The security and protection strategy research of computer network information

Yu Liu[1, a], Jing Chang[1]

[1]Jilin agricultural university, Changchun, Jilin Province, China

[a]37373021@qq.com

Keywords: Computer, Network information, Security, Protection, Policy research

Abstract. With the increasing of network applications, the problem of network security is becoming more and more serious. Due to the diversity of computer network connection, terminal distribution in homogeneity, network openness and sharing of network resources, the computer network vulnerable to viruses, hackers, malware attacks and other misconduct. In order to ensure the safety and smooth of information, the network security and preventive measures is eyebrow nimble. This paper analyzes the main factors affecting network security and the primary means of attack, from two aspects of management and technology is to improve the security of computer network is put forward corresponding countermeasures.

Introduction

With the continuous development of computer network information technology, computer network gradually occupy the important position in people's life and work, it not only changed the traditional way of life, people and bring a lot of material and cultural life to enjoy. In the rapid development of Internet technology increasingly today, follow in the footsteps of progress and development of computer network technology, network security has become the important content that cannot be ignored, if network security suffered severe damage, will seriously restrict the healthy development of national economy, cause damage to the state and the interests of the people, therefore, must strengthen the construction of computer network security facilities, improve the network security technology such as protective measures, to eliminate potential safety problems [1]. At present, ensure the safety of computer network information, is the key to the maintenance of computer network security. This article mainly is the main factor of computer network security and related protection strategy has carried on the deep discussion, in order to better strengthen the computer network security.

The status quo of computer network information security

The danger of computer network attack and security issue. Computer network attack in principle can be divided into the following categories: first, using cyber attacks in the common technical terms and social terms to describe attack. Second, using the method of multiple attribute the attack is described. Third, for a specific application type, specific system and network attack. Fourth, the use of a single property description and only from the attack of a particular attribute of network attack [1].

Basic information security threats are: first, the leakage of information. Second, it is denial of service network system. Third, a resource is used by an unauthorized person illegally. Fourth, create, modify, or through unauthorized data destruction and damage [1]. Based on the resource sharing of computer network security hidden danger for the network against the spread of the virus has brought great convenience. Shared network equipment system intranets are used based on the technology of radio of Ethernet, the network hackers as long as the Ethernet access any node is easy to get on the Internet many of the free hacking tools, by sharing network, when a user and the host computer for data exchange, are likely to be the same to listen to other users on the hub. Today's cyberspace main can realize the threat of counterfeit, bypass control, authorization assault, Trojan horses, and trap door. Potential hazards such as hacking, traffic analysis, personnel negligence.

The threat of hackers and attack. This is of the biggest threats to computer network. Hacking means can be divided into two categories, non destructive attacks and destructive attacks [2]. Non destructive attack is generally to disrupt the system operation, information is not theft system, usually using denial of service attacks or information bomb; Destructive attacks into computer systems, data theft of confidential information, destroy target system for the purpose. Hackers attack on a commonly used password, email attacks, Trojan horse attack, fishing web of deception technology and looking for system vulnerabilities, etc.

Computer virus. Appeared in the 1990 s, has caused global panic "computer virus", its wide spread, growth at a staggering rate of loss is difficult to estimate. It like a gray ghost will be attached to other programs, when the program is running into the diffusion system [2]. After computer infected with the virus, light, makes the system work efficiency drops, or cause system crash or destroyed, the part or all of the data loss, even causes the damage of computer motherboard and other components.

Computer network attack protection goals. In the 1960 s for information protection in the age of communication security; In the seventy s era is a computer security; In the eighty s is safety information era; After ninety s is the age of information security [2]. Information security is through the so-called protection, detection, response and recovery of these four methods, namely so-called PDRR. Computer network attack protection is to protect the confidentiality of information, identity authenticity, integrity, service availability, system control, reliability, access control, no repudiation and can review.

The main factors of computer network security protection

Because there are many factors affecting the safety of computer network, mainly information constitute factors, the restriction of the human factors and natural factors, the development of computer information technology is hampered by a serious [3]. The Internet is open to the public network, plus itself exists vulnerability, therefore, in large part to the units and individuals to provide convenient conditions and steal all kinds of information on the Internet, due to the openness and freedom of computer network, computer network security faces a bigger challenge and development requirements, the following main factors affecting computer network security protection is introduced.

