ATLANTIS PRESS

Advances in Computer Science Research, volume 75

7th International Conference on Mechatronics, Computer and Education Informationization (MCEI 2017)

Analysis of Computer Network Security Problems and Preventive Measures

Ying Peng

Department of economics and management, Dehong normal college,

Dehong,Yunnan, 678400,china

892011298@qq.com

Keyword: Computer; Network Technology; Security; Measures

Abstract. With the rapid development of social economy and the continuous improvement of computer science and technology, the Internet era has arrived. Modern people can feel the existence of computer networks in all fields of life, people's lives, work, learning has been inseparable from the computer network technology, it brings high efficiency and convenience. But everything has two sides, computer network technology is no exception, itself also has technical loopholes, security issues have been emphasized. This paper focuses on the security problem of computer networks is discussed, the analysis of the present situation of network security problems, and puts forward some corresponding preventive measures to solve these problems, in the hope of China's network security problems can be solved.

The advent of the Internet era means that human society has entered a more efficient and convenient world. The channels for people to obtain information have become rich, and the time of transaction has been greatly shortened, which has continuously promoted the economic development of the city. However, at the same time bring about the development, but also for people's lives and work has brought security problems. In the continuous development and progress of science and technology hackers and computer viruses such as technology or technology is also in constant development, these are gaining people's transaction information, company secrets, personal privacy by criminals, seriously affected the normal order of the network, even causing heavy economic losses to the people. Therefore, we must strengthen the maintenance of network security, crack down on the destruction of network security behavior.

Network security from the security strategy and technology diversification, if technology and the introduction of a unified strategy is not safe; network security mechanisms and technologies must constantly change; with the extension of the network in all areas of society, access to the network means more and more, therefore, the network security technology is a very complex system engineering. Security and anti security are like two contradictions, and they are always climbing up and down, so the security industry will continue to grow with the development of new technology.

Network information security is an important problem faced by the national development, should be planned from the system, from technology, industry, policy to develop it. We should not only see the development of information security is a part of China's high-tech industry, and should see the development of the security industry policy is an important part of information security system, should even see it on China's future development of electronic and information technology will play a very important role.

Computer Network Security Overview

Computer network is a virtual thing, often do not have the actual carrier, which belongs to the abstract concept, usually refers to multiple computers with independent function in different locations and the external devices connected by communication lines, in the network operating system, management and coordination of network management software and network communication protocol, to achieve resource sharing and information transmission of computer system. [1] network security is a comprehensive subject involving computer science, network technology, communication technology, cryptography, information security technology, applied

mathematics, number theory, information theory and other fields. Computer network security refers to the specific meaning of certain technologies and related measures for the protection of the existing in the network data and information, to ensure the normal operation of the computer system, realize the confidentiality and integrity requirements. The international organization for Standardization (ISO) is defined as the network hardware, software and its system of data protection, the reason is not due to accidental or malicious destruction of change, leakage, continuous and reliable system in normal operation, the network service is not interrupted. Computing and network security are theoretically divided into two types, one is physical security, which refers to the fact that the existing computer hardware facilities are intact and not destroyed. The second is logical security, which mainly refers to the protection of the internal information of the abstract system, to ensure that it has not been stolen, has the secret, and can be used in full.

Computer Network Security Problems and Analysis of the Existing Problems

There are many problems in computer network security, which are mainly caused by virus like problems, non-human manipulation problems, hacker attacks caused by their own vulnerabilities, and related system problems. These problems will continue to affect the normal operation of the whole computer network environment in our country. Therefore, we must solve these problems. Mainly related to confidentiality, integrity, availability, feasibility, authenticity, controllability, denial and other attributes of network security issues caused by the nature of the reasons. Next, this paper will analyze these problems one by one, providing a realistic basis for the discussion of computer security measures in the future.

Security Problems Caused by Computer Related Viruses. The computer virus is mainly refers to the virus creator in the existing computer system application can generate destructive effect, can use a program code on the computer or steal inside the computer information system data of the different degree of influence. In practice, the computer viruses are classified, mainly based on the extent of the impact of the actual network to be divided, including dangerous, no danger, no harm of the three categories. But the most common in reality is commonly known as the "hacker", the use of these features into virus and network transmission speed of the computer in the network fast and wide range, the virus is released to the network, thereby undermining people for the normal use of the computer and even steal secret information, this kind of behavior is to be severely punished. Even if the computer is open, but infringe on other people's own rights and interests or public rights is the law can not allow. Now the network even in the presence of a special kind of virus, the virus even daily use anti-virus software can not identify, this is undoubtedly the computing and network, is a very big hidden danger.

