Information Security and Future Trend Analysis Based on Computer Network Environment

Haoyuan Jin
School of Automation, North China Electric Power University, Baoding 071003, China;
1031868763@qq.com

Keywords: computer network; virus; network hacker; firewall; intrusion detection; intelligent.

Abstract. Based on the personal information security, this paper introduces some major security risks, precautionary measures and coping methods in computer networks, as well as the forecast of the future trend of computer network security. At the end, it also introduces the original intention of writing this article and the author's own opinion. At the same time, "the user's personal information is facing the leak" this issue gives its own answer. The article focuses on resolving the network security problems in the minds of computer network users. By mastering some precautionary measures and coping methods, the network is relatively safe. And by enhancing the user's own safety awareness, more effectively reduce the possibility of information leakage. The research contents of this article will help users to enjoy the convenience brought by network technology with more confidence.

1. Introduction

With the increasing impact of computer networks on people's work and life, computer network security is increasingly becoming a topic that people pay close attention to. What security risks exist in the networks we use? Is the user's personal information exposed? How to solve these potential safety problems? These have become urgent problems to be solved.

However, in order to solve these problems, we first need to learn the dangers hide in the computer network.

2. Some of the major security risks in computer networks

2.1 Computer virus invasion.

With the increasing openness of the network, there is more opportunity for computer viruses to "take advantage of" and "lurk" [1]. The computer virus itself is a computer program that can spread as the data flows. After entering the program It will show its destructive.

2.2 Network hacker attacks.

The definition of Internet hackers are mostly accompanied by superb programming techniques. Network hackers exploit the loopholes in the computer network to invade the user's computer network system, destroying or stealing the required information, which poses a serious hazard to the user's personal information security [2].

2.3 Internet fraud.

Some criminals use the virtual nature of the web to disguise themselves and use some chat software or trading platforms to make emotional and money frauds on the elderly, children and singles, or even extort and endanger the personal safety of users.

2.4 Network monitoring mechanism is not perfect.

There are no clear precautionary measures or penalties for some potential dangers on the Internet, which often results in network administrators not taking serious care of their work and leaving many phenomena behind [3]. For example, the vast majority of online games that indicate adults can play are mostly primary school children.

2.5 Users lack safety awareness.

This is the most important and most horrible factor. Users can't able to use anti-virus software or do not attach importance to security, making some preventive measures did not play its due effect, gave the above situation opportunities to destroy.

In fact, the only real counterattack to the malicious attack on cyber-security is the fact that the users themselves really pay attention to the issue of cyber-security and put it into actual action.

3. Significance

The problem of network security has become the focus of people's attention. The study of network security technology not only represents the development of computer technology in a country, but also represents the state's emphasis on people's information security. The more relevant laws and regulations are made, and the fewer maliciously caused network security incidents will be. At the same time, the attitude of the state also reflects the attitudes of network administrators from the side. The clearer and tougher the attitude of the state, the more thorough the law enforcement of network supervisors will be. At the same time, in terms of national security, in order to safeguard national security, network security technology is also an urgent matter.

As a college student, such a group that is most receptive to the most extensive information reception, we even more urgently want to know if some of our personal information, browsing history and even some chatting records are really being stolen by people who have the malicious psychology. In the meantime, the information scam and kidnapping extortion fraud information is "surprisingly consistent" with user information, which makes people feel concerned about personal privacy. Therefore, we say that the development of network security technology is urgent.

So, in this context, we need to learn some precautions to avoid information leakage.

4. Preventive measures and coping methods

4.1 Firewall technology.

The firewall is equivalent to a layer of barrier between the user's computer side and the connected network, which can monitor the data packets in the network transmission in real time [4]. Once problems are found, it will immediately stop the data from entering the computer system, making the virus inaccessible, blocking it and limiting the interaction between the computer and the network, which can play a good preventive effect.

4.2 Using the anti-virus software.

Most anti-virus software on the market now includes anti-virus and firewall in two parts, for example, we are well-known 360 security guards, Kingsoft AntiVirus, etc., the purpose of using anti-virus software is to cooperate with the firewall to detect the hazard information. At the same time anti-virus software library in the process of continuous update, it can effectively kill some known types of virus, the newer versions of anti-virus software, killing the virus will also be stronger.

4.3 Intrusion detection technology.

Intrusion detection technology can detect the computer system intrusion or intrusion attempt, which can detect and control the network all kinds of access [3], in the event of suspicious behavior or may cause security risk factors, it will cut off the signal, And make some safety early warning. Intrusion detection techniques include statistical analysis and signature analysis. In recent years, intrusion detection technology has been more widely used with the development of computer networks.

