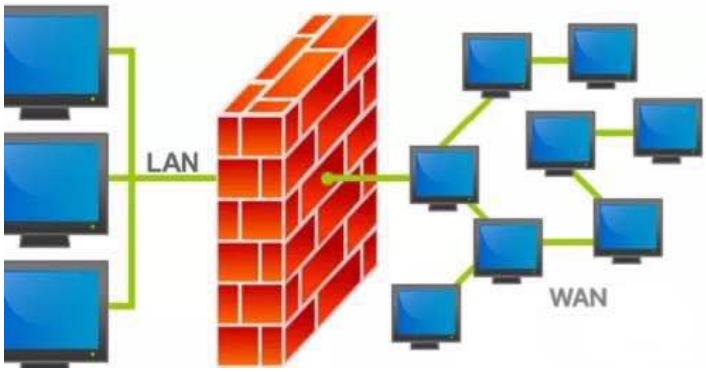

Figure 3 Firewall blocking schematic

5. Conclusion

Since the 21st century, people pay more and more attention to the problem of computer network security. In general, network security technology is not only a technical problem, but also a problem in network security management. The security factors that we must take into account in this regard should be as comprehensive as possible and reasonable plans, plans and supporting regulations should be formulated [3]. With the continuous progress of society, computer network technology has also been rapidly developed at the same time, and the protection technology of computer network security should be followed by the development.

References

[1] Shi, JT., Fan, Yuhong., Liu, Shanghui. et al. Computer Network Security and Vulnerability Prevention Technology Research. Software, vol. 41, no. 2, pp. 273-275,282, 2020.

[2] Wang, Wentao. Application of Computer Information Technology and Research on Network Security. Science and Wealth, no. 31, pp. 138, 2019.

[3] Feijie. Computer Network Security and Firewall Technology Research Digital Users, vol. 25, no. 25, pp. 95, 2019.