International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 2, Issue 9, September 2015, PP 1-3
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
www.arcjournals.org

Network Information Security and Prevention

ZHU Zhenfang

School of Information Science and Electric Engineering, Shandong Jiaotong University

Jinan, China

zhuzhfyt@163.com

Abstract: *Network information is through the firewall, data encryption, access control, intrusion detection, security management, protection against viruses and other related technologies to its confidentiality, available, various properties of integrity, and controllability to provide security. In this paper, the above various prevention technology made some simple definitions, and key technology and safety were discussed, trying to simultaneously prevent the computer system from external attacks, comprehensive and effective information for the computer network to enhance security.*

Keywords: *Network Security, Information Security Technology, Prevention technology.*

1. INTRODUCTION

In recent years, computer technology develops swiftly, and network information plays a crucial role in the progress of social development. Network information always involves various aspects of a country with very important information about political economy, military security, etc. such as government decision, securities, and economic information. The most information is important, and some are even state secrets which may cause man-made attack from foreign and domestic nations. Generally, it is difficult to get the evidence of computer crimes, so the crime rate of hi-tech crime cases like computer crime increases, making the computer system, especially the network system faces huge risk all over the world. This is also a severe problem faced by all the nations.

2. COMPUTER NETWORK SECURITY THREAT AND ITS PRESENTATION

Computer network is featured with wide terminal distribution, various composition forms, and open network and interconnection. Therefore, it is easy to be attacked by hackers, phishing websites, virus, malwares, and many other forms.

(1) Information disclosure

The confidentiality of system is damaged because some people obtain information by illegal or unallowable ways. There are some threats causing information disclosure, including business flow analysis, online tapping, individual consciousness, physical invasion, vulnerability exploitation, rogue software, virus, phishing network, and postern.

(2) Integrity compromise

Data integrity can prevent data from being damaged in illegal way. However, the integrity of computer network will be damaged by means of loophole, virus, physical invasion, etc.

(3) Denial of service attack

Normal access to information of user is denied by computer abnormally, or operation related to time is delayed. Such an attack is the most common mean existing for the longest time. Actually, denial of service attack cannot be treated as an attack form, but a result caused by the attack. It may make the system cannot be normally accessed, and may even cause physical crash.

(4) Network abuse

The improper application behavior of legal users brings a lot of security threats, including illegal internal link, illegal external link, equipment abuse, motion risk, and business abuse [1].

3. Prevention Strategy for Network Information Security

Security guarantee is provided to various properties of network information, including confidentiality, availability, integrity, and controllability by firewall, data encryption, access control, intrusion detection, safety management, virus defense, and other relevant technologies. This work mainly analyzes aspects of firewall technology, data encryption, access control, and intrusion detection.

3.1 Firewall Technology

The most economic, effective, and basic prevention measure to guarantee the network security is to configure the firewall. As the guarantee of network security, firewall can strengthen the network security strategy, monitor and audit the network access and visit, and prevent the disclosure internal information outward. Communication between networks can be scanned with firewall to provide security guarantee to computer and network by closing the unreliable ports, blocking Trojan Horse, preventing external attack, etc. [5] Firewall has following effects: firstly, it can prevent external person from illegally visiting internal network and filter illegal users and unsecure services; secondly, it can prevent illegal person from getting close to defense measures; thirdly, it can limit users to visit special websites; and fourthly, it can monitor Internet safety to provide convenience.

3.2 Data encryption

Data encryption is an important component in computer network information security. In order to ensure the safety of e-mail, people adopt encryption technique with digital signature and configure authentication technology based on encryption to guarantee the person claimed in the e-mail is indeed the sender. With this method, information is encrypted with chaos to make unauthorized people cannot understand [7].

3.3 Access control

The main measure to protect and prevent network security is access control which can ensure the online resources will not be illegally visited and used. The adoption of access control limits the users who can access to the system and resources that can are accessible, including the way to use the accessible resources. A certain access control can prevent unauthorized users from obtaining information. Access control with ways of general login control, authorization inspection, command, and audit is not only an important means to protect online resources and network security, but also a significant way to combat hackers.

3.4 Intrusion detection

Intrusion detection is the combination of hardware and software for intrusion detection, reasonable supplement for firewall technology, and the second security gate following firewall. It can collect and analyze information through the key points in computer system or network to find if there is any sign of being attracted and violating security strategy.

4. Consideration about Network Security Education

The rapid development of computer technology has made a great progress, and modern computer has made people feel convenience brought by intelligence. It can be believed that computer intelligence will continuously develops and improve in the future, and it is reasonably believed that computer technology will certainly extend to other emerging technology field. In such a background, there will be more and more people touching and being familiar with computer technology. Actually, it has become a social trend in reality. However, a negligible problem that is, education problem also occurs. To some extent, the mastery degree of computer technology among citizens can reflect the comprehensive national power and the wisdom focusing on the future of a country. However, we should not only give the education about computer technological knowledge to citizens, but also give education about sense of morality and responsibility in maintaining computer network security.

5. Conclusions

Network security is not only the so-called technology problem, but also a problem involving security management. We have to consider about security problem comprehensively, and formulate rational goal, technical plans, and corresponding matching laws and regulations as requirement. There is no absolutely safe network system, but the network security protection technology will certainly accompany with the development and breakthrough of network application with the rapid development of computer network technology. When focusing studying on the development of network security protection technology, necessary guarantee should also be provided to network security information from the side. It can be believed that families, schools, and society play a crucial role in the educating and guiding teenage on this point.

ACKNOWLEDGMENTS

National Natural Science Foundation (61373148), National Social Science Fund (12BXW040); Shandong Province Natural Science Foundation (ZR2012FM038, ZR2011FM030); Shandong Province Outstanding Young Scientist Award Fund (BS2013DX033), Science Foundation of Ministry of Education of China(14YJC860042).

REFERENCE

[1] Ge Xiuhui. Computer network security management [M]. Beijing: Tsinghua University press, 2008

[2] Huang Xianjiao, Zhang Lin. On the network security technology [J]. computer knowledge and technology, 2006, (11).

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

[4] Chen Bin. Computer network security and defense. Information technology and network defense, 2006.04.

[5] Lin Jianping. Analysis of computer network security control strategy. Journal of Shanxi Radio&TV University, 2006.11.

[6] Xiao Jun. Network information countermeasure [M]. Beijing: Machinery Industry Press.

[7] Luo forest, Gaoping. Information system security and confrontation technology experiment tutorial. Beijing: Beijing Institute of Technology press.

[8] Li theory. Network information security and prevention.2013.06.

[9] Zhu Yanhui. Firewall and network packet capture technology [M]. Electronics Industry Press, 2002

[10] Zhang Hongqi. Information network security [M]. Tsinghua University press, 2002

AUTHOR'S BIOGRAPHY

ZHU Zhenfang, PhD, lecturer, he was born in 1980, Linyi City, Shandong Province. He obtained Ph.D. in management engineering and industrial engineering at the Shandong Normal University in 2012, his main research fields including the security of network information, network information filtering, information processing etc.. The authors present the lecturer at the Shandong Jiaotong University, published more than 30 papers over the year.