Research on security of computer network information and its protection strategies

Xiangcheng Xie

College of Computer, National University of Defense Technology, Changsha 410073, China

xiexiangcheng1@163.com

Keywords: Computer network, Information security, Influencing factors, Protection strategies

Abstract: In recent years, with the widening of the application field of technology of computer network information, it has played an increasingly important role in various industries of the society, which greatly facilitates the development of all kinds of work. Based on this, this paper introduces the factors affecting security of computer network, and analyzes the protection strategy to improve security of computer network information.

1. Introduction

At present, people's life and production aspects are inseparable from computer network technology. The use of computer network technology greatly improves the convenience of people's work, but also brings some security problems. In the process of using the computer network, the security problem will cause certain impact. Therefore, necessary measures should be taken to strengthen the protection of security of computer network information.

2. The security of computer network information issues

2.1 The computer network itself is fragile

With the widespread application of computer network, we need to face the problem that the main characteristics of Internet technology are its openness, practicality and intellectuality. These features are double-edged swords, which not only facilitate users, but also bring security risks. For example, Shared network resources can fully meet people's needs for information, but also become a way to attack or invade. The opening of the computer network makes it very vulnerable to attack. Once the computer network is attacked, there will be serious security problems. Provided that it cannot be solved in time, serious impact on the security occurs no matter enterprises' or individual users', and even cause’s severe property losses. At the same time, the IP protocol of the Internet network does not have high security, which leads to different kinds of attacks in the operation of the computer network, as well as security problems such as tampering of data and denial of service, which seriously affect the experience of network users.

2.2 Network security problems caused by natural disasters

Although computer network technology is constantly developing. But a computer is still a machine that cannot withstand external damage. In the event of a major natural disaster, or the impact of a harsh natural environment, serious damage to computers can be done. At present, many computers are not equipped with corresponding equipment of heat protection, which makes them less able to resist the impact of the external natural environment. This is mainly because the grounding system of the computer is not fully considered. Once the grounding system cannot be taken into account, computers affect with large changes in external temperature and humidity. At the same time, some natural disasters such as rainstorms, earthquakes and tsunamis can damage computers. Therefore, it is necessary to protect the external equipment of the computer, improve the waterproof

and fireproof function of computer equipment during the installation process, and effectively guarantee the safe operation of the computer.

2.3 Network security problems caused by man-made attacks

At present, the poisoning of the computers becomes a kind of phenomenon of the common occurrence. For some hackers will use their own knowledge of the advantages of computer technology to invade other people's computers, which will pose a serious threat to the computer network. This kind of artificial computer network security problem basically divides into active attack and passive attack. Active attack means that hackers adopt corresponding methods, and selectively destroy the new integrity of the computer, while passive attack means intercepting and decoding all kinds of information without affecting the normal operation of users. No matter either way of attack would be taken, it can cause the release of important information. The leakage of computer network information will lead to the loss of important data of network users, which will seriously endanger the computer network security. At present, some computer system software is in an immature state, and the software will be vulnerable in operation. Hackers will steal sensitive information by using the vulnerability of calculation, and then cause serious rigidity to the normal use of user information network, which will lead to the paralysis of the computer system and the loss of a large amount of data information.

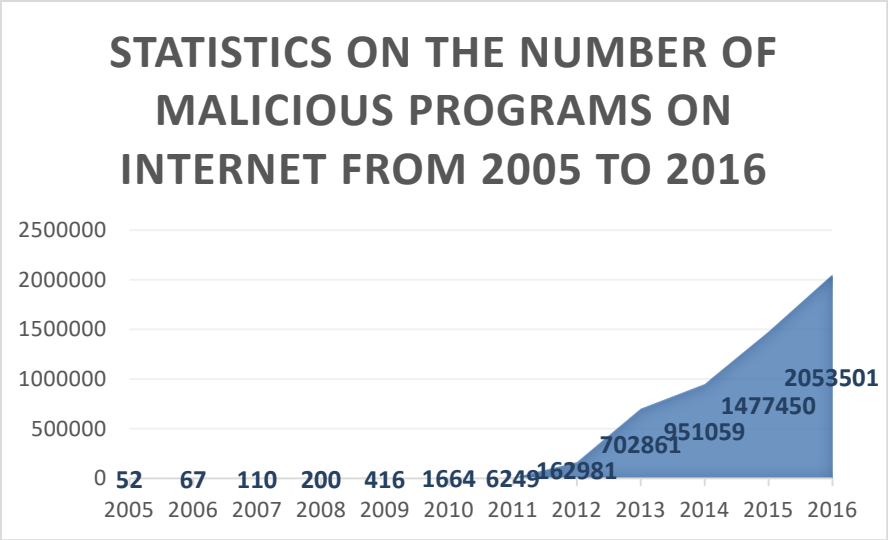

Figure 1. Statistics on the Number of Malicious Programs on Internet from 2005 to 2016

