The Security and Protection Strategy Study of Computer Network Information

Junyan Shi[1,a], Juanjuan Li[1]

[1]Xuchang Vocational and Technical College, Xuchang, Henan province, China

[a]xinxipg@163.com

Keywords: Computer networks; information security; protection strategies

Abstract. With the rapid development of science and technology, computer network technology has spread to all areas of production and life. However, because of the network has connectivity and openness characteristics, that resulting in network security problems are more prominent, network data theft, hacker attack, viruses, Trojan attacks and other issues direct threat to network information security, economic and social life and even national security have caused a very threat. This paper analysis the computer network security risks existing for the information security threats that facing explore appropriate protective strategy.

Introduction

With the development of computer and communication technology, security and confidentiality of network information has become a vital and urgent problem. Computer networks have openness, interconnectivity and sharing of online information security and other features make the existence of deficiencies [1]. Plus the system software security vulnerabilities as well as the lack of strict management that causing is the network vulnerable to hackers, malware attacks. Therefore, measures for network security should be taken in all directions for a variety of threats. Protect the confidentiality, integrity and availability of network information. Existing network systems and protocols is still not perfect, imperfect, and unsafe: Some thoughts paralysis [1]. Not clearly aware of hacking can lead to serious consequences: some did not devote the necessary human, financial and material resources to strengthen the security of the network; did not use the correct security policy and security mechanisms: the lack of advanced network security technologies, tools, tools and products; there is still a lack of advanced disaster recovery measures and grief consciousness.

Network security issues facing information

Computer network own problems. Since the ill-considered or other factors cause the computer software put into use when there is vulnerability developers during the software design. Various types of computer software loopholes vulnerable to exploitation and to destroy the computer network attackers [2]. These vulnerabilities have caused great threat to computer network information security, but all systems are difficult to exclude the presence of vulnerabilities and repair work on the computer vulnerability is difficult to completely fully completed, which is a buffer overflow attack outside the computer network information system when most easily exploit loopholes in the system, the length of the instruction buffer by sending an attacker cannot handle, it will make the system into an unstable state, the more serious the attacker can take root access to the system [2]. Therefore, system vulnerability maintenance preventive work is imperative.

External computer security threats. Computer viruses, Trojan horses damage, Widely used in mobile storage medium, and large memory capacity and easy to carry, but computer virus tend to be widely disseminated for file transfers via mobile storage medium, thereby causing a computer to suffer serious viral infection, causing the computer system failure, and even hardware system file is missing varying degrees of damage [2]. And with advances in network technology, destructive Trojan virus is also growing, propagation speed, society and people's lives, causing increasingly serious harm.

© 2016. The authors - Published by Atlantis Press

Network hacker attack. Hackers through the network security flaws, illegal means to steal confidential information of others, such as political and military secrets, banking and finance and other economic secrets, to achieve their own purposes, to safeguard their own interests [3]. Meanwhile malicious hacker attacks may cause the computer information network system has been severely damaged, the use of malicious deletion, modification or forgery and malignant viruses, Trojans and other attacks the other's network information system, causing paralysis of the system. Hackers generally use denial of service attack, suspicious activity, protocol decoding and other means of attack, often superb and diverse means of attack, destructive.

Computer Network Information Security Policy

Set up a firewall. Firewalls are an important means to ensure network security, network management applications through the use of technology, packet filtering technology and agent technology, effectively control network access permissions, comprehensive data to external restrictions and discrimination [4]. Meanwhile, the firewall can make the internal network structure concealed, the external network to the internal network access to be limited in order to ensure the security of the internal network. In short, the firewall plays separated, analysis and its restricted role.

Access control. Security policy and security model based on access control body set access permissions, such as to the identity of the user, password authentication, in order to gain the true identity of the user, to facilitate tracing network behavior [4]. Combined with network licensing, issuing access permits the use of effective passwords and other means to prevent unauthorized users on the network information resources maliciously modified or used. Care must be taken to select a password which should enhance the security of the password strength, password and change them regularly to ensure information security.

Strengthening Intrusion Detection. Network intrusion detection is a real-time network detection system can effectively compensate for the lack of firewalls and other protective means [5]. Through real-time intrusion monitoring system to detect network security policy violations or external attacks, and calls the security warning and emergency response systems to ensure the security of network information. Intrusion detection technology with real-time detection, early warning and response to counter other powerful features, is increasingly becoming an important means of enhancing network security.

Information encrypted. Information technology is the key encryption technology to achieve information security, help strengthen security, through a particular encryption algorithm translated the important plaintext ciphertext, so unauthorized users can not directly read the raw data, even if the data file is lost or stolen, as long as difficult to crack the key, so it will not lead to the leakage of confidential information, which greatly ensure information security [5].

Close some not commonly used services and ports. From the theory in terms of computer security, computer systems were more port system is also more secure. For using the computer in the process, especially when the operating system is installed in inadvertently will not have to install some service functions and ports, it will not only occupy a certain system information and also reduce the security of computer systems sex [6]. In addition. In order to understand the use of the user interface can be installed port monitoring program. It can be determined by examining those ports are not commonly used. In addition, once a virus into a computer system, the monitoring program can automatically alarm, some of the function can automatically shut down the port, effectively prevent hacker intrusion.

IP addresses are correct hidden PC. IP address of the hacker and virus attacks must have a condition that is on the network and information attacks must have a real IP address to be a hacker to obtain the user's IP address mainly through the use of network technology to detect host information view, some of the traditional hackers and virus attacks, Floop overflow attacks and so must obtain address as preconditions [6]. Therefore, the user should use a computer system when hiding your IP address, using a proxy server is the most common way to hide IP address, a hacker can only detect the proxy server IP address, but can not get the user's real IP address You can not find the real IP address will not be able to attack, effective maintenance of computer information and network security.

