ATLANTIS PRESS
Advances in Engineering Research (AER), volume 107
2nd International Conference on Materials Engineering and Information Technology Applications (MEITA 2016)

The security and protection technology research of computer information

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

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

[a]37373021@qq.com

Keywords: Computer, Information, Security, Protection, Research

Abstract. Computer network information security is more and more attention in the national life, the reason: much important information is stored on the Internet, once these information leaks out will cause immeasurable losses. The network information will leak out, on the one hand, there are many invaders one thousand ways to want to "see" to some concerned data or information; On the other hand the network own existence safe hidden trouble that made the invaders, succeed. To solve these problems, this paper summarized and put forward some methods and strategies of network information security protection.

Introduction

With the development of technology, network is overcome the geographical restrictions, it distributes in a region, a country and even the global branch. They use public passing sensitive business information transmission channel, through a certain way can be used directly or indirectly, private network in an organization. Private network organization and departments also need because of business inevitably linked with external public sites directly or indirectly, the above factors make the network running environment is more complex, the regional distribution is more extensive, use more diversified, resulting in network sharply lower controllability, security.

With the augmentation of the organization and the department of network dependence, a relatively small network also highlight the character of a certain security problems, especially when the organization department of the network will face all kinds of security threats from external network, even the self-interest is no clear security requirements, may also be caused by an attacker use and unnecessary legal disputes. The spread of network hackers, network virus and various network security requirements is the urgent need for network security.

In this paper, the existing network security threats are analyzed and compared, especially to strengthen security measures should be taken to do a more in-depth discussion, and describes the future development trend of this research field.

The security threats and forms of computer information

Despite many now used for information security products, such as firewall, anti-virus software, intrusion detection system, but there are still many illegal invasions of hackers. Fundamental reason is the network security hidden danger cannot be eradicated. This makes the hacker flashpoint for invasion [1]. Nonetheless, safety protection still must be cautious, as much as possible to reduce the possibility of hacking, to protect our network information security.

Pose unsafe factors to computer information two aspects, on the one hand is artificial and natural factors, the two outside on the one hand is the security of the network architecture itself exists defects. Refers to man-made factors among them, some outlaws leaky computer network exists, or into the computer room, stole computer system resources, illegal access to important data, tamper with the system data and hardware equipment, the establishment of computer viruses [1]. And the security of the network architecture itself defects is to point to: the vulnerability of network operating system, TCP/IP protocol security flaws, and the database management system security vulnerability. Human factors are one of the largest factors for computer information network security threats. Computer network unsafe factors mainly manifested in the following aspects:

Computer network vulnerability. The Internet is open to the entire world network, any unit or individual can easily transfer and get all sorts of information on the Internet, the Internet has the characteristics of openness, sharing, and international poses challenges for computer network security [2]. The Internet is not safety basically has the following items:

1) The openness of the network, the network technology is completely open, make the network facing the attack from many aspects. Or come from the physical transmission line of attack, or from the attack on network communication protocol, and vulnerability of computer software, hardware to carry out attacks.

2) The international network, means of network attack is not only from the local network of users, other countries can also be the Internet hackers, so network security is facing the challenge of internationalization.

3) The freedom of network, most of the use of network to the user is not technical constraints; the user can free Internet access, publish and get all kinds of information.

The security problems of the operating system. The operating system is the basic support software, computer network make your program, or other use system above the normal operation of an environment [2]. The operating system provides many management functions. The main function is management system software and hardware resources. Operating system software own insecurity, flaw of system development and design to leave, leave the network security hidden danger.

The content of the database storage security problems. Database management system (large amount of information stored in various databases, including all of the information that we see on the Internet, convenient main consideration is the database information storage, use and management, but in less safety into consideration. Authorized users, for example, is beyond the access data changes. Illegal users to bypass security kernel, steal information [2]. Data security is to prevent the database was damaged and illegal access. The integrity of the database is to prevent the existence is not in conformity with the semantics of the data in the database.

