Computer network information security and Its Countermeasures

Zou Yanli1, a Bu ruiqin1

[1]Faculty of Electrical and Information Engineering, oxbridge college,Kunming university of Science and Technology, yunnan 650106, China

[a]704685@qq.com

Keywords: Computer network; information security; Protection Countermeasures

Abstract. Due to the rapid development of our country, the computer network is becoming more and more rapidly, the security problem of our people on the computer is more and more attention, a series of software and various types of account are required to record on the user's personal information, all accounts and a series of information about user damage or outside leakage, unnecessary trouble and damage to the user. Therefore, the protection measures and computer network information security as the key is a key task for Chinese related industries, how confidential information on the personal information of users and part of the country's secret work is now the main cause to the successful development of computer technology.

Today is the computer network technology has brought us a lot of convenience, but also enhance the quality of our life to a great extent, our lives to provide a lot of convenience and happiness, but also bring us many problems and challenges, these problems especially security issues of personal information is the most important. Almost all of our personal information can be checked out and we visited the site with the computer network technology and the use of the software, if you only have a mobile phone, then you will be personal information through the network by others using a variety of techniques to find out where the mobile phone or computer, but the invasion of our own by virus so, our personal information will be leaked out, is even more exaggerated service terminal of some software you often used by hackers, so our identity information will also be leaked out after the criminals use, this situation has made our property safety severely affected.[1]

The main problems of computer technology

In recent years, the problems that have occurred in this respect have increased gradually, resulting in the destruction of our personal information and confidential information of our country. There are many factors that lead to these problems, there are criminals with professional technology intrusion of computer system, some parts of the system has not been perfect and there are still some problems, the relevant units of other countries to carry out illegal collection of network information. For example, the relevant enterprise through to people, chat, email, language information and historical records, stored information, audio information transmission, call records, photographs and other social software and method of collection and monitoring, eavesdropping on personal information, confidential information to anyone else. American government agencies do not take into account the private information of the masses, and they illegally eavesdrop and spy on others, which have seriously affected the personal information and security of the masses. No matter what they have in their purpose, this approach is very wrong, has given us life caused serious problems, not to mention who can't ensure that the user's personal information eventually in the wrong hands. There are many special hacking government agencies and some of the network system to attack the example, regardless of the network system senior department or lower departments, have been a hacker intrusion, the data not only relates to the people's interests and security, also led to the safety and benefits of affected countries. Therefore, how to do the work of network security in this area is currently one of the key issues of our concern.[2]

Computer network security problems

Security problems in operating systems. Key safety issues in this system is the computer appears in the buffer process, the computer system is particularly easy to let hackers exploit the vulnerability to attack and destruction of the network, the system does not check the user's computer program and its data buffer area is changed, the information transmission network will receive long, will store the extra information to the stack, let the computer system can get the information command. As a result, gives hackers take advantage of the opportunity to convey information. After long instruction than the system requirements, the system was also the most unstable, will give the computer data within a certain threat. After the service is against the loopholes, so would disrupt the computer network TCP connection order, especially the DOS vulnerability, it is most likely to damage all the data in the computer, let the computer system cannot work normally. After we update and improve the system and software, we will always be tested, and if we wish to solve all the problems, it will be a very difficult task for us. For these problems, the loopholes in the buffer zone are highly vulnerable to attacks by criminals. The system and buffer area change can not be timely inspection, just received long conveying information, placed on the stack in multi holes arranged in a stack, each instruction of the system can still run normally, this is the most system program will be used. This will only let the criminals have more chances for the intrusion, as long as the delivery instruction than the buffer area required, system work happens unstable, if the attacker set some numbers and symbols to invade the system. In this case, you can view the root directory of the system.[3]

Irrational uses of legal instruments. Most systems have backups, which are tools for future updates and changes to the system. However, this also provides a posterior approach to the system, for example, the NBTSTAT instruction, originally in order to make the relevant staff query system and applications of the remote data, but hackers can use it to do some illegal things, use it to set the break using layers of protection etc.. It was originally a tool for enterprises to improve and update the system, but some unscrupulous people used it for their own purposes. So that the network in all aspects there will be security issues, unreasonable repair and the traditional design method of the system, and the system does not have higher detection ability, can let the criminals take over. The computer system is in accordance with the requirements of various users to arrange some software tools on it, this tool is generally the management of the system to improve and update the relevant staff and not the tools to master, as a result, it is very easy to be illegal use, then do some harm to individuals and countries things. So we must think of some countermeasures to stop this happening.

Irrational system protection countermeasures. If there are some loopholes in the operating system, it is very easy to intrusion by hackers, the staff did not manage and operate the computer in accordance with the regulations, but also to the security of the computer system has a certain impact, the emergence of new vulnerabilities when you need to staff for further research according to the actual situation, the corresponding problem use the corresponding measures, the system maintenance and use the correct method, and constantly improve the system operating software, often clean and antivirus software in the computer, and take some protective measures to protect the security of the computer, so that you can find the computer vulnerabilities in the first time, and will handle these vulnerabilities fall, avoid network information will cause unnecessary losses. In addition to the computer vulnerabilities and too much damage tools, there are other reasons for the security problems of network information, which is not managed properly. When a staff member looks for new problems, they should first make a study of the risks and where they are performed, and adopt remedial measures in a timely manner. Although we often repair the system, but also regularly to improve and update the software, but for various reasons, there will be additional security problems, so we should pay attention to system repair.[4]

The impact of natural disasters. Computer operating system is a system at all levels. The natural environment is very easy to bring a serious threat to the computer network. For example, earthquakes, weather, climate and other factors can cause network security to be affected. In addition, when people use computers in our country, they can hardly use a series of systems such as anti radiation interference, nor have they adopted some countermeasures for the emergence of ecological disasters. If computers are destroyed by natural catastrophes, the harm that we do will be very great. The structure of a computer is almost composed of some electronic equipment. It is very sensitive to the external environment, so it is easily affected by natural disasters. Look at the current computer room, not for those securities risks taking relevant countermeasures. Usually in the use of computers, often because of power failure, resulting in our collation of information or critical data is not saved, the phenomenon of loss.

