Advanced Engineering Forum *Online: 2012-09-26*
ISSN: 2234-991X, Vols. 6-7, pp 107-111
doi:10.4028/www.scientific.net/AEF.6-7.107
© 2012 The Author(s). Published by Trans Tech Publications Ltd, Switzerland.

Study on the Problems and Countermeasures of Information Security

Congjun Rao[1, a], Qing Zhang[1,b] and Jianping Gan[2,c]

[1]College of Mathematics and Computer Science, Huanggang Normal University,
Huanggang 438000, China

[2] Institute of Demographic Ecology and Resources Management,
Huanggang Normal University, Huanggang, 438000, China

[a] cjrao@163.com, [b] zhangqing@hgnu.edu.cn, [c] jpgan@hgnu.edu.cn

Keywords: Information security; Cryptology; Internet security

Abstract. Information has become a significant resource of strategy. The selection, the handling and the ability to keep safety of the information constitute an important section of a country's comprehensive national power. The information security counters about the stability of society, even the state security. Thus, it's time to take measures to guarantee our nation's information security. Recent years, the area of information security has acquired more new science results, which develops fast. Through discussing about Internet security, the major aspect of information safety, this dissertation points out the defections in our national security, and then presents some countermeasures to solve the problems.

Introduction

The 21st century is an information age. For one thing, the information technology and industry develop in a high speed, presenting a boom in the development. For another, Internet technology brings human convenient life, however, with the realization of resources sharing, the safety problems come out. It happens now and then to damage our information safety. All kinds of network attack technologies are developing progressively[1-2]. The revolution of information technology in the area of national safety has a profound significance. It not only brings new problems for those developing countries at this area, but also raises new threats and security leaks to those which have the most advanced information technology. The information security counters about the stability of society, even the state security. Thus, it's time to take measures to guarantee our nation's information security. Studying on the information security becomes a profound task for us to concern about.

Causes of the Information Security

The information security mainly contains 4 aspects: safety of information technology equipment, data security, content security and behavior based safety. The safety of information-system hardware structure and operating system is the basic of information-system security. Cryptogram, Internet security and such technologies are the key technologies [3-4]. Only taking security measures from the base of the information-system hardware and software could we insure the safety of information system .

Information security has become a tough nut. Technologically speaking, it is caused by following several aspects:

(1) The structure of microcomputer is oversimplified. In the 1970s, microcomputers were created because of the development of integrated circuit technology. Microcomputer is called personal computer, for it is used as private computer, but not public. To reduce the cost, many users believed that it's unnecessary to install security mechanism, thus many mature security mechanisms such as the memorizer's isolation protection mechanism and procedural security protection mechanism ,were deleted. As a result, the program would be executed without authentication, and the data of the system realm would be changed randomly. Computer virus, worm and Trojan such programs would reproduce fast.

(2) The development of information technology turns microcomputers into public computers. Microcomputers were not only private computers, but also have been used as public computers in an office or a house. However, when faced with public environment, the security defense capabilities of microcomputers appeared weak, because microcomputers had been canceled with lots of advanced security mechanisms.

(3) Internet changes computers into one section of it. The development of the Internet has changed computers into one part of it, which breaks the limitation of the computer's geographic isolation. Thus, the scale of massages' interaction is enlarged to the whole network. As the Internet is lack of enough security mechanism, computers are under unsafe atmosphere. No wonder that people always say "If one surfs the Internet, he will undertake more risks than often; however, if not, he will gain less services". Moreover, the complexity of the network protocol makes its security certification and authentication pretty difficult. Currently, people can only carry on some tests on simple one. So there exist no methods to avoid the security's loophole within network protocol. Even if the deal is correct, we cannot make sure its safety, as the correct one may also be used to attack computer. Attackers could start vast normal visits to occupy the computer and network's resources, which would make machine run wild, according to the theory of repletion and accumulation. The famous DOS is a typical evidence .

(4) The operating system has security drawbacks. Operating system is the most important system software, one base of the information security. However, it is because the operating system is so huge, like Windows has thousands of programs, that it is unable to handle the data correctly. Sometimes, the function failure has always been overlooked. For instance, when Windows system crashes, we should press the reset button to restart the computer. But if the system's weakness is used by attackers, the impact of the security drawbacks cannot be ignored .

