

# Discussion on the Protection and Problem of Computer Network Security

Biao Wan

School of Computer Technology and Software Engineering, Wuhan Polytechnic, Wuhan Hubei, 430070, China

**Keywords:** Computer Network, Security, Protecting Methods

**Abstract.** With the advent of the Internet era, people's life has changed a lot. In this change, on the one hand, the Internet has brought a lot of benefits; on the other hand, it also brings a lot of troubles. In order to reduce the unnecessary loss in the process of using computer networks, many network technology experts provide a lot of good advice to the users. Here, this paper analyzes the current situation of computer network security problems, and discusses some methods of protecting computer security.

## Introduction

With the development of the world economy, science and technology update quickly, people's production, are becoming symbiotic with our computer tools. Many important things people need to deal with through the network. However, the vulnerability of computer networks, often causes great harm to people, so it is necessary to explore and solve the problem of computer network security.

## The current situation of the computer network security

### The detector on the scanner.

In the process of current computer network applications, most computers have a scanner tool, which can detect all kinds of file data stored in this computer. From this point of view, the computer installation of the scanner is necessary, because it can greatly reduce the amount of people looking for the relevant documents, save working hours. But the problem is that when the scanner scans a variety of data inside the computer, it is often found in the computer system. In this case, the detector in the scanner is likely to transmit the information of the computer through the computer's network port<sup>[1]</sup>, to the monitoring network information. Because of this at the way information is hidden, it is difficult to be aware of the computer security system, its great harmfulness.

### The implementation of attack through the transport protocol.

In computer network security, the more common is that the attacker attacks the computer in the way of transmission protocol, steal various of data information. Specifically, the attacker sends a link to the user to cause the user's curiosity. In this case, some users due to the vigilance is not high, the relevant link address of the hasty click. The results, the attacker through the link address to the user to transmit a variety of protocols, the user simply can not use the computer, and even the user's computer system immediately paralyzed. Although this process is very short, but once this is the case, it shows that all the information inside the computer has been stolen.

Not only that, some of the attackers without the user to click on the link address, it is able to carry out attacks on computer networks. This is because they use the TCP/IP protocol in the computer vulnerabilities, so that the huge flow of data packets out of the results, the computer system of high-speed operation, the target system in a variety of resources will be consumed.

### The network security awareness of the computer user is not strong.

Third problems in network security is a part of the computer users do not have the security awareness. In this case, on the one hand, because of the computer users seldom encountered the problem of network security, so as to relax. This idea in the current majority of Internet users are there, however, the fact is also true, we usually use the computer in the process, very little information is stolen, was attacked by hackers, etc.. However, it needs to be explained that, due to the progress of the

network technology, in some cases, the computer's internal information is stolen, the computer can still work properly. That is, in the case of the user is not informed, various data information has been mastered by others. On the other hand, most people think that the information in your computer is not very important, so you don't pay attention to the network security. However, once the user has developed this thinking habit, it is likely to cause adverse consequences. For example, if the enterprise internal staff do not pay attention to the network security, it is easy to disclose some of the secrets of the enterprise, and even threaten the survival of the enterprise.

#### **Strengthen the supervision of computer security.**

The fourth problem in computer network security is that the relevant laws and regulations are not in place. Although Chinese computer penetration rate has been greatly improved in recent years, but the relevant regulatory measures are not corresponding to keep up with. Moreover, China is currently in a period of economic transformation, and the resulting social problems are more prominent<sup>[2]</sup>. The government in the network security supervision, it is not immediately take a relatively perfect regulatory measures. So some criminals drilled regulatory network security loopholes, through various illegal means to steal corporate confidential documents, and even the country's confidential documents, in order to grab huge profits.

According to the relevant department statistics, China's computer network security caused by the loss of as many as 100 million yuan per year. This not only damages the interests of the information owner, but also has a bad effect on the computer network security. Thus, it is necessary to strengthen the construction of laws and regulations on network security,.

#### **System vulnerability.**

The existence of computer system vulnerabilities also causes a significant computer network security risks. This is because, in recent years, the speed of the computer replacement is very fast. In almost a year or so, there will be a new version of the computer products. In this case, the majority of people can not immediately change the corresponding computer software and hardware. That is, compared with the more advanced computer version, the previous computer system will appear or big or small vulnerabilities, which gives the attacker left the material conditions of the computer.

More serious is that this system vulnerabilities are often the first choice for a number of network hackers. Because of the cost of the computer through the system vulnerabilities and attacks are relatively low, the probability of a successful attack. Therefore, network hackers often through computer viruses, network intrusion, etc., to violate the user's computer. Moreover, according to the relevant departments of the investigation, the security of the information leakage caused by the system vulnerabilities is more common, and the computer's damage is very large.

### **The protective measures of computer network security**

#### **Use computer's firewall.**

In order to prevent and control the relevant information in the computer, the computer can be transmitted through the scanning detector and the computer can use the firewall technology. Under the control of the firewall, the computer system is in a safe state, so the operator can protect the security of the computer by setting up the network communication, network state and monitoring state. Because of the technical control of the firewall, it can filter the data of some suspicious network, filter, and ensure that the computer network is in normal condition. In particular, when the host needs and outside the network for information transmission and exchange, it will remind computer users should pay attention to the safety of website information and not. However, in some cases, the use of the computer can not have to set up a firewall to reduce the computer's operating burden, improve work efficiency. It should be explained that, under the protection of the firewall technology, the use of the computer can also take some other security policy, to prevent the failure of the technology, the information is stolen.