Computer network information security protection strategy

Strengthen people's sense of safety protection. We are using the time of network information, will use a variety of accounts, but the criminals invade our computer is to get our account password, once the criminals invade our computer, then I will bring harm to us. In this case, we need computer users to encrypt and set some of the more complex passwords on their computer, in addition, in the process of the password, the password must be set about, we set the password for the security should be the letters and numbers and special symbols together, especially to change a password in a certain period of time, which helps to protect personal information security account. Some criminals will use to send mail, fake a legitimate company to the customer to take some mail, email reply to the customer at the time the slightest mistake will be their account and password to disclose to the criminals, bring unnecessary losses to our own, and the loss is very serious. Therefore, if you receive this kind of mail, you must not trust it and clear it up or call the corresponding customer service to confirm it so as not to cause property damage to you.[5]

Install firewalls and antivirus software. This technology is a special Internet facilities, the most critical applications of this technology are to control network access between criminals, in addition, it also helps to prevent outside intrusion of computer system, and finally the protection of the computer department of operating procedures. For our computer installation technology, when it is installed, we often configure it to an antivirus software. We present the most widely used security technology is anti-virus software, this technology not only can find the presence of the virus and the virus cleared up, but also to prevent the invasion of Trojan implanted and criminals, we should pay attention to is, in the use of the software, must be the first time it updates only to enter its update to cannot update the level that can prevent the virus. When we visit some website or download something, it is easy to criminals a virus also downloaded to our computer, this time, if our computer with antivirus software, it will remind us not to download a virus.

Strengthen the management and maintenance of computer network system. A computer network environment is a kind of environment that users use when they use a computer. Users are very concerned about their security when they are using the Internet. The user in the process of utilizing the computer must own the network environment carefully verify and check if there are security risks, so we must carefully consider whether to use, only in this way can we prevent the computer were criminals or natural disasters. There is a user must often on their own computer security check protection software must often change the security, often give their computer antivirus treatment, so you can avoid important information leakage or loss.

Document security and digital signature technology. If you want the security of the computer network information to be truly improved, in the actual solution of personal information will be leaked problems. Do not forget to use encryption and digital signature technology for files. According to different functions, we divide the text, encryption and digital signature techniques into the following categories: first, the transmission of information. It is used to encrypt the information in the process of transmission, and then divide it into two categories: link encryption and encryption at both ends, followed by the preservation of information. To keep the information kept secret. Its most important purpose is to prevent the loss of information during the preservation process, and finally to ensure the integrity of the information. It serves to test the transfer, storage, and extraction and processing of incoming data, which ensures that the information is not compromised during the transmission. Digital signature technology is a kind of potential safety problems are often used in our country at present a network communication in the process of elimination, in the use of this technology in the process, it can check and confirm the electronic document and can achieve the best effect of its information integrity protection, is essential. There are numerous ways of using this technology. The environment can meet the requirements for the use of a computer is very important, some companies in the use of the computer, the computer can be in line with the instructions to adjust its temperature and humidity, achieve the best use of the state. In addition, in the face of natural disasters, on their own internal computers can encrypt the data information, there is a computer when a sudden power outage can save the file, so as to avoid the phenomenon of information loss, thus protecting important information is not our loss is very favorable to us.

Concluding remarks

Because our country's level of economic development is relatively fast, our life has become increasingly dependent on network technology, but in between there are many security risks, how to solve these security risks is one of the things we value most now. Almost all of the computer network data is public, and when we use computers, there are always some security risks. Even now there are a variety of anti-virus software and protection of data network software, but only the general protection technology for network security protection is not common, can eradicate the problem of network security. Therefore, the study of computer network security risks and the exploration of its measures is very critical, and it plays an important role in the development of computer in our country.

References

[1]Hamdi M, Boudriga N. Computer and network security risk management: theory, challenges, and countermeasures[J]. International Journal of Communication Systems, 2005, 18(8):763－793.

[2]Sklavos N, Souras P. Economic Models & Approaches in Information Security for Computer Networks[J]. International Journal of Network Security, 2006, 2(1):14-20.

[3]Talooki V N, Bassoli R, Lucani D E, et al. Security concerns and countermeasures in network coding based communication systems: A survey[J]. Computer Networks, 2015, 83:422-445.

[4]Luo Y. Study on the Current Situation of Information Security and Countermeasures in China[J]. Energy Procedia, 2011, 5(5):392-396.

[5]Li Y, Zhou L, Zhu H, et al. Privacy-Preserving Location Proof for Securing Large-Scale Database-Driven Cognitive Radio Networks[J]. IEEE Internet of Things Journal, 2016, 3(4):563-571.