Vulnerability factors. Computer network vulnerability is mainly manifested in the network of openness and freedom, because of the network technology is opening to the outside world, lead to physical transmission lines at network attack, or from the attack on network communication protocol, caused severe paralysis, computer system and software, hardware, appear more holes, and the vulnerability to attack [4]. On technology, on the other hand, now the network has no strict constraints to the user, the user can free release and get all sorts of information on the Internet, the computer network security caused great impact. Computer network vulnerability factors greatly threaten the safety of computer network.

The operating system itself security issues. In computer facilities for the whole system, the operating system is the support of the computer software, which is the most important operation system, it is the normal running of all the procedures, provide a healthy environment [3]. But due to the operating system itself insecure factors are even provide more management functions, will be buried under a series of network security hidden danger, coupled with the development of the system design more problems, leading to the computer network security appears more serious consequences. The security threats to computer security are great, and often failing to defense.

Software vulnerability factors. Computer of every operating system or network software flaws and loopholes, therefore, makes computer face danger, once connected network, because computer speed is slow or even crash. More serious on the other side of the computer caused irreparable losses.

Improper security configuration. Once computer security configuration errors, it is easy to appear more holes, for example, firewall software configuration if it is wrong, so it's not the computer network security protection [3]. When launching web application, the corresponding open a series of security gap, cause and the corresponding software has also been opened, once the user is not the

correct configuration of the program, can produce many safe hidden trouble, negatively impact of computer network security protection.

The invasion of the virus. Virus is a computer network security number one enemy, is also a fatal factor to the computer network malfunction, if a computer operator in time to install the program, deliberately inserted some detrimental to normal operation of computer functions and instructions or code, not only influence the computer hardware and software facilities, and the virus replication and concealment etc., have seriously restricted the normal operation of the computer network.

The hacker's attack. Computer hackers are a threat to computer data security another aspect, it used the computer system security vulnerabilities in unauthorized access to computer system, and in direct attack, serious damage to the computer network security, its harmfulness is more serious than the average computer viruses and, therefore, hacker attack, seriously affects the safety of computer network [4]. In recent years, the hacker attack has evolved gradually from the threat of institutions for the attack on individual users, affects all aspects of social life, great harm to society.

The security protection strategy research of computer network information

Firewall technology. A firewall is a network security barrier and firewall configuration is to realize the network security is the most basic, one of the most economic, most effective safety measures. Firewall is a made up by software or hardware and equipment, in the enterprise or the network group channel between the computer and the outside world, limit as internal network users to access and manage internal users access to the outside network. When connected to a network system net, the safety of the system in addition to consider a computer virus, system robustness, more important is to prevent the invasion of illegal users, and the measures to prevent the main current is completed by firewall technology [5]. Firewall can greatly improve the safety of an internal network, and through the filter not security services and reduces risk. It to the transmission of packets between two or more network according to certain security policies such as link way to carry out inspection, to determine whether the network communication between the promise, and monitor the network running status.

Data encryption. Data encryption is of information coding, and hidden information content, make illegal users unable to get the real information content of a kind of technology. Data encryption technology is to improve the security and privacy of information systems and data, to prevent the secret data by external broken analysis using one of the main means. Data encryption technology according to the effect of different can be divided into the data storage, data transmission, data integrity, identification, and the key management techniques [4]. Data encryption is to prevent data loss in storage link for the purpose, can be divided into cipher text storage and access to two, data encryption technology is the purpose of the transfer of data stream encryption. Identification data integrity is involved in information transmission and access, processing of identity authentication and related data content, reached the requirements of confidentiality, the Eigen values of the system by comparing the validation of input meets the preset parameters, implementation of data security protection.

Antivirus technology. With the continuous development of computer technology, computer viruses have become increasingly complex and advanced, pose a great threat to the computer information system. Widely used in virus defense antivirus software, from the function can be divided into network anti-virus software and single machine of two kinds of antivirus software. Stand-alone anti-virus software installed on a single PC, to local and local workstation to connect remote resources with the method of scanning test, removes the virus. Antivirus software mainly focus on network anti-virus, once the virus invasion of network or spread to other resources from the network, network anti-virus software will detect and delete immediately [3]. Virus is mainly composed of data destruction and delete, back door, denial of service, spam to transmission network and several ways of the spread of damage, according to line congestion and data loss. So establish unified whole network virus prevention system is an effective protection for computer network as a whole solution.

