Analysis of Computer Communication Network and Security Technology Architecture

Guangnan Liu

Haikou University of Economics, Haikou, Hainan, 570203

Keywords: computer communication network; security technology architecture; skill

Abstract: The 21st century ushered in a new era of computer network and opened up a new era of modern network information. As a booming and mainstream computer communication network technology, the tertiary industry has emerged in a short period of time and has developed rapidly. In today's age of information explosion, computer communication network technology has been widely used in all walks of life, bringing unprecedented changes and convenience to people's lives, and more and more people are beginning to pay attention to information of this aspect. Therefore, it is necessary to study and discuss the reliability design of computer communication networks. This paper focuses on the practice and theory of research and development of computer communication network reliability design technology, briefly describes the factors that affect the reliability design of computer communication network, and proposes corresponding countermeasures for how to optimize the design of computer communication network reliability.

1. Introduction

With the advent of the information age, the digital information revolution is changing people's work and lifestyle. The digital revolution has brought new technologies to the fore. The computer communication network technology is one of its development products. The rapid development of network technology has enabled the Internet to cover millions of households. With the advent of the information age, computer and network communications have developed rapidly, and the use of computer communication network technology has become more widespread. It has not only brought people a lot of convenience, but also has become one of the most important roles in information network systems [1]. At present, China's computer network technology is developing well. However, the technology in communications still needs to be improved. Therefore, in view of the current problems, it is necessary to take reasonable measures to optimize the computer network communication system so as to improve the reliability of network communications.

2. Information and the concept of Computer Communication Network Security and its Causes

The appearance of the computer has improved the work efficiency, has already obviously promoted to the information gathering and the processing and the transmission, the utilization efficiency, but it has the very high request to the information transmission channel. From a theoretical point of view, computer communication network security is to improve the security and reliability of information transmission and processing by preventing security risks in the network operation process. The security of computer communication networks is the most effective way to ensure information security. At present, the trend of integration of communication networks is becoming increasingly apparent. From such development trends, the sharing of information resources is expanding, but it also has a certain impact on people who use them, especially the security issue is very prominent. In this regard, the relevant researchers must take appropriate measures to improve, enhance the security of the communications network, reduce the impact of information security issues on people's lives. Fundamentally speaking, computer network security is to enhance the security of network information through certain methods, reduce malicious destruction, malicious use or falsification of information, ensure the security, integrity and accuracy

of information, and ensure the use of information channels. Correctness [2].

The emergence of any thing is a double-edged sword. The emergence of information technology will inevitably bring about certain negative effects. From the point of view of the emergence of security problems, it can be mainly divided into the following points: First, subjective reasons. The emergence of computer networks has led to the rapid development of a large number of industries. The network software and hardware industry is one of them. However, driven by interests, the hardware and software facilities produced by many merchants fail to pass, resulting in the frequent attacks on people during use. Lead to information leakage, even lost, causing serious losses. In addition, the management personnel of computer network systems lack a sense of responsibility in management and have a weak sense of security. Because of this, many people use computers illegally in the process of operating computers, and shielding facilities are not perfect, resulting in the transmission of information. Damaged or even lost. Many attackers use the software's own flaws to attack the communication system so as to destroy or obtain the required data or information. Second, objective reasons. The computer communication network has its unique operating characteristics. Once these characteristics are recognized by determined people, it will inevitably be used as an attack point to attack the entire network system, destroy the operation of the system, and lead to information loss, even though the speed of patch update is constant. Accelerated, but also from a certain point of view to prove that the system itself has more problems to be solved. Affected by the characteristics of the computer communication network itself, its operation has strong openness and connectivity, which provides network hackers with convenience and facilitates attacks. At the same time, there are some Trojan horses in the network. The virus spreads quickly. Once the system is infected with a virus, it will affect the operation of the entire system, and it will even threaten the entire communications network. The entire system will face the result of a crash, leaving many security issues [3]. Third, the security risks of network transmission channels. In addition to the two points above, there are certain problems in the design of the transmission channel, and the protection facilities are not in place. This will inevitably lead to the loss of information in the process of information transmission. Therefore, this has given many people who are in trouble to take advantage of it. The machine will use some professional equipment to steal information or destroy it, affecting the operation of the entire system. At the same time, there are also some other factors. These factors combine to result in poor overall system security and inadequate system stability.

3. Factors Affecting Computer Communication Network Security

Hackers refer to illegal computer engineers who use superb computer technology to steal information from others and bring safety hazards to people. At the same time when installing computer viruses into the user's computer, the continuous self-replication of computer viruses will interfere with the computer's ability to work, sometimes undermining the computer's program, letting the computer stop working, that is, crashing, restarting and so on. There is also a situation That is, the user data in the computer is destroyed or stolen by them for more benefits. 2.2 Using Software Vulnerabilities Nowadays, Taobao, JD.com, and Vipshop.com’s online shopping platform have developed rapidly. People have become accustomed to this kind of way to buy things without leaving the house. This is also a danger that affects the security of computer information networks. People are When payment software and online banking system payment are made, once one of them leaks, it will reveal a lot of information, causing people to panic. Many people set the bank card password and payment password as one for the convenience of memory, which provides an opportunity for the non-participating elements. 2.3 The security threats of the computer ip address being exploited by the communications network lie in the modification and spoofing of the computer's location information [4]. A computer virus can find the location of a computer user by finding the original path information, thereby transmitting harmful data to the computer, causing damage to the computer. In addition, the IP stream is used to directly destroy the server, and illegal intrusion occurs later. Destroy the user's computer system after copying the desired user data, or install Trojans and monitoring tools. Real-time voyeurism on computer data. Or illegally open the

user's camera or recording device, illegally infringing upon the privacy of the computer user in life and work. This kind of behavior is a crime. It is a kind of computer intrusion that people hate.