The Study and Development of the Internet Security

The Internet security contains two parts. One is the security of network itself, and the other is the network information security. This chapter focuses on the latter. According to the safety necessity of network, the domestic and international academic and enterprise term are mainly studying about Network Content Security, Network Certificate Authority, Fire Wall, Virtual Private Network, Network Intrusion Detection, Network Vulnerability Testing, Secure Access, Security Isolation and Exchange, UTM, Safety Monitoring and Management, Network security audit, Malicious Code Detection and Prevention, Spam Disposal, and Emergency Response and so on. And also they have explored plenty of related network products, which formed a industry initially. It is a trend for the security technology based on the Internet to develop fast in the future information security's developing. From 3 aspects like Public Key Infrastructure, Emergency Response Network, and Network Survivability[7-8], the chapter summarizes the present research situation and development trend of the Internet security.

(1) Public Key Infrastructure

Public Key Infrastructure is a kind of an important technology that can solve the problems of trust and authorization on Internet, which contains the identity of the authenticity, the data confidentiality and the undeniable character of the behavior and so on. Recent years, the industry, the academic and the government has paid full attention on to the research and application of the PKI. Further more, the world's big information industry companies, such as IBM, MICROSOFT, BALTIMORE, CERTCO, RSA, FUJITSU, MITSUBISHI, have acquired PKI products. Many Chinese information industry companies also have explored independent PKI products. In fact, our academic area, such as the Information Security State Key Laboratory, has made a research about the PKI standard, the PKI's own security technology, and the crossing authentication technology, and they have got some advanced technology's achievements.

PKI is the key to solve the problem of network trust and authorization under the environment of network, especially in the e-commerce and e-government system has a broad application. The development of PKI presents following 3 trends: application trend, standardization trend and integration trend

(2) Network Emergency Response

With the development of network technology and related technology, the traditional and static security measures which were originally adopted are not enough to pretend the computer's hackers and the attack of a means of organized information, and we must set up a new security mechanism. In 1989, the United States Department of Defense funded Carnegie Mellon University to build the first "Computer Emergency Response Team (CERT)" and Its Coordination Center (CERT/CC) of the world. The establishment of CERT marked the change of information security, from static to dynamic protection.

In 1989, the CERT/CC was established by the United State Department of defense, shortly after that, the United States armed forces and the Department of defense, the national security agency and the defense communications agency established emergency organization, then the United States Federal Bureau of investigation the Department of energy, Department of Commerce, NASA and other important departments have also set up emergency treatment mechanism. So far, the United State Department of defense, the federal government departments and major enterprises, have created more than 50 computer emergency response organizations in the USA, which has formed a nationwide emergency network under the coordination of the National Infrastructure Protection Committee and Its Coordination Committee. Europe, Oceania, North America and many Asian countries and regions, especially the developed countries have successively established the information security emergency organization. According to the proposal of the emergency organization in the USA and Australia, on the 11th month of 1990, the international "computer incident response and security forum" organization was established. In addition, the Asia-Pacific countries and regions have built the "Asia-Pacific incident response coordination organization". Obviously, to establish the information security emergency organization, perfect the information security system and strengthen international cooperation, have become an international trend in the field of information security.

Although the academic circle and the industrial field have started an extensive and in-depth study for emergency response, which has gained many excellent achievements, there are many problems still need deeper research[9-11].

1) The research of emergency response system. The research of emergency response system includes emergency response organization system, emergency response system and emergency response support system.

2) Research and formulation of technical standard. Emergency response standardization work is not only the base of emergency response system communication coordination mechanism, but also the foundation of its normal operation. Emergency response standardization work is centered around the security event stream, which means the entire process of safety events from occurring until the elimination, including network security event's detection and reporting, the analysis and classification for security incident, the delivery, analysis and decision of security incident, coordination and response, and security events such as filing. There exist like emergency response process standards, security event classification standard, network security incident report format standard and security event description and exchange format standard, now.

3) The construction of the experimental environment. The construction of the experimental environment is to solve the emergency response system on practical application and inevitable demand. Furthermore, a typical tiny hardware experimental environment, which can be adequately modeled, to describe large-scale network features, and coupled with the corresponding simulation software, can provide a theoretical research platform for the practice and application of the verification environment.

4) The exploration of the core tool. The exploration of emergency response core tool is the key of the construction of emergency response system, including information sharing and analysis center, large-scale network security events coordinated early warning and rapid isolation control, security event plan system, large-scale network security simulation platform, protection association system, and backup and recovery system.

Chinese information security problems and corresponding countermeasures

Chinese current computer information security system is relatively weak, mainly including such several aspects of the problem:

(1) the capability of the network and information system emergency response is not strong, and the protection level is not high;

(2) the lack of high level of information security technology and management talents, and the key technology is still backward on the whole, and the work of security early warning and detection has not been launched, and the protection, emergency and recovery and other aspects of the work is still not deep enough and perfect;

(3) the information security management system and standard are lack of authority;

(4) the shortage of some essential information security equipments due to financial reasons;

(5) the concept of information security management is weak, and the awareness of relevant personnel especially those who are in charge is not strong;

(6) the information security management agencies and organizations are not perfect, restricting the further development and the promotion of information of security.