The vulnerability of a firewall. Firewall is a made up by software and hardware equipment, between Intranet and extranet, private network and the structure of the interface between public protection barrier. It is a combination of computer hardware and software, set up a security between the Internet and Intranet gateway, thus protecting the Intranet from the invasion of illegal users [3].

But can only provide network security, firewall does not guarantee the absolute security of network; it is difficult to prevent network internal attacks and viruses. Doesn’t count on the firewall can give computer security by itself? The threat of a firewall to protect you from a kind of attack, but does not prevent attack from within the LAN, and if the internal and external, even if again strong, firewall is also no advantage. It even can't protect you from all those it can detect attacks. With the development of technology, and some also makes the method of crack caused by firewall must be hidden. This is the limitation of the firewall.

TCP/IP protocol security flaws. TCP USES three-way handshake mechanism to establish a connection, shake hands the first message for the SYN packet. The second message for SYN/ACK is packet, which indicates that it should be the first SYN packet to continue the process of shaking hands at the same time [3]. The third message is just a reply, expressed as an ACK packet. If A put for the connection, in response to party B, during the possible threat to have:

1) The attackers listening SYN/ACK is packet from party B.

2) The attacker to send party B the PST package, then send the SYN packet, fake A party launched A new connection.

3) Party B the corresponding new connections, and send the connection response packet SYN/ACK.

4) On the attacker to fake A party B an ACK packet.

This allows an attacker to destroy the connection effect, if an attacker to take inserts harmful packets, the more serious consequences.

Common form of computer information security threats

Natural disasters. Computer information system is just a smart machine, vulnerable to natural disasters and the environment (temperature, humidity, vibration, impact, pollution). At present, we have a lot of computer room and have shock, fire prevention, waterproof, lightning protection, preventing electromagnetic leakage or interference measures, such as grounding system is failing to thoughtful consideration, the ability to resist natural calamities and accidents, was poor. In the daily work of equipment damage due to power outages, data loss is often happened [4]. Due to noise and electromagnetic radiation, resulting in a decline in network signal to noise ratio and bit error rate increases, the information security, integrity, and availability are threatened.

Network software vulnerabilities and "back door". Network software can't be one hundred percent without defects and loopholes, however, these loopholes and defects is the first target of the hacker attack, had seen the hackers network internal events, most of these events is incurred because of security measures are not perfect [5]. In addition, the software "back door" is the design of the software company set up by the programmer to help you is generally not known to outsiders, once "back door" wide open, the consequences will be unimaginable.

The threat and attack of hackers. This is of the biggest threats to computer network. Hacking means can be divided into two categories, non destructive attacks and destructive attacks. 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 [4]. Hackers attack on a commonly used password, email attacks, Trojan horse attack, fishing web of deception technology and looking for system vulnerabilities, etc.

Spam and spyware. Some people use the E-mail address of "openness" and "system" can be broadcast "for business, religion, politics and other activities, you’re E-mail to" push "other people's email, forcing others to accept junk mail [3]. With a computer virus is different, the main purpose of spyware is not cause damage to the system, but steal system or user information.

Computer crime. Computer crime usually used to steal passwords and other means of illegal invasion computer information system, the spread of harmful information, malicious damage computer system, and the implementation of embezzlement, theft, fraud and financial crime activities. In an open network environment, a lot of information flow on the Internet; it provides a target for criminals [5]. They use different means of attack, gain access or modify the flow of sensitive information in the network, enter the user or the government departments of computer system, undertake peek, theft, tampering with the data. Not restricted by time, place, and condition of the network fraud, its "low cost and high income" to a certain extent, to stimulate the growth of crime. Made in view of the computer information system crime is increasing.

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 [6]. After computers infected with the virus, light, make 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.

The information security strategy

Firewall technology. Firewall, as a barrier to information security, firewall configuration is the most basic implementation of information security, one of the most economic, most effective safety measures. Firewall is to point to in the network of the computer and it is connected between the hardware or software, can also be between two or more networks, such as between LAN and the Internet, the network between all data flows through a firewall. Through a firewall, the network communication between close unsafe port, prevent foreign does attack, block a Trojan horse, etc. , to ensure the security of network and computer [7]. General firewall can achieve the following objectives:

1) The first it is to limit others into the internal network, filter out the unsafe service and illegal users;

2) The second it is to prevent the intruder is close to your defenses;

3) The third it is to limit users access to specific sites. Four is to monitor the Internet safety and convenience.

