Analysis and Discussion on Computer Network Security Issues

Zhengliang Liu[1, a] Xinyu Zheng[2, b]

[1 2] Gannan Medical University, Ganzhou, Jiangxi, China, 341000

[a]email, [b]email

Keywords: Computer Network, Security Issues, Analysis, Discussion

Abstract. With the rapid development of computer network technology in the application of computer networks, the importance of network security issues become increasingly prominent, computer network security is a growing concern of the community. Faced with the problem of computer network security risks exist, and take relevant measures to ensure the security of computer networks is critical, this paper, computer network security as the starting point, based on the analysis of computer network security issues discussed on computer network security precautions measures designed to illustrate the importance of computer network security, to provide a reference for the protection of computer network security.

Introduction

Computer network technology development has already entered a new area of development among the various sectors of society in which access to the most widely used, encourage people to enter a new era of information development. In recent years, computer network technology has greatly improved the way people's daily life and work, and even a direct impact on people's habits, the Internet become indispensable activities. However, despite the computer network it has brought us great convenience, but the corresponding network security issues have begun to follow, and economic losses due to network security problems are caused by the gradual growth. Therefore, we must attach great importance to computer network security, or if their network security problems will inevitably cause the entire computer network cause severe paralysis, or even directly affect people's normal life and work. Therefore, it must be possible to protect the computer network information technology and constantly upgrading its security has become an urgent problem immediately.

The Definition of Computer Network Security

Computer network security refers to information security and security control in two parts. Information security means data network hardware, software and systems are protected from accidental or malicious destruction of reason, continuous and reliable system uptime, information service interruption. Information security is defined as "integrity, availability, confidentiality and authenticity"; control security refers to authentication, non-repudiation, authorization and access control.

The Status of Computer Network Security

Computer network security for people's daily lives more and more important, whether it is online shopping pay, bank transfer or credit card business, can be achieved through the network, people can stay at home to easily handle the affairs of daily life, for young people in the information age and it is simply convenient to the extreme. However, network security issues cannot be ignored, such as intentionally or unintentionally modify or destroy the system, or in an unauthorized manner and cannot monitor the data modify data integrity breaches; using a broad network of computer information systems and anonymity , walking the wrong information to discredit the image and visibility of an object of defamation; and in the network system, to read data transmitted over the Internet, install the monitor communication and reading online information, so that people have to

pay sufficient attention .

Internet access to people living in every corner, a lot of things people need to be done through the network. Because of this, cyber crime has become increasingly common. People use the Internet to steal someone else's information, confidential information to users, and other property, causing serious damage.

For Internet users should strengthen security awareness, all users have their own network protection awareness, but also pay attention to whether the conduct of its own network to others harm consciousness, sometimes casual user behavior will cause a security threat to other users

Internet continues to develop, more and more commercial activities, now there are a lot of viruses with commercial interests, the way the virus Trojans, worms, spyware, etc., resulting in a network of information and data being stolen. The reason why hackers give users data threat because it enables the virus to disguise and hide, making it impossible to check for viruses in general, and anti-virus software.

Analysis of Computer Network Security Problems

External Physical Damage Issues. Due to computer security issues caused by an external physical damage, usually a computer network security field of information among the major basic problems. Under normal circumstances, the computer network itself has physical threats are a direct result directly through floods, earthquakes, landslides and other natural weather disasters. Apart from these main reasons, computer network itself and its equipment will be placed in the environment caused by computer security is very direct and serious implications of this type of damage is particularly electromagnetic interference, fire and water impacts and lightning attacks and so many aspects.

Network Viruses and Malware Problem. Given the importance of computer security information, the state has also introduced a special problem for such a variety of related laws and regulations, and directly against computer viruses made a clear definition. Computer viruses are mainly among computer running the program, the purpose of the system is a kind of computer program and destruction. However, when the corresponding virus infected the computer itself, so its file system among the information will be stolen and copied directly, which directly affect the normal operation of the computer itself. However, due to the destructive computer viruses have very strong, but also has very clear self-replication features. Typically the virus to spread through all forms of network development, and the computer itself once infected with the virus, unless it itself has very powerful anti-virus capabilities and it will be difficult to really clear. There are too many economic losses due to events caused by computer virus infection, which are a direct result of the people's attention.

Vulnerabilities of Computer System Security. Such a system which specifically refers to security vulnerabilities exist in the computer hardware and software problems which, once the corresponding virus itself is a serious virus attack, you will be vulnerable to significant damage, this situation is more and more present behave obvious. Today, the computer operating system used generally contains Vista, Windows XP, Windows7 and 8, etc. These types, these systems sound generation than the generation, but still inevitable there will be some vulnerability in which systems. And computer users in the use of a variety of software, usually due to software defects caused by the problem itself, it is easy to direct attack by hackers and viruses, thus contributing to the safety of the computer itself under serious threat.

