Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 166 (2020) 438–442

Procedia Computer Science

www.elsevier.com/locate/procedia

3rd International Conference on Mechatronics and Intelligent Robotics (ICMIR-2019)

Computer Network Security and Preventive Measures in the Age of Big Data

Min Xiao[1] and Mei Guo*[1]

[1] *College of software and Communication Engineering, Xiangnan University, Chenzhou, hunan 423000, China*

Abstract.

Compared with the past, life is much more convenient now. Among them, computers have made great contributions to the convenience of people's lives. As contemporary aspiring youth, while enjoying convenience, we should also see clearly the potential dangers behind the big data era. In our daily life, we may not know much about the potential dangers of computers. This is because we use computers in a relatively small area at this time, such as a family, company or campus, and so on. If we use computers on a large scale, there is a good chance that a series of problems will break out. Therefore, the author will sum up the forms and factors threatening computer security in this paper. After understanding the factors threatening computer security, the author puts forward his own suggestions on improving computer security precautions and makes his own contribution to the unlimited development of computer in the future.

© 2020 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)
Peer-review under responsibility of the scientific committee of the 3rd International Conference on Mechatronics and Intelligent Robotics, ICMIR-2019.

Keywords: big data era, computer, network security, preventive measures.

1. Introduction

(1).Overview of Computer Network Environment Security

The convenience of computers for our daily life is the simplest, because its real function is not here. For example, automation, aerospace, medicine and health, scientific research, criminal investigation and so on, computers are playing an irreplaceable role. There is a lot of information in these industries is very secret, because these information can not be understood by irrelevant people, otherwise it will cause irreparable losses. It is precisely because of the high secret nature of computer information that some criminals have the idea of committing crimes

[1] Corresponding Author. Tel.+(86) 18075531998
*E-mail :jasmine_mm@163.com

1877-0509 © 2020 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)
Peer-review under responsibility of the scientific committee of the 3rd International Conference on Mechatronics and Intelligent Robotics, ICMIR-2019.
10.1016/j.procs.2020.02.068

and always hope to obtain some benefits from the channel of computer network security. Computing network security technology is developing continuously, and the criminal technology of these criminals is also developing continuously. Even some criminal technology is higher than the level of our computer experts, so that our network security can not be guaranteed. Because the evidence in the process of computer crime is difficult to grasp, computer network security crimes are becoming more and more frequent. For us, the most important thing we need to do is to do a good job of computer network security precautions, to minimize the possibility of crime.

(2).Composition of Computer Network Security

Computer network security is not made up of a single aspect, but contains four essential links: software, networking hardware, Internet of Things services and shared resources.According to the definition of computer network security by the International Organization for Standardization, computer network security refers to the protection of hardware, software and data resources in computer systems from being destroyed, altered or leaked for accidental or malicious reasons, so that computer systems continue to operate reliably and normally, and computer services are also orderly. For a system, the physical equipment such as hardware circuit should be used as the carrier first, then the functional program on the carrier can be run. By using network devices such as routers, hubs, switches and wires, users can build the communication networks they need. For small-scale wireless local area networks, people can use these devices to build the communication networks they need. The simplest way to protect them is to set corresponding instructions on wireless routers to prevent illegal users from intruding[1].As a kind of communication protocol protection, WPA2 encryption protocol is widely used to achieve protocol encryption. Users can access routers only by using keys. Usually, drivers can be regarded as part of the operating system. After registering with the registry, the corresponding network communication driver interface can be invoked by the communication application program.

2. Forms of Threatening Computer Network Security

From the above definition of computer network security, we can see that computer network security involves four different links, and the above emphasizes the irreplaceability of these four links. Therefore, in the following sections, there are potential relations with the four major aspects when describing the forms of threats to computer network security. There are four main forms of threats to computer network security: abuse of Internet of Things information, denial of service background attacks, damage to the integrity of computer network environment, and leakage of computer information.

(1).Misuse of Internet of Things Information

Usually, in the process of using the computer, many users are more casual about clicking on the website and downloading pictures, files and so on, and will not be used after screening. This has caused great hidden dangers to our computer network security, because every website, file, link and so on may contain viruses or other hidden dangers, if we do not screen, it may lead to our information leakage or computer poisoning.

(2).Attacks on Service Background

The so-called denial-of-service background attack is that the user intentionally delays or illegally delays the network in the process of visiting the website or downloading files as usual, thus causing certain harm to the network security of our computer.

(3).Destroy the integrity of computer network security

Hackers or other people who do not conform to our code of conduct use various illegal means to destroy computer network security, thus affecting the integrity of our computer security.

(4).Leaking Computer Information

When the information in the computer network is transmitted directly to the unauthorized entity without the permission of the user, our information has been leaked. Common forms of leaking computer information include the following aspects: virus or Trojan horse intrusion into computer, user's own system vulnerabilities, radio frequency interception of computer information, installation of monitoring equipment, computer network fishing, etc.

3. Factors Threatening Computer Network Security

There are many factors threatening computer network security, which can be divided into subjective factors and objective factors. In order to describe the factors threatening computer network security more comprehensively, this paper mainly elaborates from six aspects.

(1).Spam and Spyware

In our usual form of communication, mail is a more commonly used way. Especially in all kinds of work occasions, e-mail plays a very important role in our work. For this reason, many criminals want to use email to steal users'privacy or achieve other purposes. They mainly force users to receive spam by inserting it into the normal emails they send in advance. If users do not pay attention to the validity of this email, they may click on or download the specific software they insert, thus losing their information. Figure.1 below is a screenshot of British spyware, which has caused great losses to computer users in the UK.