Data encryption. Encryption is through a way to make the information become chaos, so that unauthorized people don't understand it. There are mainly two kinds of main types of encryption: private key encryption and public key encryption.

1) **Private Key encryption**. Private Key encryption is also called the symmetric key encryption, because of the information used to encrypt the key is to decrypt the information using the key [5]. Private key encryption provides a further information of tightness, it does not provide certification, because the use of the key encryption anyone can create an effective message. The advantage of this encryption method is fast, is easy to implement in hardware and software.

2) **Public key encryption**. Public key encryption private key encryption appear than night, using the same private key encryption key to encrypt and decrypt, and public key encryption to use two keys, one for the encrypted message, the other for decryption [6]. The disadvantage of public key encryption system is that they are usually computation intensive, and therefore much slower than the speed of private key encryption system, but if the two together, you can get a more complex system.

Access control. Access control is the main strategy of information security and protection, its main task is to ensure that will not be illegal use of network resources and access to very much. Access control determines who can access the system, what resources can access the system and how to use these resources. Appropriate access control to prevent unauthorized users consciously or unconsciously to get the data [4]. The means of access control including user identification code, password, login control, resource authorization and authorization verification, logging and auditing. It is to maintain information security, protect the principal means of network resources, is also the key means of dealing with hackers.

Virus defense 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. Standalone antivirus software generally installed in a single PC, to local and local workstation to connect remote resources with the method of scanning test, remove the virus [6]. Network anti-virus software mainly focuses on network, once the virus invasion of network or spreading to other resources from the network, network anti-virus software will detect and delete immediately. Virus invasion will pose a threat to the system resource, so the user to do after the "prevention first". A lot of the spread of the virus is through the transmission medium, so the user must pay attention to the media spread of the virus. In the course of everyday use computer, we should get into the habit of killing virus on a regular basis. Update the installation of the Windows operating system patches from time to time and do not log in unknown web site and so on.

Security technology trends. Information security research in our country through the communication security, data protection, two stages, and is entering the network information security research stage, has now developed a firewall, security router, security gateway, the hacker intrusion detection, vulnerability scanning system software, etc [7]. But because the information is a comprehensive information security domain, cross disciplines, it integrated the use of mathematics, physics, chemical and biological information technology and computer technology of long-term accumulation of many disciplines and the latest developments, proposes the system and complete and collaborative solutions of information safety, should from the security architecture, security protocols, modern cryptography, information analysis and monitoring, and five aspects to carry out the research of information security system, parts work together to form organic whole.

Due to the continuous improvement of computer operation speed, various cryptographic algorithms is facing new password system, such as quantum cryptography, DNA code, password new

technology such as chaos theory is under exploration [7]. So the information security technology in the 21st century will be the key to the development of information network technology

Summary

In general, information security is not only a technical problem, is also a question of safety management. We have to consider safety factor, setting reasonable goals, technical scheme and related supporting regulations, etc. There is no absolute safety network system in the world. With the further development of the computer network technology, the information security protection technology is inevitable with the development of network application and development.

Acknowledgement

This project, Research on the Stability of A Small World Network with Higher Order Time Delay, is supported by Research Initiation Fund of Jilin Agricultural University (Project No.: 2015043). Project Principal: Jing Zhou.

References

[1] T. J. Lin, The computer network information security and protection strategy research, Network security technology and application, 2014, vol. 1, pp. 31-35.

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

[3] X.H. Ge, Computer information security management, Beijing: Tsinghua university press, 2008, vol.3, pp.9-13.

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

[5] L.T. Zhang and X.J. Huang, Information security technology introduction, The computer knowledge and technology, 2016, vol.8, pp.52-56.

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

[7] Ch.H. Xu, Computer information security and data integrity technology, Beijing: electronic industry press, 2015, vol.7, pp.13-17.