4.4 Focus on "management".

As the saying goes， "one-third of the network security depends on technology and the rest on management". The guarantee of network security focuses on management, and management on the other hand has two levels. At the national level, only establishing and perfecting the management system and cracking down on those criminals who endanger cyber security while strictly enforcing the law can deter more misconduct people. From the level of related supervisors, only by strengthening the training of related technical personnel and assuming their own responsibilities can such illegal activities be effectively stopped.

5. The future trend

5.1 From passive to active.

Analysis of the current network security technology, mainly passive defense, when a malicious attack occurs we will go defense, and the future of network security technology will change from a passive network security defense to active cyber security defense [5]. At the same time, it will also strengthen the development of network security supervision and network risk assessment system, and take the initiative to detect and eliminate hidden dangers. To protect users enjoy a safe and healthy Internet environment.

5.2 More intelligent and automated.

With the rapid development of Internet business, intelligent network supervision and network optimization means will inevitably replace manual supervision and manual optimization [6]. Network security is undoubtedly a problem that runs through the network development. The upgrading and development of network technology inevitably accompany the development of network security technology towards a more advanced and intelligent direction.

5.3 Develop more advanced systems.

For network hackers and most computer viruses, their attacks are based on vulnerabilities in computer systems [7]. So at this point, only by continually using stronger encoding techniques to patch vulnerabilities or to develop more advanced systems can better solve this problem.

5.4 Strengthen international cooperation.

A large part of cyber criminals use the Internet to commit crimes across the country. Due to geographical barriers and other reasons, these cyber criminals are at large. Therefore, only by strengthening international cooperation and forming an agreement on jointly cracking down on cybercriminals and jointly cracking down on cybercrime among nations can we effectively curb this phenomenon [8].

6. My own opinion

In fact, computer network security problems have always existed in our side, but never before written articles so detailed understanding of it. Through the study of some preventive measures can know, in fact, the information in our computer is relatively safe, after all, hackers will not attack everyone's computer for no reason.

On the basis of possessing certain cyber security capabilities, what really causes us to lose information are some network behaviors and software usage habits, such as having no security awareness to register their own information on various websites or browsing the unhealthy website incurs viruses in the computer. At the same time, some software becomes more terrible when smarter. For example, applications such as *Baidu*, *Taobao* and *QQ* will analyze your preferences based on your browsing habits, shopping habits and chat history. Many online products that serve our lives will also be more thorough analysis of us.

A lot of people may say I have no other way to deal with the latter, but what I want to say is that we first assume that these companies will follow the agreement to protect user privacy, then you? What can you do for yourself? For example, do not be tempted by some advertisements on the webpage to browse through the spam messages, for example, be vigilant at all times and not fill in your personal information everywhere. For example, regulate their own behavior to establish a healthy network concept and don't browse the bad information actively, each of these can make us avoid virus attacks and information disclosure.

In the process of simultaneous development of network security technologies, we also need to raise the awareness of network security. Only when we assume responsibility will the network environment become safe and pure.

7. Summary

There is no doubt that the Internet has become an integral part of our lives. As people in the Internet age, learning to protect our own information security has gradually become the ability we have to learn. Only when we grow together with the network security technology, improve safety awareness and master the ability to prevent, can we enjoy the convenience brought by the network better.

References

[1]. Dongfang Wang, Jie Ju. Research on Computer Network Information Security and Protection Strategy in Big Data Age [J]. Wireless Internet technology. (2015) No. 24, p. 40-41

[2]. Wusimanjiang Yihebaguli. Analysis of the main hidden dangers of computer network security and management methods [J]. Electronic test. (2016) No. 09, p. 69-70

[3]. Shang Wu. The Development and Trend Analysis of Computer Network Security in China [J]. Electronic Technology and Software Engineering. (2015) No. 24, p. 196-197

[4]. Dongyang Jiang. Research on the Trend of Computer Network Security Technology [J]. Technology economy market. (2017) No. 04, p. 39-40

[5]. Zehan Wen. Discussion on Computer Network Security Technology and Its Development Trend [J]. Heilongjiang science and technology information. (2015) No. 26, p. 178

[6]. Zhu Ming. The Current Situation and Development Trend of Network Security Technology [J]. Network Security Technology and Application. (2015) No. 02, p. 156-157

[7]. Zhenghao Wang. Future development trend of computer network information security [J/OL]. Electronic Technology and Software Engineering. (2017) No. 24, p. 214

[8]. Shuai Li. Analysis of Computer Network Security Protection and Development Trend [J]. Silicon Valley. (2012) No. 07, p. 21+161