The Computer Network Information Security and Technology Classification

The Meaning. Computer network security not only refers to the computer itself, information security, and also includes the computer's internal hardware and software security and the corresponding data privacy security, etc., the most important is the security of network information, should pay attention to protect the information is subject to network viruses and hackers attacks and damage. This form definition is simply the definition of a pure sense. Once they were extended to

the field of science, it will directly be defined as network and information security is closely related to the theory and the corresponding research fields, which contains the information during transmission confidentiality and security, therefore encompasses a wide range of more [2].
The computer network information security system is mainly to be able to protect the data inside the computer, and the leak will not be infringed, thus ensuring the normal operation of the computer system, and ultimately provide a sustainable and stable development services for the development of countermeasures enterprise networks. While most of today's companies are beginning to introduce more advanced nature of the product to help companies build a sound internal network information security systems, but in many aspects of practical products, such as most of the problems are still not solved.

The Classification. Computer network information security has many specific types can be divided into the following categories: First, an important foundation for the physical level of information security, this level of information security a security system, once it lost its own security support physical level, even then the perfect network information will not make any sense. Mainly refers to the computer's internal components very complete, like on switches, servers and data storage hardware required class facilities, which also contains some not even human-controlled natural environmental disasters, and so on.

Protective measures commonly used form of business is to set up a local area network, in order to encourage foreign direct visitors to get a real hard data sources and information from the corporate sector. Second, the information network level security, and this particular type of security or is that part of the network connection is the focus, often contain properly configured network communication line selection, network settings, and routers, etc., it is easy to produce the corresponding network in such aspects loopholes, thereby defects due directly caused serious damage to the development of enterprises and organizations.

Third, the level of information system security category, this level also refers to specific servers and computers are closely related, routers and other aspects of hardware security, and security systems which are primarily refers to the internal computer security software, such as where the system, facilities and procedures loopholes, these issues will be an urgent need to carry out their respective systems to be truly effective clean-up, otherwise it will be difficult to produce a truly effective protection process. Fourth, the communication level information security, specifically refers to the information itself in the transmission process of information security, which are among the most important foundation of network information security, can really protect the safe and reliable dissemination of information. Therefore, we must combine specific ways to communicate to implement protection strategies targeted, so as to secure communications system.

The Measures of Computer Network Information Security

Take Effective User Authentication Form. Specific to the respective legitimate users who implement user authentication, the purpose is to be able to avoid and prevent unauthorized users to obtain the corresponding effective way system information, and this authentication mechanism can effectively control the user to view their own information without permission. Under normal circumstances, the authentication mechanism taken from the specific needs of identity authentication and users’ authentication, password authentication and password authentication and other means to carry out. So in order to truly ensure visitors are legitimate users. There is also a form of message authentication are mainly to be confirmed by both parties of the communication content delivery, and sent by the sender directly to the recipient, the need to protect the entire transmission process cannot be tampered with. The access is mainly refers to access to the set-sector resources for authentication. There are digital certification, specifically refers to the use of encryption and authentication of electronic information approach to certification, its safety and effectiveness will be directly protected by a secret key. Finally, the digital signature technology, which is mainly based on encryption technology up be able to effectively achieve symmetric encryption and asymmetric encryption hybrid encryption and other forms to achieve.

Data Encryption Technology. Data encryption is particularly upset the original rule information,

and to promote it is in a state of confusion, did not get permission to view the person is unable to understand better. Data encryption is currently divided into two types of concrete form, that is, private key encryption and public key encryption both forms. Wherein the private key encryption is to provide better security for your data and other information, all using the private key cryptography to authenticate the users do not need to be created directly in order. Usually these forms are encrypted with high-speed, efficient methods and advantages. Among them, the real time public key cryptography to generate relatively late, and this can take two forms of encryption keys to. But still there is a corresponding defect itself, which directly leads to abnormal computationally intensive, which is generally much slower than private key on the calculated speed, a combination that you can get more complicated encryption system.

Application of Firewall Technology. The use of firewall technology is mainly used to protect the security of network systems, thus contributing to its truly effective in the internal and external networks to establish a good monitoring system, which for the transmission of data for monitoring will play a very significant role. But also can effectively control some artificial, malicious use of network security vulnerabilities to malicious attacks, which directly resulted in the system have been very severely damaged, resulting in computer users can not normally use. However, in the actual use of the process, the firewall itself is effectively cut off between the LAN and the external network, not only can directly intercept some of the external factors of instability, but also to carry out the user does not get permission for a visit. But it is undeniable that the firewall technology currently employed there are still some problems and defects, so it can only be prevented attacks outside the network, but it cannot prevent transmission of the virus from within the network behavior of malicious actions. Therefore, network security firewall technology in terms of safety, do not say is absolute.

Conclusion

the computer network security assurances should not just be achieved through computer technology, but also need to continuously upgrade their own computers for security management, and in order to carry out comprehensive network security for a variety of factors consider, finally a way to develop a truly effective way to plan, combined with the corresponding laws and regulations to protect the safety of the final network information.

References

[1] Jia Xinzhang, Li Jingyuan. Information and Computer, Vol. 6 (2014) No 53, p.25-26

[2] Wang Yunhui. Electronics and Software Engineering, Vol. 12 (2015) No 27, p.74-76

[3] Jing Jianfen. Computer Engineering, Vol. 30 (2010) No 19, p.144-145

[4] Wang Kuailiang. Information and Computer, Vol. 29 (2011) No 27, p.21-23

[5] Zhang Gongxu, Sun Jing. Electronics and Software Engineering, Vol. 8 (2013) No 27, p.57-60

江西省赣州市渡口路 7 号南阳东升 2 栋 2 单元 504 室
手机号码：13907078663　收件人：赖敏