# Analysis of computer network information security and protection strategy

Wenye Yu

Nanchang institute of science & technology,China

**Key words:** computer network; information security; protection; strategy

**Abstract.**This paper mainly analyzed the factors which affected the reliability of computer network information security, and on this basis, providedthe protection strategy of computer network information security.

Computer network has become an important part of public life, with the advent of the information era and increasingly developed of network, brought infinite convenience to people's life, at the same time, also let us involuntarily worry there were hidden danger. On this basis, it is particularly important to guarantee the security of network information.

## The definition of information security

Information security is an involved multi-subject comprehensive discipline, such as computer science, network technology, communication technology, password technology, information security technology, applied mathematics, number theory, information theory and so on. Security contents include four aspects: physical security, operation security and data security and management security. The definition of information security was given by special product category of computer information system in our country is that involving three aspects, that is physical security, operation security and information security.

## The factors affecting the reliability of the computer network information security

Computer network information security and protection are faced with varieties of potential threats, mainly reflected the following aspects:

The invasion of virus

Computer virus is a set of computer program code that are programmed or inserted in a computer program to destroy computer functions or destroy data, affect the use of computers, and be able to be reproduced, such as trojans and worms are common computer viruses. It will not necessarily directly harm the computer, but it will control computer in a certain extent, and steal information in the computer. Computer viruses have the characteristics, such as parasitism, destructiveness, latency, infectivity and unpredictability, etc. In the process of using a computer, common mobile storage and network are the medium to spread the computer viruses. Computer virus is a kind of computer technology and social information technology development inevitable product with the computer technology as the core.

Hacker's illegal intrusion, data’s eavesdropping and interception

In information security, "hackers" refers to researchers who outwit computer security system, using public communication network, such as Internet and telephone system, without permission, using computer technology in his field, try to visit computer file or network in the case of unauthorized. After collected some information which ready to attack, hackers can detect each host on the target network, seek security loophole in the system, establish simulation environment of similar attack object, and then proceed a series of attack for the simulated target, including through hackertechnology"Funtenna" - can steal physical isolation data in a computer by soundwaves, completely don’t connect to the Internet, this method can avoid the test of network security protection measures such as network detection, firewall and so on.This attack will cause great damage to the network, cause serious destruction and leak of some important information and data, the loopholes of network software also provide channels for hackers' illegal intrusion, make the revised information network cannot be used properly, cause great economic losses.

The lack of network management

The loopholes in network management, the lack of audit trail mechanism in the internal network, the network administrators and system administrators don't put enough attention to log and other audit information. Some institutions in the design of the internal network, only consider how to defense the external attack, but neglected the defense of internal attack. In addition, the low level of professional management personnel, switch can't be operated correctly, lead to partial or all broken network phenomenon. Besides, improper management measures and the user security consciousness are the important factors caused the network information stolen.

The attacks of E-commerce

E-commerce is the business activity which based on information network technology as the mean and commodity exchange as the center. E-commerce even in different countries or areas have different definitions, but the key is still the business model which relied on electronic equipment and network technology, with the high-speed development of E-commerce, it has not only including the main connotation of shopping, but also including incidental services such as logistics distribution. E-commerce includes electronic currency exchange, supply chain management, electronic trading market, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management and automatic data collection system. In the process, the information technology we used includes: Internet, extranet, email, database, electronic directory and mobile phones. Nowadays, E-commerce has filled with our life, work, study, everywhere, so it is particularly important to link the E-commerce system security and network information security closely, to ensure E-commercefromattacks.

The vulnerability of the network system

The sharing and openness of the Internet easily makes the Internet information security have a colossal security hidden danger, because it lacks corresponding security mechanism which depends on the survival of TCP/IP, and theoriginal design consideration of Internetis that the network will not affect the spread of information with local disturbance. Basically don't consider the safety problem, various applications such as server and browser are found to be unsafe. In addition, the security of the TCP/IP protocol used by the computer network system is very low, the computer operating system is easily suffer the threat of viruses, spoofing attacks and so on.