Information system is dynamic, and the corresponding safety system should also be dynamic. How to try our best to make all the potential unsafe factors nipped in the bud requires that we must build up a set of perfect security safeguard system of information system. System construction depends on the overall information system safety and the details of safety comprehensive quantification and grasp, and to develop the corresponding safety rating system.

(1) To strengthen a leadership, establish and improve the information system security management responsibility system. We should focus on ensuring the foundation information network and the important information security, creating a safe and healthy network environment. Improve the ability of emergency management, and according to the existing information security emergency response frame, refine to improve the information security contingency plan. Strengthen the spirit of information security work file conscientiously, study and formulate relevant information system security planning and management responsibility system.

(2) Establish the information security level protection system. Practically, balance safety cost and the risk of information security comprehensively, optimize resource allocation, and to ensure the key, set up the information security level protection system. Pay attention to the information security assessment work, analyze and assess the threats, weaknesses, protection measures in the network and information security system, consider the importance of the network and information system and the information security risks and other factors, and build up corresponding level of security construction and management.

(3) Build and perfect the ability of the information system security monitoring. Information security monitoring is an important method, for the protection of network and system, to detect timely and dispose with network attacks, preventing the transmission of harmful information. Construct and improve the centralized information system monitoring ability.

(4) Improve the information system security coordination mechanism. Establish a sound command scheduling mechanism and safety reporting system, and strengthen the emergency response disposal of it. Important information system construction should fully consider the invulnerability and disaster recovery. Constitute information system security emergency plan. And also, the construction of disaster backup should proceed from the actual situation, to promote the sharing of resources and mutual backup. We should strengthen the construction of information security emergency support service team, promote social forces to participate in disaster backup facilities construction and provide technical services, and improve the ability of emergency response.

(5) The information system security relates to information security and confidentiality. The information safety is our national security, so we are obliged to build a politically reliable, superb technology, excellent style of the technical staffs, offering talent assure to guarantee the security.

(6) Ensure the investment funds. Security construction of information system is the organic part of informatization, which must synchronized planning and construction. In informatization, construction, to make sure the information system security facilities operation and maintenance costs, we should simultaneously consider the security construction of it. When reporting information system construction projects, make security investment less than 15% of a total investment.

(7) Under the situation that the information security technology is relatively backward and security facilities are quite insufficient, improve and perfect the regulations about information network security, give full play to the management and regulation that are not technical means, and penetrate the information security into each link of the network, to make sure the protection of information system's security by policy rules and regulations.

Acknowledgments

This work is supported by the Natural Science Foundation of Hubei Province, China (No. 2011CDC028), the Key Project of Hubei Provincial Department of Education (No. D20122701 and No. D20102902), the Ph.D. Fund of Huanggang Normal University (No. 2011CD229 and to C. J. Rao), and the 2012 Excellent Youth Project of Hubei Provincial Department of Education (No. Q20122702).

References

[1] C. R. Shen, Thinking about Strengthen Safety Guarantee System-Information Security General, Hubei Science and Technology Press, Wuhan, 2002.

[2] H. G. Zhang, L. N. Wang, C. H. Huang, Information security discipline construction and talents training of research and practice. The national computer the dean (President) conference proceedings. Higher Education Press, Beijing, 2005.

[3] C. P. Pfleeger, S. L. Pfleeger, Security in Computing(3rd Editon), Prentice Hall, 2003.

[4] S. H. Liu, W. Q. Liu, H. G. Wen, Operating System Security. Tsinghua University Press, Beijing, 2004.

[5] J. P. Anderson, Computer security technology planning study. ESD-TR-73-51, Vol.II, Electronic Systems Division, Air Force Systems Command, Bedford, MA, USA.

[6] D. G. Feng, Network Security Principle and Technology, Science Press, Beijing, 2003.

[7] S. S, Y. Shim, L. Gong, A. D. Rubin, Securing the High-speed Internet. IEEE Computer 37 (2004) 33-35.

[8] C. C. Enz, A. El-Hoiydi, J. Decotignie, Wise NET: An Ultralow-power Wireless Sensor Network Solution, IEEE Computer 37 (2004) 62-70.

[9] J. Carle, D. Simplot-Ryl, Energy-efficient Area Monitoring for Sensor Networks, IEEE Computer 37 (2004) 40-46.

[10] D. G. Feng, X. Y. Wang, Progress and prospect on information security research in China, Journal of computer scitech 21 (2006) 740-755.