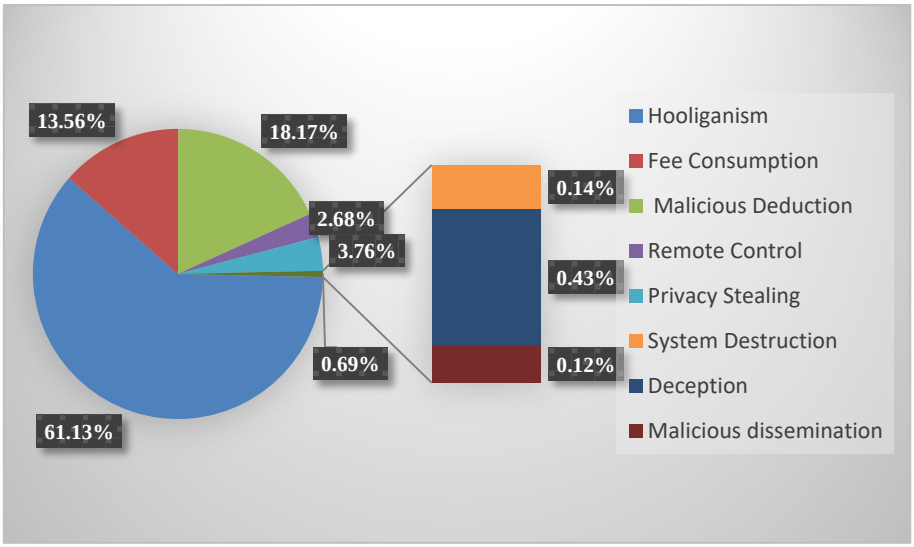

Figure 2. Statistics of Internet Malicious Programs by Behavior Attribute in 2016

2.4 Computer viruses

Computer viruses can spread quickly and are often difficult to eradicate. They can attach themselves to various types of files, and when files are copied or transferred from one user to another, they spread with the files. Infectivity is the basic characteristic of a virus. Once a virus is found in a computer in the network, the virus in the computer will spread from the infected computer to the non-infected computer through various channels to achieve self-reproduction. An elaborate computer virus program that enters a system and then generally does not strike immediately, but lurks in legitimate files. They can generally remain undetected for a long time. The more latent the virus, the longer it remains in the system and the greater the spread of the virus. Once a computer virus plays a role, it can not only steal, damage, tamper with data information, but even ruins the computer hardware, causing great harm.

3. The security of computer network information and its protection strategies

3.1 Enhance the security of computer network user's account

In the course of the development of computer network, some security problems have appeared. In order to solve these problems successfully, the security of user account can be strengthened. Generally, the method of hacker attacking computer network is to steal the user's account password. For such security problems, users should not set a simple password. The more complex the login password is, the harder it is to crack. At the same time, when setting an account, try not to set a similar account. The password is mostly composed of letters, numbers and special symbols, which increases the difficulty of the password. At the same time, the password needs to be replaced regularly and a longer password is set.

3.2 Install firewalls and use anti-virus software to prevent external attacks

To guarantee the security of computer network technology, installing firewall is an important means. The firewall can strengthen the access control between the computer networks, also effectively avoid the external network to illegally invade the internal network, and guarantee the security of the internal network, together with protecting the operating environment of the internal network. According to the adopted technology, firewall contains four types as follows. Firstly, conversion of the home address, refers to the conversion of the internal IP address into registered type to prevent the access of internal correct IP address. Secondly, packet filter, means scanning data packets through subcontracting transmission technology, and blocking firewalls if it is found to be dangerous. Thirdly, monitoring type is a type that monitor external access. The last one is the bright proxy type. By setting up a firewall on the computer network, it can block out the danger at the first time when the network creates a vulnerability, with effectively ensuring the security of the operation of the computer network. In addition to the firewall, the installation of anti-virus software is also an important means of protection. With the enhancement of people's awareness of computer network security, the types of anti-virus software are gradually increased, such as Ruixing anti-virus, 360 anti-virus and Jinshan anti-virus, etc., users can install anti-virus software in the computer to play the role of security protection and intercept malicious attacks.