Natural disaster

Computer system is an intelligent machine, easily affected by natural disasters and the environment (temperature, humidity, vibration, impact, pollution). At present, we use a lot of computer space that all have no measure of shock, fire prevention, waterproof, lightning protection, electromagnetic leakage or interference and so on, grounding system is also lack of thoughtful consideration, and the ability to resist natural disasters and accidents is poor.

## The protection strategy of computer network information security

Improve the security protection system of computer network information

Computer security protection system includes various aspects of content, such as complete inspection and audit of the invasion, the network vulnerability scanning, detection of the virus, the network monitoring and so on. Intrusion detection is to monitor system operation state, to find a variety of attack attempts, aggressive behaviors or attack results, to ensure the confidentiality, integrity and availability of system resources. Through the analysis of the data packets, to filter out data packets from the data flow, to compare with known way of invasion, then to confirm invasion whether is a type of invasion, and to alert. The technical level of network dynamic scanning including scan line leak eavesdropping, whether there are loopholes of communication protocol and operating system, etc. At the same time, make standard network management rules to ensure information security system, regularly check the scanning computer, take the initiative to put away virus, and kill latent computer virus.

To strengthen the security of user account and password

User accounts are involved in a wide range, including many application accounts, such as system logged accounts, email accounts, online bank accounts and so on, the most commonly used method of hacker attack network system is access to legal account and password. First is to set up more complex account password, the second is to use the combination of numbers, letters and special symbols set up the account and password, finally, try to set a longer password and change your password regularly.

Install a firewall and anti-virus software

Network firewall is a kind of softwarethat is located between the computer and the network.The computer flows in and out of all network communication must pass through the firewall. Firewall can scan the network communication, and will filter out some of the attacks, so as not to be executed on the target computer. Firewall also can close the port that is not used. What is more, it can prohibit the outflow communication of specific ports, block the Troy Trojan. Finally, it can prohibit the visit from special site, so as to prevent all communication from an intruder. According to the firewall technology is different, it can be divided into: packet filtering, address translation, agent and monitoring. The firewall that Personal computer used is primarily software firewall, usually associated with anti-virus software installation. Antivirus software is the most security technology we use, this technology is mainly against the virus, it can kill virus, and now the mainstream of the antivirus software can also defend trojans and other hacker program invasion. At the same time, the antivirus software must be timely upgraded, upgrading to the latest version, to effectively prevent virus.

File encryption and digital signature

Using the file encryption and digital signature technology can effectively improve information security. File encryption is a common form of cryptography application.Fileencryption technology is the combination of password technology, operating system and file analysis technology. File encryption mainly includes the contents of the file encryption usually adopt the method of binary encryption, file attribute encryption, encryption of file input and output and operation process, namely dynamic file encryption. Digital signature is some data attached to the data units, or cryptographic transformations for data units. This kind of data or transformation allows the recipient of data units to confirm the source and integrity of the data units and protect the data, to prevent forgery. There are a lot of digital signature algorithm, the most widely used is: Hash signature, DSS signatures and RSA signature. Use file encryption and digital signature both can make we store files more safety.

## Conclusion

With the rapid development of computer network, network information security issues are constantly changing and developing. To get better protection for computer system, preventive measures are yet to be perfected; therefore, we should fully use a variety of protective strategies, absorb the advantages and strengths of various protection strategies, and gradually establish protection system of network information security.

## References

[1]Xiaoqing Peng. Analyze security technology of computer network [J]. Silicon valley, 2014 (11).

[2]Hongmei Wang, Huijuan Song, Aimin Wang. Research the security and protection of Computer network information [J]. Value Engineering, 2015(1).

[3]Guang Yang, Feifei Li, Yang Yang. Analyze preventive measures of computer network security [J]. Science and technology information, 2013 (29).

[4]Guoqing Liu, Guilin Yan. Research the security and protection strategy ofcomputer network information [J]. Electronic technology and software engineering, 2015 (8).

[5]Ping Yang. The problems and Countermeasures of computer network and information security

existed in China [J]. Mining machinery. 2013 (10).

[6]Shaolan Yang, Guozhen Xie. The assurance system of information security under the network environment [J]. Journal of Henan university (Social science edition).2015 (05).

[7]Kefeng Fan. Research the security and protection strategy of computer network information [J]. Industry and technology forum.2014, 13 (6).