Security Problems that Do not Belong to Human Manipulation. As far as the calculation is concerned, it can be divided into two types in essence. One is manipulated by human behavior, and the other is that human beings can't control it. And then, the author will give a brief introduction to the second types. This type also happens frequently in people's daily life. First of all, natural causes. Mainly refers to a kind of when affected by extreme weather, such as wind and thunder, will affect the computer network of the electromagnetic wave normal transmission problem, related equipment may also be because of thunder and damage the computer. Secondly, environmental reasons. Many natural things can affect the transmission of computer networks, such as our mines. Finally, the computer equipment due to long-term use and constantly aging, thereby affecting the security of computer networks. Similar to the introduction of the above is not artificial security problems, can reduce the risk of occurrence, should do everything possible to reduce, after all, once happened, the impact is very serious.

Loopholes in the Computer Itself. Any computer system is the pink of perfection, even if it is currently running well, but with the passage of time and the progress of technology, the future will be a new technique to overcome the system, thus the loopholes in the system. Computer vulnerabilities can be said to be a very common phenomenon, although in daily public opinion does not matter, but for professional hackers, they can use these loopholes to achieve certain purposes. They can get secret information from their computers, destroy other people's computer systems, and

cause losses to others. Computer vulnerability is not caused by human intent, many loopholes are itself. Maybe it's just because users install pirated software that can cause bugs. Vulnerabilities are also divided into many types, big and small, but in any case, they have the same characteristics, that is, it will cause security risks to users, resulting in losses.

The Lack of Corresponding Legal Norms and Internal Use System. The security problem in today's society of computer network almost daily in the occurrence, number is also very alarming, the reason, in addition to its own system or virus invasion, or the lack of corresponding legal regulation. At present, the law of computer specification is not perfect, even if the relevant safety management regulations are introduced, but the legal responsibility is not strict enough, which can not bring warning to offenders. Just imagine, if the value of the illegal gains is higher than the legal liability, the offender will choose which way, definitely the former. In addition to the legal system, the use of computer management system is lack of effective, especially for the group enterprises, employees of the daily office is the use of computer technology, the enterprise to make the standard for internal use of employees, employees are more likely to make illegal use of network technology, the nature, the daily work of the enterprise file with commercial secrets therefore, regulate the use of the lack of staff of computer technology is very serious.

For Computer Security Problems Prevention Measures

Pay Attention to the Use of Antivirus Software. In the process of daily use of the computer, the installation of the corresponding antivirus software or firewall is a relatively simple and efficient means. Because now antivirus software is very much, and basically are free, people can choose the latest real-time antivirus software for their computer set up a basic protective barrier. Now the more popular is 360 antivirus software, the effect can also achieve the ideal degree. Install this type of antivirus software only, it can automatically detect the presence of the virus in the computer system and can be eliminated, even this kind of software for computer system vulnerabilities can be identified. But it is important to note that although the antivirus software easy to use, simple, but need to be updated regularly, because the virus knitter technology in the unceasing progress, so update antivirus software can be achieved on the new virus killing better, so as to protect the safety of computer system.

Network firewall technology is a kind of used to strengthen the network access control, external network users to prevent the illegal means through the external network into the internal network, access to the internal cyber source, special network interconnection equipment to protect the internal network operating environment. It links the packets transmitted between two or more networks according to a certain security policy to determine whether the communication between the networks is allowed and the network running state is monitored.

The current firewall products include bastion host, packet filter router, application layer gateway (proxy server), and circuit layer gateway, shielding host firewall, dual host, and other types. Since 1986 the United States Digital company installed the world's first commercial firewall system on Internet, proposed the concept of a firewall, the firewall technology has been rapid development, at home and abroad have been dozens of companies launched the function of different firewall products. According to the technology adopted by firewall, we can divide it into four basic types: packet filtering, network address translation, NAT, proxy and monitoring.

Constantly Reduce the Impact of other Factors. One of the common uses of computers is to avoid the use of computers in extremely bad weather, because it can cause a fatal blow to computers. In addition, in the process of using, should pay attention to the problem of the loss of computer, computer equipment are too aging should be timely replacement, not only to save the moment of force, and to the computer system's potential dangers. These can be avoided by the small details of the usual use process, computer users should pay attention to these, can not wait for security risks occur when only conscious.

Update the Computer System Regularly and Deal with the Computer Bug. Regular updates of the computer system can effectively find the system vulnerabilities in the computer and solve them. Although it is only a casual download can solve the problem, but it has a vital role in the

security of computer information systems. In reality, by computer vulnerabilities patches, as the name suggests, the patch here is similar to the people's clothes on the same patch, the clothes damaged place to make up to prevent cold access. To make up for loopholes in the computer system, it can avoid malicious programs, viruses and other intrusion, so as to achieve their own security. Often hackers can successfully attack other people's computer, it is to use the loopholes in the computer network system, to make up for loopholes in order to hinder the security threats to their computer system. Now there are a lot of software that can make up for system vulnerabilities on the market, and 360 of the security guards are one of them. It can automatically find vulnerabilities in the system, users only need to click the mouse can quickly achieve repair.