Authentication technology. Authentication should include at least verification protocol and license agreement. A variety of network applications and computer systems are needed to confirm the legality through authentication, and then determine its personal data and specific permissions. For authentication system, the legitimate user's identity is easy to be someone else pretending to be its most important technical indicators [6]. User being impersonated user may not only damage their own interests, but also may harm the interests of other users or the entire system. Therefore, authentication is the basis of authorization control. Only valid identity authentication, to ensure the effective implementation of access control, security audit, intrusion prevention and other security mechanisms.

Timely installation of Vulnerability Patch. Vulnerability can be utilized during the attack weaknesses can be software, hardware, procedural shortcomings, functional design or improper configuration. University of Wisconsin Miller gives a research report on today's popular operating systems and applications, noting that the software can not be without flaws and loopholes [7]. Nowadays more and more viruses and hackers exploit software vulnerabilities to attack Internet users, such as the famous wave of virus attacks is to use the Microsoft RPC vulnerability to spread, the Sasser virus is the use of a Windows LSASS buffer overflow vulnerability exists in the attack. When our system there are loopholes in the program, it will cause great security risk. To correct these vulnerabilities, software vendors release patches [7]. We should be installed vulnerability patch, effective solution to the security problems posed by vulnerable program. Vulnerability scanning can use specialized vulnerability scanners, such as COPS, tripwire, tiger and other software.

File encryption and digital signature technology. File encryption and digital signature technology is to improve the security and confidentiality of information systems and data, one of the secrets to prevent external data theft, interception or destruction primary technologies [8]. Depending on the role, file encryption and digital signature technology is mainly divided into data transmission, data storage, data integrity of the three kinds of discrimination.

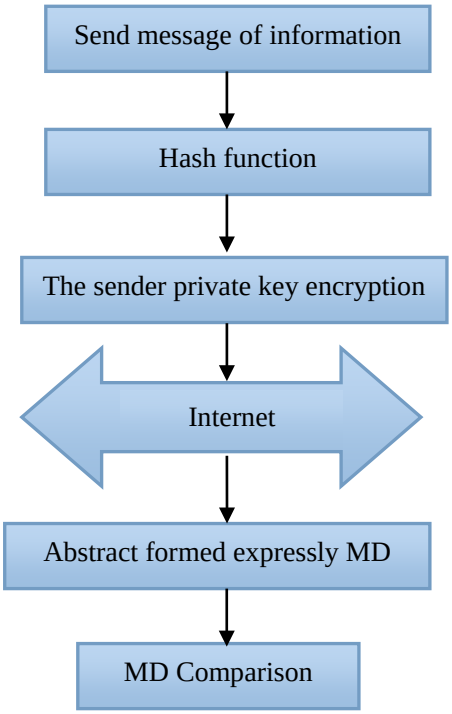

Fig.1 Usually the digital signing process
MD means Encryption key

Data integrity identification technology is mainly involved in the transmission of information, access, processing of data related to the identity and to verify the contents, to confidentiality requirements, including general identification passwords, keys, identity, data items of the system by Comparative validation object input feature value meets the preset parameters, to achieve data security.

A digital signature is an effective method of network communications-specific safety issues, it enables the identification and validation of electronic documents, to ensure data integrity, privacy, non-repudiation has a very important role [8].

Realization of digital signatures:

1) Usually a digital signature. A sender sends a message to give the recipient B M, the first one-way hash function is formed message digest MD, and then signed. This can confirm the source of the information and ensure the integrity of information, workflow is shown in Fig. 1.

2) Using asymmetric encryption algorithm and one-way hash function for digital signatures. This method uses two keys (public key and private key), respectively, the data encryption and decryption. If the public key to encrypt data, only with the corresponding private key can decrypt; if the private key used to encrypt the data, only the corresponding public key can decrypt. This approach allows anyone with the sender's public key can verify the digital signature is correct. Because the sender's private key confidentiality, so that the recipient can verify the results to either reject the message, but also makes it impossible to forge signatures and message packets to be modified.

Summary

Computer network security has become an important issue of network development at this stage, to ensure the network information security. We must depart from security threats through the use of advanced security technology and software technology to effectively monitor potential threats, and timely warning, response, to prevent malicious behavior. And should raise awareness of network security, improve the morality of the whole society, reduce network violations, efforts to establish a secure network environment.

References

[1] Q.X. Zhao and Z.Q. Liu, The information age of computer network security, Information security and confidentiality of communications, 2009, pp.12-16.

[2] X.Q. Su and Zh.H. Sheng, Computer network security and firewall technology to explore the development of technology, Science and technology innovation Herald, 2012, pp. 34-37.

[3] D.M. Liu, The computer and network security prevention strategies, Heilongjiang Science and technology information, 2010, pp.43-48.

[4] Y.L. Sun, Security and prevention of computer network technology, Metallurgy Heilongjiang, 2013, pp.65-68.

[5] Zh. Xu , Computer and network security countermeasures, computer knowledge and technology, 2011, pp.7-10.

[6] Q.Y. Huang, Based on Intranet information secure digital signature technology, Computer knowledge and technology, 2014, pp.70-74.

[7] J. Wang, Digital signature technology, Computer Engineering and Science, 2013, pp.67-70.

[8] X.G. Bai, Principle and application of digital signature technology, computer Fujian, 2010, pp.15-19.