Research and Practice of Security Technology in Computer Network

Qinghong Qu
Media College, Baicheng Normal University, Baicheng, 137000,China
email:quqinghong@163.com

Keywords: Computer network; security technology; defense mechanism; development status; service level

Abstract. The arrival of the information age has gradually expanded the practical application of computer networks, provided more convenience for people's lives, and promoted the rapid development of Chinese information industry. In this situation, the process of using computer network has gradually produced network security problems, affected the security of the user's personal information. Affected by various illegal attacks will bury a large security risks to popularization and use of computer network, indirectly reduce the efficiency of a variety of information security transmission, restrict the future level of network services . In order to change the current situation of the development of adverse, we need to pay attention to the rational use of network security technology, structure reliability computer network defense mechanism, enhance the safety performance of network. This will maximize to meet the actual needs of users. Based on this, this paper will carry on the systematic elaboration to the security technology in the computer network.

Introduction

Research on strengthening security technology in computer network will reduce the potential security risks of using computers; provide a reliable guarantee for the security of user information, and optimizing the service function of computer network in long-term use. Therefore, we need to improve the comprehensive understanding of network security technology, the working performance of the computer and structure by using different security technology flexibly, and the utilization efficiency of all kinds of antivirus software. These measures will ensure a stable and efficient working state for a long time, and lay a solid foundation for expanding the scale of China's information industry.

Related Content of Computer Network Security

The Connotation of Computer Network Security. The security of the computer network mainly refers to enhance the technology and safety management mechanism of the security of computer systems, it can make sure that the computer network data, hardware and software resources will not be disturbed by various factors. These interferences result the phenomenon of information leakage phenomenon. The main purpose of paying attention computer network security is to protect the integrity and availability of data information and improve the utilization efficiency of hardware and software. Take the necessary measures to enhance the security of computer network will help to improve the efficiency of the system, expand the practical application of computer networks and meet the needs of users [1].

The Key Features of Various Factors Threatening Computer Security. The objective existence of various factors threatens the security in using the computer network. Under the certain conditions, it may destroy the existing security defense mechanism of computer network and increase the probability of information leakage. Therefore, it is necessary to understand the relevant characteristics of threading computer network security in order to provide effective reference information for the formulation and implementation of various preventive measures. These features mainly include the following aspects: easy to spread and emergent property; Hazardous and destructive outburst; concealment and latent prominence.

When the computer network is destroyed by Illegal attack in normal work, the related information data, file resources of computer network have been destroyed continuity and the diffusion rate is very fast [2]. At the same time, due to the openness and sharing characteristics of computer networks, all kinds of sudden problems are prominent, which indirectly expands the scope of actual impact and threatens the security of computer network.

Interference by various illegal attacks increased the probability of the system being destroyed, which may cause the phenomenon of network emergence. When some latent virus is activated, they will infect the entire network in a relatively short time and affect the security of users' data. All these have a great influence to uses when they use computer network to complete related works [3].

According to the summary analysis the illegal attack phenomenon of the computer network, we can see that these attacks have strong concealment and latent prominent. Many users lack of necessary safety awareness in using the computer network, that result some attacks lurking in the various procedures. Under certain conditions, these will attack the safety of computer network, and threaten the reliability of a user's computer system.

Various Security Risks of Computer Network in the Long-Term Use

Password Intrusion Mode. This way is that intruders can obtain user's passwords with illegal attacks, and then log on the user's computer system to attack. Password intrusion mode requires decipher the user password and implements various illegal operations to the user's computer supported by reliable attack. This buried a great security risk when using the computer networks, and threatened the safe operation of the system.

Various Deception Techniques. When user accessed to computer network through the explorer, like browsing the web, opening interface, entering a strange site, they ignored the network security problems. Illegal intruders tampered the related data and the site interface, buried a larger security risks to user's normal visit. When the user enters the hacker's service interface, they will leave some network security vulnerabilities. These vulnerabilities create favorable conditions indirectly to hackers attacking computer network system.

Threat of Various Network Viruses. As the current biggest security risks threaten to computer network, the network viruses' exist make computer servers infected easily [4]. The network viruses affect the normal operation of the computer system. The ratio of different types of viruses shows in Figure 1. These viruses have certain characteristics: high propagation speed, wide influence and strength destructive power. This brought great challenges to promote the defense level of the computer network security.