3.3 Use files encryption

In recent years, people use computer more and more widely in the office. In order to solve network security problems and prevent secret information from being stolen, file encryption technology can be used, which can encrypt files and avoid the loss of important data in case of poisoning of the computers. The technology of files encryption can improve the stability of computer information system and also greatly improve the confidentiality of data. In the process of protecting computer network information, digital signature technology is also used to encrypt the data in network transmission in real time, mainly to encrypt the transmission data in line and end to end. Both of these encryption technologies can greatly improve the security of network information. Line encryption

focuses on encryption on the transmission line, and end to end encryption is to send the file encryption, also the recipient needs to use the key to decrypt with effectively guaranteeing the security of the files.

3.4 Timely installation of bug patches

When a hacker attacks a computer network system, one of the common ways is the system vulnerability, and it is possible that hardware vulnerability, software vulnerability and so on become vulnerability. Generally, software and hardware design manufacturers will release corresponding patches after discovering the vulnerability, so as to patch the vulnerability. Users should install the patches timely in the process of using the computer network to avoid the vulnerability becoming a threat to the security of computer network information. In addition, the technical software for detecting the vulnerability can be installed in the computer, such as the COPS software, so as to find the existing system vulnerabilities early and try to repair them to ensure the security of the network information.

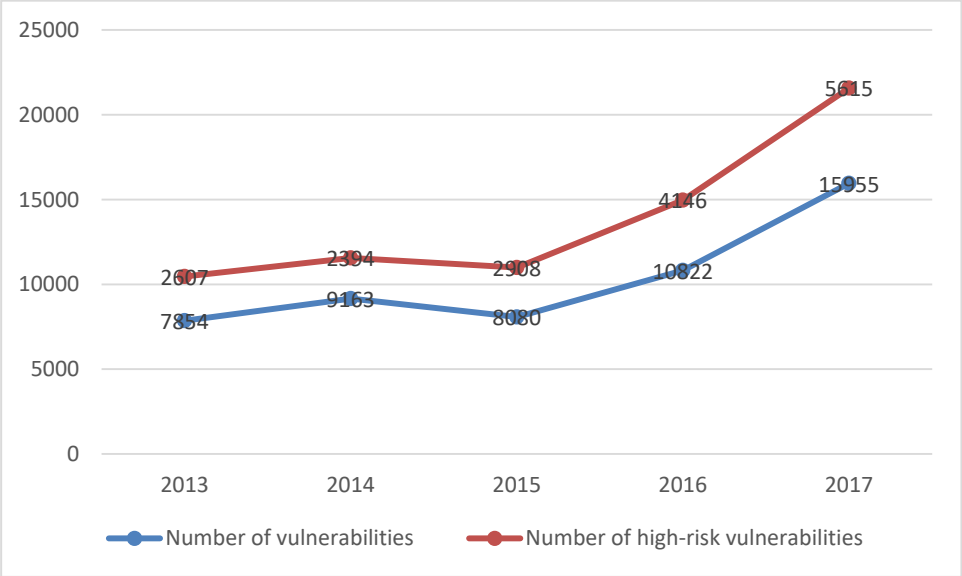

Figure 3. Comparing the Number of Security Vulnerabilities Included in CNVD from 2013 to 2017

3.5 Intrusion detection and network monitoring technology

With the development of prevention technology, intrusion detection technology has emerged. The role of this technology is to clarify the presence of abuse and intrusion in computer systems and monitoring networks through the development of detection. In the application process of intrusion detection technology, there are two commonly used analysis methods. One is statistical analysis method, and the theoretical basis is statistics. After judging the action, check whether a certain movement is normal or not. The other method is the signature analysis, which takes the behavior of the existing vulnerability of the attack system as the object to monitor.

4. Conclusion

In general, the development of computer network information makes computer technology widely used. In order to better guarantee the security of computer network information, it is necessary to analyze the causes of network security problems, and analyze on this basis, also put forward solutions, so as to guarantee the security of computer network information.

References

[1] Wang Lei, A research on security of computer network information and protection strategies [J] Computer knowledge and technology, 2014, 1019:4 ~ 416.

[2] Wu Si, Exploration of the security of computer network information and protection strategies [J] Information and computers (theoretical edition), 2015, (19): 184 - 185.

[3] Pang Yao, A research on security of computer network information and protection strategies [J] Communications world, 2017, (7) 83

[4] Yu Dekuai, Computer network information management strategy research [J] Computer fan, 2017, (9): 181, 61

[5] Wu Yifan Qin Zhigang, Research on security of computer network information and protection strategies [J]. Science and technology communication, 2016, 802: 156 ~ 157.