4. Ways to Improve the Reliability of Computer Communication Networks

The use of network protection and recovery technologies can effectively improve the reliability of computer communication networks. Both protection and recovery are aimed at network failures, and the flow of the faults connected to the devices is directed to backup connected devices to ensure the continuity of the business. The difference lies in the choice of alternative paths. Protection is to reserve reserved network resources for protection when establishing a connection or planning a network, that is, before a network failure occurs. This method has low utilization of network resources, but can guarantee 100% recovery and comparison of services. Fast business recovery speed. The recovery is that when the network fails, network resources with free capacity are dynamically searched for in the network, and no resources need to be reserved. However, there may be situations in which no free resources are available when a fault occurs, resulting in no guarantee of 100%. Business recovery, and the required recovery time is longer. Nodes (nodes in the device) in the network, links between two directly adjacent nodes, or end-to-end paths can be protected or restored to ensure the reliability of the entire network. The protection of the link or path can be protected or restored. The selection of the solution is mainly based on the degree of service recovery, recovery speed, availability of standby resources, and the cost to be guaranteed.

The principle of reliability of computer communication network is the basic point of ensuring network security. The reliability of computer network equipment should be improved from the following points. First, the quality of computer equipment should be strictly controlled. When purchasing equipment, the equipment manufacturer's actual R&D capability and perfect reliability assurance process should be the primary considerations. To use a comprehensive integrated product development process to ensure the reliability of the hardware and software design of the equipment, adopt system reliability design and optimize the system structure, fully combine the actual situation of the computer communication network to propose a scientific solution, and use comprehensive procurement control, design specifications, etc. Device reliability and application specifications provide closed-loop problem-solving and tracking process solutions to ensure equipment issues can be tracked and resolved in a timely manner [5]. Secondly, properly improve the equipment configuration level and constantly improve equipment business backup protection. The use of redundant backup protection for key functional modules can improve equipment reliability. Thirdly, to improve the reliability of network equipment by improving the protection capabilities of the equipment itself and the reliability of detection levels as a means.

Security audit technology can record the user's intrusion process and activities, and is divided into two stages of trapping and counterattack. Trapping refers to deliberately arranging loopholes and allowing intruders to invade, so as to obtain more intrusion characteristics and evidence; counterattack refers to the fact that the computer system, after possessing more evidence and making full preparations, gives follow-up to intrusion behaviors and queries. Its source and identity, thus cutting off the system's connection with the intruder. In addition, IDS can also be referred to as intrusion detection technology. It can provide dynamic intrusion detection and take effective preventive measures. When detecting a computer network has been illegally invaded, it can give effective preventive measures to block, and can also track and locate and attack. Source counterattack.

The virtual LAN technology developed on the basis of ATM and Ethernet switching technology can develop the LAN technology into a connected technology, further preventing the network from performing illegal operations such as monitoring and intrusion. For example, the information in the company's intranet is separated from the e-mail and data servers to form VLAN 1, and then the enterprise extranet is divided into VLAN 2. This effectively controls the flow of information in the intranet and intranet. The Intranet has access to extranet information; the Extranet does not have access to Intranet data and information. In this way, important internal information and data of the enterprise are protected from unauthorized use and access, which greatly improves the security and

reliability of the communications network.

5. Conclusion

Although the situation of computer communication network security is severe, the current situation can be improved through continuous innovation and technological means. Although we can't find out all the hackers and clear all computer network viruses, we can improve our anti-virus and anti-hacking methods and use various methods to make hackers and viruses unable to start and ensure the security and normal use of computer information. Computer communication network security is a long-term war with hackers, viruses and loopholes. As long as we continue to use new technologies and insist on genuine copyrights, we can gain an advantage in this war.

References

[1] Fan Jixin. Information and computer communication network security technology research [J]. Engineering Technology: Abstract Edition, 2016 (8): 289

[2] Gu Xingshe. Several Researches on Computer Communication Network Security and Related Technologies [J]. Science and Technology Innovation and Application, 2016(5):77.

[3] Xu H. Research on several key technologies of network security situation assessment[J]. Information and Communications, 2015(10):161.

[4] Chen Chengbin. Some research and discussion on the problem of computer local area network security[J]. Electronic Technology and Software Engineering, 2016(9):212.

[5] Ren Yanfei. Analysis and research on reliability design technology of computer communication network [J]. Scientific Review, 2013(13):136-137