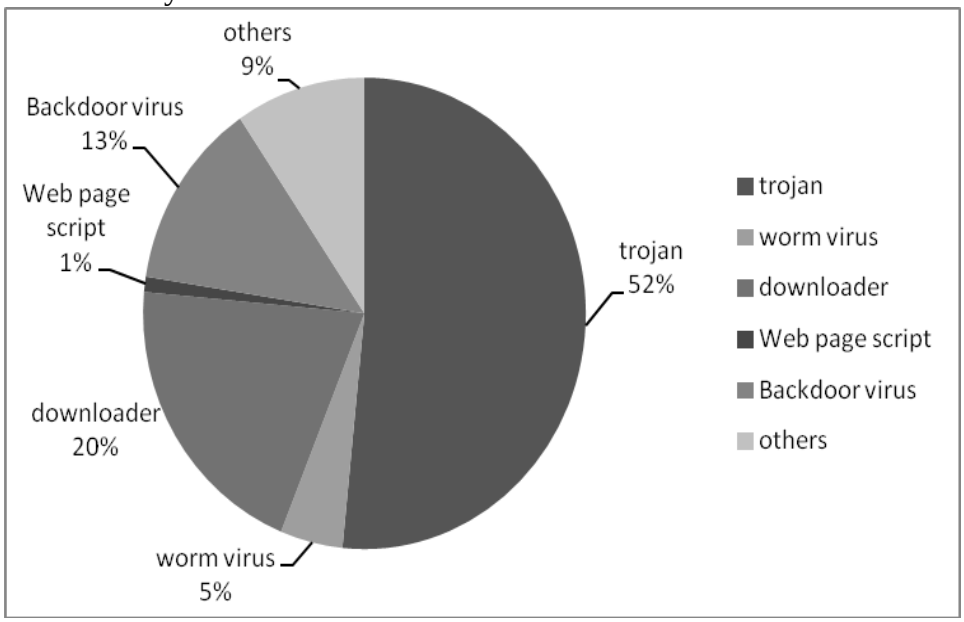

Figure.1Ratio of different types of viruses

Illegal Attack of E-mail. As an efficient and convenient communication tool, e-mail is efficient used in computer networks, which meets the actual needs of user's communication. Network attackers will access to the user's mailbox with illegal software or link address and send mails within a certain period time, which affects the normal use indirectly. When these spam accumulated to a certain extent, it will reduce the efficiency of the mail system. Therefore, to strengthen the effective prevention of illegal attacks of e-mail can ensure the safety of using computer.

Various Security Technologies In Computer Networks

Firewall Security Technology. In order to ensure the security of the computer system, eliminate the potential security problems in the system operation, and optimize the performance of the computer network, we need to pay attention to the effective use of firewall security technology. The working principle of network firewall is: when accessing to the computer system, any user needs through the firewall, and hides the internal information system according to the mechanism. This process makes the user must access the internal structure of the system through the firewall protection, so the firewall enhance the computer network security indirectly and achieve effective protection of the computer system.

Reliable Data Encryption Technology. As an important computer network security technology, data encryption technology has a good effect in actual application. It can prevent the emergence of network intruders tampering user information effectively and optimize the safety performance of the computer network. The principle that the data encryption technology works is encrypting data information in computer network according to reasonable mechanism to enhance network security and eliminate hidden security risks in time. Security technology depends on the network key, and Shift transformation of respective network data to ensure the safety and reliability of the data. Data encryption technology includes the private key and public key encryption technology. When using the public key encryption technology, the encryption and decryption is completed by public key and private key respectively. When the user uses the private key to make the network data encryption come true, network users achieve decryption through the role of public key. The point of public key encryption technology is that the user can have the private key legally to realize the protection of data information. Private key encryption technology only used the same key to encrypt the data. Only the users who obtain the key through the network can access the data information. The information security technology has the advantage of using a DES encryption algorithm to ensure the security of computer networks.

Hacker Intrusion Detection Technology. In order to prevent hackers attack computer network through illegal means, we need to improve the utilization efficiency of hacker intrusion detection technology, so we can achieve effective protection of computer network security. The principle that this security technology works is: when the computer network detected working in abnormal condition, it can issued a security warning in time. The users can deal with the situation with necessary technology. Under the support of the technology, Various violations of network security standards in using computer network can be detected immediately. Hacker intrusion detection technology provide important technical support for enhance computer network security management level.

Effective Virtual Private Network Technology. With the continuous development of information technology, virtual private network technology has gradually become an important technology to protect computer network security. This new security technology relies on the use of ISP and NSP, and achieves computer network security through the construction of reliable private network on the public network. It can reduce cost of the user through the rational use of virtual private network technology, and strengthen the protection effect on using private network through authentication or a reasonable set of encryption methods [5]. These measures play an important role to realize the modernization of computer network security management. Such as authentication technology, tunnel technology, encryption technology, all belong to the category of virtual private network technology. At the same time, with the support of effective virtual private network

technology, it can provide necessary vulnerability protection technology for users to access the computer network, and ensure the safe use of computer network.

Vulnerability Patch Update Technology. Users of computer network existing Vulnerability will increase the probability of illegal attack in system, so it buried a large hidden danger for the security of computer network. Therefore, in order to avoid this kind of phenomenon, we need to focus on the advantages of update patches, and to realize the automatic update of security technology when new vulnerabilities in computer network appears. When this software installed in user's computer, it can detect the computer network vulnerabilities automatically, and remind users to take the necessary preventive measures timely. Like some genuine website patches, Kingsoft antivirus software, 360 anti-virus software, thunder computer housekeeper, they are different forms of updated patches technology. They can improve the reliable guarantee for the security of computer network.

Conclusion

It shows it is important to enhance the security of computer network in the future with the deep research on the security technology in computer network. Therefore, in the future development process of computer network, it should be combined with the actual needs of users and information industry's strategic requirements. We should pay attention to the promotion and application of the relevant security technology, give more emphasis on computer network security problems. In long-term use of computer network, it should ensure that all kinds of information in the network security and efficient transmission, enhance the overall level of service, and keep the high efficient of production plan implementation in relevant industry. At the same time, the engineer should increase the technical personnel of all kinds of security technology; strengthen the understanding of computer network structure; speed up the modernized development of computer network.

References

[1] Wang Jilong, Wu Jianping, Zhu Gang. Research on Key Technologies of Computer Networks and Its Applications [J]. Journal of Software,2002,13(2):266-268.

[2] Chai Zhengwu. Computer Network Security Management and Related Technology Research [J]. Computer Knowledge and Technology,2013,(36):8227-8228,8233.

[3] Zhou Yanzhou, Zhang Huanguo, Song Yang. Research on the Critical Technologies of Trustworthy Networks [J]. COMPUTER SCIENCE,2009,36(6):112-113,143.

[4] Yao Yuchun,Li Jie,Wang Chenghong. Network Virus & Network Security[J]. JOURNAL OF CHONGQING UNIVERSITY(NATURAL SCIENCE EDITION),2003,26(9):141-144.

[5] Zheng Qian,Wang Wei. Analysis on the Effect of Virtual Private Network in the Computer Network Security [J]. Value Engineering,2014,(35):196-197.