#### **The encryption skills of Transmitted channel and security testing.**

In order to solve the problem that the transmission protocol is attacked, it can encrypt the transmission channel. That is, when the user receives certain link address, must pass through the detection of security measures. In this process, the system will automatically prompt or automatically

if the detected link is not safe. This ensures the security of the computer network to a large extent. But only this is not enough, in some cases, in some cases, the attacker does not send the link under the premise, but also on the computer network implementation attack. So in order to prevent this situation, the user in encryption process at the same time of transmission channels should be set some safety measures, the computer network were all-weather, 360 degree of monitoring, to ensure the safe of the computer network.

In addition, the need to pay attention is that the attack through the transmission protocol, the network is generally caused by hackers. This is much more serious than the simple theft of computer internal information, because the computer after being attacked often to replace the system, and even change the hardware equipment. Therefore, in order to prevent the occurrence of such a serious problem, but also to respond to computer security testing. This security testing is generally called fuzzy testing [3], which is based on the white box testing, but the test method is more scientific than white box testing. After the security test, the computer software has been very good protection, but also can be a variety of bug highlights, to inform the user may be attacked by the path, so that the user can do a good job in advance of various preventive work.

#### **Improve your network security awareness.**

From the previous discussion, we can know that it is necessary for everyone to strengthen the network security awareness. Under a high network security awareness, the information leakage caused by the human will be greatly reduced. For the problem how to improve the network security awareness, you can start from the following aspects. First, the education apartment increases the awareness of teaching content of network security. Because most of the computer basic knowledge, are in the school period, and, this concentration, the system of education can also strengthen the students' awareness of network security. Generally speaking, the more time people have access to certain knowledge, the better it will be for this knowledge. Therefore, in the current network popularization of the times, so that people in the school period to develop the awareness of network security is particularly important. Second, the government departments can carry out network security theme publicity and education activities. Through the power of the government, to cause people to pay attention to the network security. Subject education content, should focus on the expression of a good network security awareness of the benefits; at the same time, also can give some classic examples, in order to cause everyone's attention and concern.

In some cases, the enterprise can also carry out network security awareness education activities, training and improve the safety awareness of employees. This is mainly based on the size of the enterprise and the nature of the enterprise, to decide whether to carry out this activity. Like some high-tech enterprises, it is necessary to carry out this activity; and the general business of the company, you can decide whether to carry out the activities according to the economic situation of the enterprise. However, from the long-term development of the enterprise point of view, large enterprises to carry out such publicity activities are still very necessary.

#### **Strengthen the supervision of computer security.**

On the current situation, the so-called strengthening network supervision, in fact, is to improve our country's computer network supervision of laws and regulations. Generally speaking, the construction of laws and regulations should be in the front, because the computer application in foreign countries is earlier than our country, and our country can learn from the experience of developed countries. However, on the one hand, our country is in the stage of deepening reform, the focus of government departments is the economic field, and the problem of computer network, not too much time to deal with. On the other hand, in recent years, the development of computer networks is very fast, some of the loopholes in the legal system has not been found before. Therefore, the government departments in the relevant laws and regulations construction, there is still a lot of room for improvement [4].

However, the government should attach importance to this, first have to increase the punishment, especially for those who steal State secrets of criminals, should be given criminal punishment. At the same time, the government departments should carry out network security cooperation with the developed countries, to prevent foreign personnel to destroy the network security of our country.

### **Pay attention to the security of the account.**

Faced with the problem of system vulnerabilities, users should take comprehensive preventive measures. Because the computer's replacement is inevitable, so, no matter which one of the computer users, it is possible to become the target the network hacker may attack. However, we know that the focus of network prevention should ensure the security of the user's account, that is, to ensure that the user's property is not lost. Because of the loss of the user, in the final analysis is the economic loss, so the user should pay attention to protect the safety of the account.

When the users use a variety of network accounts, should try not to save the password, while the regular update of the important account password, reduce the probability of being hacked. In setting the password of the account, should try to avoid using a pure digital form of a password, while the use of long and complex passwords, thereby reducing the possibility of the password is cracked.

Not only that, users can also download the system to patch the way, to plug the system vulnerabilities<sup>[5]</sup>. And, in some places, it has also made a significant effect. Therefore, users should also pay attention to the timely update of system patches, to ensure that the account is in a state of twenty-four hours of protection. In order to be able to effectively protect the computer network is not violated, the above five measures should be used in combination, so that the five points of network security measures constitute an organic whole.

### **Conclusion**

In this paper, the current situation of computer network security is analyzed, and the five main problems are pointed out: first, the scanner on the detector; second, the implementation of attack through the transport protocol; third, network security awareness of the computer user is not strong; fourth, computer security regulations are not in place; fifth, system vulnerabilities. Aiming at these problems, the author puts forward the corresponding solutions, they are: first, the use of computer firewall; second, the encrypting skills of transmission channel and security testing; third, improve the network security awareness; fourth, strengthen the supervision of computer security; fifth, pay attention to the security of the account. Hope that these computer security protection measures, can provide useful help for the computer user's practical application.

### **References**

- [1] Zheng Yujin. Analysis on the protection measures and problems existing in the security of computer network. *Information System Engineering*, 2014,(3):80.
- [2] Lu Lian. The protection measures and problems existing in the security of college computer network. *Value Engineering*,2014,(29):211-212,213.
- [3] Lin Risheng. The protection measures and problems existing in the security of computer network. *Electronic Testing*,2015,(10):68-70.
- [4] Shao Yanzhen. The protection measures and problems of the security of computer network. *Network Security Technology and Application*,2014, (5):111,113.
- [5] Tao Hong. Analysis on the problems of the security of computer network and protection measures. *Industrial and Science Tribune*,2013,12(14): 97-98.