Figure. 1. Spyware

(2).Hacker Attacks and Threats

Hackers refer to a group of people with high intelligence and ability, who are familiar with computer knowledge and are very good at computer network security[2].Compared with ordinary people, they are simply frightening existence. Hackers can choose destructive attack and non-destructive attack if they want to meet their own needs through the network. Destructive attacks, as the name implies, destroy users'systems so that their computers are completely unusable. Non-destructive attack means that hackers only take the information they need without affecting the normal use of users. Our common hackers use the means of attack: Trojan horse attack, phishing website attack, e-mail attack and so on.

(3).virus implantation

For a long time before, computer users were afraid of viruses. Because viruses can be attached to various types of programs, users will accidentally click on such viruses, and then the virus quickly spread to the entire computer system. Once the user's core system is infected by the virus, it will affect the normal work of the user in a short time, causing inestimable losses to human beings.

(4).Backdoor and Leakage of Computer Software

There is no software in the world that does not leak, so many hackers like to choose software to attack. The so-called "back door" means that programmers leave a door for their families at the beginning of software design, in order to "facilitate" their future operation. Such a backdoor is obviously not because programmers are not competent enough, but because they are too competent to think of such unreasonable means. In a word, such behavior is unreasonable or not recommended.

(5).Direct Attack System

With the development of science and technology, some people who are familiar with computers directly attack other people's computer systems through their own computer networks. This type of crime is emerging with the development of computer field. These direct attacks on the human system are more sophisticated, leaving few traces that can be queried [3]. They steal their privacy, destroy the real information and cause great trouble to others. Because of the unrestricted nature of computer networks, these criminals are becoming more and more rampant and terrible. They devote little time and energy, but they can get great rewards, so their desire is becoming stronger and stronger.

(6).Natural Disasters

No matter how intelligent a computer is, it is only a machine, which is always inferior to human beings. Therefore, there is another external factor that will have a great impact on the security of computers, that is, natural disasters. Natural disasters here mainly refer to uncontrollable causes such as changes in humidity, temperature, earthquakes or tsunamis, sudden power outages or computer water intake accidents. These natural causes are beyond our control and can not be completely avoided. Therefore, if we want to improve the security of computer network, we should start from other aspects.

4. Preventive Measures of Computer Network Security

(1). Virus Defense Technology

Virus defense technology is an important precautionary measure for computer network security at present. The power of virus has also been mentioned above. The damage caused by the virus to humans is simply incalculable. Some viruses can be isolated from our computers through our effective defense, but some of the more severe viruses can not be completely eliminated through several protective nets. Computer technology is constantly updated and developed, but hackers and outlaws are also constantly learning, so we must not stop studying computer network security technology. Our protective technology must be faster than the speed at which they study viruses, otherwise our computer network security will not be guaranteed.

(2). Data Encryption Technology

As mentioned earlier, information leakage is one of the most frequently mentioned problems in computer network security. We can use data encryption technology, so that users'information is not so easy to steal. Data encryption technology refers to the use of special data processing technology to hide or specialize data, through which other users may not understand the information. Data encryption can be divided into two forms: public key encryption and private key encryption. Public-key encryption is more secure than private-key encryption, and it develops relatively late. Private key encryption can be divided into two processes: encryption and decryption. The encryption and decryption process correspond to each other, which has a certain protective effect on the security of information. Private key encryption is not restricted by users, anyone can set up and use it. In terms of decryption speed, private key encryption is faster than public key encryption and easier to implement in life. Comparing the characteristics of public key cryptography and private key cryptography, we find that they have their own merits. Personally, if public-key encryption and private-key encryption are used together, the effect of data encryption should be higher. I hope this idea can be realized as soon as possible.

(3).Access Control

The most important feature of access control is to verify the identity of the users who access computer resources. It requires auditing, authorization verification, password, key and other authentication methods to protect user information and computer security. Simply put, the core idea of access control funds is that information is only open to those who really need it, and that users who enter illegally are intercepted. Access control is an important means to protect computer network security. It has great research value. It has a good effect on hacker intrusion. It is hoped that there will be significant development in the future.

(4). Firewall Technology

Firewall, on the surface, is a security barrier to protect computer security and prevent computer failure. It is also the most common type of computer security measures used by ordinary people. Firewalls can be hardware, software, or between two or more computers. Firewall can play a more substantive role in protecting computers, because after all, all data streams need to be filtered through the firewall[4].Generally speaking, firewalls have the following functions: first, firewalls can prevent other unrelated people from entering the user's own private computer; second, even if someone from outside enters our system, firewalls can prevent him from approaching your defense facilities; third, firewalls can prevent me from visiting special sites; and finally, firewalls can prevent us from visiting special sites. Computers provide security monitoring.

5. Conclusion

Computer network security is a problem that every computer user needs to pay attention to. We must pay attention to the cleaning of phishing websites, illegal links, spam and so on in our life. Don't give the outlaw a chance because of his negligence. In addition, the technological development of computer network security should

keep up with it as soon as possible and suppress the illegal elements technically. There is still a long way to go for the future development of computer network security technology. Technical breakthroughs should be realized as soon as possible, and our security protection measures should be improved.

6. Acknowledgments

This paper is funded by Project of :School level scientific research project of XiangNan Universit，Research on network security situation prediction based on data fusion，(No. 2017XJ16)

7. References

1 Hu Shichang.Analysis of hidden dangers of computer network security and discussion of preventive measures[J].Information and Computer (theoretical edition), 2010, 11 (10): 159-158.

2 Zhang Lin, Huang Xianbo. Brief discussion on computer network security technology [J]. Computer knowledge and technology, 2006:45-46.

3 Wang Tao. Brief analysis of computer network security problems and preventive measures [J]. Scientific and technological innovation and application, 2013 (02): 45.

4 Xu Chaohan. Computer network security and data integrity technology [M]. Beijing: Electronic Industry Press, 2005:11-13.