Physical security. Physical security is to point to by means of radiation protection, password, state detection, alarm confirmation screen, emergency recovery means protecting the network server computer system, network exchange routing and other network devices and network cable hardware entities from natural disasters, such as physical damage, the electromagnetic leakage, error, and human disturbance and pulling attack damage [5], such as: the firewall and core switches and a variety of important as far as possible on the core server and other important equipment room for centralized management. Such as optical fiber communication lines buried deep, threading, or overhead, prevent damage of unintentional. The core equipment, main equipment and access switches to people, strict management. Physical security is to ensure that the campus network system to work normally, from the most basic means of disturbance.

Equipped with network security device or system. In order to reduce from the inside and outside the network attack and destruction, and need to be in the network configuration necessary network security equipment, such as network intrusion protection system, homepage tamper-proof system, firewall, network anti-virus system, vulnerability scanning system, content filtering system, patch upgrade system, server security monitoring system, and so on [6]. By configuring network security equipment, can realize the control and regulation of the campus network, to be able to block a lot of illegal access, can filter unhealthy data from the network information, and can help network administrators in the case of network fault locating rapidly. Make full use of this equipment can greatly improve the campus network security level of security.

Server access control policy. Server and router network infrastructure, to avoid illegal intrusion is an effective method to remove unnecessary network access and network access around based access control in need. In addition to the user and account for the necessary permissions [7]. One is to limit the number of the database administrator user and give users the minimum permissions granted its need. The second is to cancel the default account don't need permission to choose the appropriate account to connect to the database.

Establish a more secure electronic mail system. There are some good email security system has high accuracy and low rate of false positives, unique strategy module can help users to easily realize the mail system management and maintenance, some discriminate accuracy of spam E-mail system is close to one hundred percent [6]. Each user to analysis and comparison, choose good E-mail security system ensures that the network system security, to change the email system, such as spam, virus mail, E-mail leaks the status quo of safe hidden trouble.

For a long time, malicious attacker like using cloning method to control your computer account. They use of the method is to activate a default account in the system, but it is not often use this account, and then use the tool to promote this account to administrator rights, from the account or the same appeared on the surface, but the cloning of account is the biggest security hidden danger in the system. A malicious attacker can arbitrarily control your computer with this account. In order to avoid this kind of situation, can use the simple way to test the account.

To improve the quality of the network staff, strengthen the network security responsibility. In order to strengthen the responsibility of the network security, an important task to improve the management quality of the network staff is necessary. Want to combine the data in all aspects, such as software, hardware, network system staff safety education, improve the sense of responsibility, and through the relevant business skills training, improve staff's operation skill, network system to consider the safety management, to avoid man-made accidents [7]. Due to network research starts late in our country, and therefore needs to be improved and the development of network security technology. In addition, in order to ensure the safe operation of the network can, we should also develop a perfect management measures, establish a strict management system, perfect the laws and regulations, the law, raise their awareness of network security, increase of computer crimes law.

Summary

To sum up, the complexity of computer network security is a comprehensive and security issues, but in the face of the rapid development of network security industry, the whole process of social informatization faster and faster, with all kinds of new technology will appear constantly and the

application. Computer network security gestates unlimited opportunities and challenges, as a hot research field, has important strategic significance, this paper mainly related protection problem in the computer network security strategies discussed in this paper, in order to better to do a good job of computer security protection. At the same time we also believe that the future computer network security protection measures will be made more long-term development.

Acknowledgement

This project, Research on the Existence of Quasi-periodic Solutions to Partial Differential Equations with Given Frequencies, is supported by Foundation for Scientific Research Projects of the Education Department of Jilin Province (Project No.: 2016166). Project Principal: Jing Chang.

References

[1] Y. X. Yang, Network security theory and technology, Beijing: people's posts and telecommunications publishing house, 2008, vol. 4, pp. 32-36.

[2] X. Sh. Li, Computer system security technology, Wuhan: Huazhong University of science and technology press, 2009, vol. 1, pp. 12-15.

[3] X. H. Ge, Computer network security management, Beijing: Tsinghua university press, 2008. Vol. 2, pp. 43-46.

[4] Zh. T. Lin, X. J. Huang, Introduction to network security technology, Computer knowledge and technology, 2006, vol. 11, pp. 3-6.

[5] Ch. H. Xu, Computer network security and data integrity technology, Beijing: electronic industry press, 2005, vol. 8, pp. 61-65.

[6] J. T. Peng, J. H. Gao, Computer network information security and protection strategy research, Computer and digital engineering, 2011, vol. 1, pp. 24-28.

[7] X. R. Lu, Computer network information security and protection strategy research, Electronic production, 2013, vol. 10, pp. 8-13.