The Application of Encryption Technology. Encryption technology is another effective means to deal with the current network security problems, mostly used in important document files or data. It is based on the open file, set the corresponding password, if there is no correct password, can not open and use the contents of the document. In the prevention process of computer network security encryption technology is adopted to invade the system a hacker or virus is another barrier, and if it is set more complex encryption technology, it will be difficult to be cracked. Encryption technology is like an iron gate, in order to enter, you must have the password key.

Perfecting Relevant Legal System and Strengthening Legal Consciousness. Through the system of computer technology can only protect the safety protection on the one hand, to be solved to improve the relevant legal system fundamentally, especially for that computer system intrusion of others, to steal personal information or destroy others system cause serious harm behavior must be severely punished, strengthen the legal regulation of related behavior the. In addition to improving the legal system, we need to strengthen people's legal awareness in this regard. Only by establishing the correct legal concept can we reduce the occurrence of illegal acts. At the same time, people can pick up the law to protect their rights and interests. When the computer network system of their own destruction, when criminals violated the relevant rights and interests, must use the law, can not let the criminals escape legal sanction, if neglected, unchecked, will only make those criminals more arrogant. Therefore, to improve the legal system and strengthen the legal consciousness of all parties must be carried out at the same time, so as to more comprehensive protection of computer network security, to prevent the occurrence of risk.

The Research Status and Trends of Network Security Technology

The research of China's network security information communication security and data protection has experienced two stages, is entering into the stage of research on network information security, has developed a firewall and security router, security gateway, hacker intrusion detection and vulnerability scanning software etc.. But because of the information network security is a comprehensive and interdisciplinary field, which combines the long-term accumulation of many disciplines by mathematics and physics, biochemical information technology and computer technology and the latest achievements, put forward systematic and complete solution and collaborative information network security solutions, the following five aspects of safety architecture, security protocol, modern cryptography theory, information analysis and monitoring and information security system to carry out research, each part together to form an organic whole.

The international information security research started earlier, intensity, accumulation, wide application, foundation of network security theory research "in the 70s U.S. computer security model (Beu&Lapadula model) based on the specified" trusted computer system safety assessment criteria "(TCSEC), subsequently developed on the network database system and formed a series of safety, safety information system standards. Security protocol is the important content of information security, analysis of the formal method began in the early 80s, there are three kinds of analysis method of state machine, modal logic and algebra based on the tool, but there are still limitations and vulnerabilities, in improving stage of development. As the key technology of information security, cryptography has been unprecedentedly active in recent years, and the academic conferences on cryptography and information security have been held frequently in the United States, Europe and asia. The public key cryptosystem proposed by American scholars in

1976 overcame the difficulty of key management in network information system, and solved the problem of digital signature, which is the focus of current research. But the safety of the electronic commerce is the focus of people's attention, is currently in the stage of research and development, which led to the study of argumentation theory and key management, because the computer speed continues to improve, all kinds of cryptographic algorithms are facing new cryptosystems, new technologies such as quantum cryptography, DNA cryptography and chaos theory. The password is being explored. Therefore, network security technology in twenty-first Century will become a key technology of information network development, twenty-first Century human into the information society, guarantee the important strategic resources of information the social development needs of network security technology, the formation of social development impetus to. In China's information network security technology research and product development is still in its infancy, there are still a lot of work we need to research, development and exploration, to get out of joint research development road Chinese characteristics, catch up with or exceed the level of the developed countries, in order to ensure the safety of China's information network, to promote the rapid development of our national economy.

Concluding remarks

The whole world is in the Internet era, people's lives and work more and more rely on computer network technology, it brings convenience at the same time, also will produce a lot of problems. In recent years, frequent hacking incidents, network privacy leaks incident sounded the alarm to the people, we must pay attention to the computer network security issues. At present, the problems of system vulnerabilities, virus invasion, hacker problems and imperfect relevant legal system need to be solved. People in daily life must strengthen the computer network system maintenance, regular virus killing, vulnerability repair. At the same time, the legislature should also introduce applicable legal norms for related issues. Therefore, we can ensure the security of our computer network, and create a safe and reliable network environment for people.

Reference

[1] Zhang Yue. On the regulation of computer network legislation [D]. Southwest University of Political Science and Law 2014.

[2] Liu Huaping. Analysis of computer network security in China [D]. Chongqing University 2014.

[3] Zheng Shiyan Hu. Study on [J]. social science measures to prevent computer network security risk. 2013 (03).

[4] Zhang Jianming. Analysis of the current situation of computer network security in China [J]. Journal of East China University of Science and Technology (SOCIAL SCIENCES EDITION). 2014 (01)

[5] Liu Xiaoyuan. Computer basic knowledge research [J]. theory exploration. 2013 (01)

[6] computer network security analysis, [J]. network security technology and application. 2014 (01)