Analysis on Security Management Strategy of Computer and Internet Information System

Yuan Chen[1,a]

[a] email

[1] Nanyang Medical College, Nanyang, Henan, 473000

Keywords: Internet; Information Management; Security Strategy

Abstract. With the rapid development of network, network information security more and more people's attention. Through the network information security threat factor analysis, and then we present five common computer network information security policy, information security and network development were discussed) to form a network information security system. Key words computer network; network information security; security threats; precautions; security system

Introduction

With the extensive application of information technology and Internet technology, and now the network has become an indispensable part of life, people's needs and that reliance on information network system is increasing. At the same time, threats to network security has become more and more serious. Therefore, the analysis of the impact of network security reasons put forward countermeasures to protect network security becomes very important. Internet openness and other factors led to the computer system network environment there are many security risks. In order to solve these security issues, a variety of security mechanisms, security policies and network security tools been developed and applied. Network security is an information related to computer science, network technology, communication technology, cryptography, information security technology, applied mathematics, number theory, information theory and other disciplines comprehensive discipline. It mainly refers to the network of data protection hardware, software and systems, from accidental or malicious destruction of reasons, changes and disclosure to ensure continuous and reliable normal operation, without interrupting network services [2].

Security Threats Facing Computer Network Information

There is a wide range of network security threats, a common natural disaster, network system itself vulnerability, user error, malicious man-made attacks, computer viruses, spam and spyware, computer crime.

Computer information system is only an intelligent machine, vulnerable to natural disasters and the environment (temperature, humidity, vibration, shock, pollution). Currently, we use a lot of space on your computer are not earthquake, fire, water, lightning, anti-electromagnetic interference leakage or other measures, the grounding system also lacks thoughtful consideration, ability to resist natural disasters and accidents is poor.

The most significant advantage of Internet technology is openness. However, this wide open, from a security point of view, it has become vulnerable weaknesses. Plus the Internet relies on TCP /IP protocol itself is not a high security [2], to run the network protocol exists spoofing, denial of service, data interception and data tampering threats and attacks.

User security awareness is not strong, simple to set up a user password, the user will be free to disclose their own account, will be a threat to network security.

This attack is the biggest threat facing computer networks. Malicious attacks can be divided into two kinds of active attacks and passive attacks. Active attack in various ways to selectively destroy the validity and integrity of information; passive attacks without affecting the normal work of the network, they were intercepted, theft, decipher important to obtain confidential information. Both attacks can cause great harm to the computer network, and result in leakage of important data.

Network software now used more or less there are some flaws and vulnerabilities, hackers usually use illegal means to invade vital information systems, eavesdropping, access, attack invasive important information about sensitivity, modification and destruction of normal use of information networks state, resulting in data loss or system failures, and have inflicted major economic losses and political influence.

A computer virus is storable, enforceable, can be hidden in the executable programs and data files without being found, after triggering acquisition system control section of the executable program, it is contagious, latent, and can trigger damage and other characteristics [4]. Computer viruses mainly by copying the files, transfer files, run the program and other operations spread. In everyday use, the floppy disk, hard disk and network is the main way the virus spread. After running a computer virus may reduce the efficiency of the system ranging from weight may damage your files, and even delete files, data loss, hardware damage the system, causing a variety of unpredictable consequences. More vicious virus emerged in recent years are based networks to spread these viruses devastating computer network, such as the "CIH virus", "panda virus" can be all talk about the mere mention of it to the network with to a very serious loss.

Some people use the system openness and e-mail address may broadcast of commercial, religious, political and other activities, their own e-mail forcibly pushed into someone else's e-mail, force others to accept spam. Computer viruses, the main purpose of spyware is not to cause damage to the system, but the system or to steal user information, user privacy and computer security threats and possible small impact system performance.

Usually use to steal passwords and other means of illegal intrusion into computer information systems, dissemination of harmful information, malicious damage to computer systems, the implementation of embezzlement, theft, fraud and financial crime and other activities.

Common Computer Network Information Security Policy

Although the computer network information security threats, but take appropriate protective measures can effectively protect the security of network information. Common computer network information security policy are:

Covers a wide user accounts, including the system login name and e-mail accounts, online bank account applications such accounts, and obtain a valid account and password hacking network system is the most commonly used method. The first is the system login account set up complex password; Second, try not to set the same or similar account, as far as possible the use of numbers and letters, special symbols combination manner account and password, and try to set a long password and change them regularly.

Firewall is a network technology used to enhance network access control between to prevent external network users to illegal means to enter the internal network access to internal network resources, protection of special networking equipment internal network operating environment. Transmission of data packets according to some security policy to implement it between two or more network checks to determine whether the communication is allowed between the network and monitor the network running. According to the technology used different firewall, it can be divided into: packet filtering, network address translation type, type and monitoring-type agents. Packet filtering firewall uses network transmission technology subcontracting, by reading the packet address information to determine the / 0 if the packet from a trusted secure site, once the packets from the dangerous site, the firewall will these data shut out. NAT firewall to the inside of the IP address into a temporary, external, registered IP address. When the internal network to access the Internet, external hide the true IP address. External network access to internal network, it does not know the internal network connection through the network card, but only through an open IP address and port to request access.

Proxy Firewall, also known as a proxy server located between the client and server, completely blocking the exchange of data between the two. When a client requires the use of data on the server, the first data request to the proxy server, proxy server and then request data to the server upon request, and then transferred to the client. Since there is no direct data path between the external

system and internal server, it would be difficult against external malicious damage to the internal network. Monitor firewall firewall is a new generation of products, the use of technology has gone beyond the original definition of the firewall. This type of firewall can be active layers of data, real-time monitoring through the analysis of these data, it is possible to effectively determine the layers of trespass. At the same time, monitoring the firewall also generally with distributed detectors, these detectors placed among the node servers and other network applications can not only detect attacks from outside the network, but from the inside of vandalism also have a strong preventive effect. Personal computer firewall is mainly a software firewall, antivirus software, and generally supporting the installation. Antivirus software is the most secure technology we use this technique mainly for the virus, killing the virus, and now the mainstream anti-virus software can also Trojan defense
Hacked and some other programs. Note, however, antivirus software must be time to upgrade, upgrade to the latest version in order to effectively virus.

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. 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. We should be installed vulnerability patch, effective solution to the security problems posed by vulnerable program. Vulnerability scanning vulnerability scanner can use specialized than
Such as COPS, tripwire, tiger and other software can also be used 360 security guards, Rising Kaka and other protective software to scan for and download patches.

Intrusion detection is a recently developed technique of a deterrent, using a combination of statistical techniques, rules, methods, network communication technology, artificial intelligence, cryptography, reasoning and other techniques and methods, its role is to monitor network and computer systems if there is invasion or signs of abuse. According to the analytical techniques used can be divided into a signature analysis and statistical analysis. Signature analysis: used to monitor the system behavior of known vulnerabilities to attack. People are summarized in the attack mode from its signature, write to Ds system code, signature analysis is actually a template matching operation. Statistical analysis: The theoretical basis of statistics to the system under normal use conditions observed operation mode basis to identify whether an action deviated from the normal track.

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. 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. Data encryption technology is mainly used to transmit the data stream encryption, there are usually two kinds of line encryption and end to end encryption. The former focuses on the route, regardless of the source and sink, is each line of confidential information by using different encryption keys to provide security protection. The latter refers to the message by the sender through a dedicated encryption software, using an encryption technology to encrypt files sent to encrypt the plaintext into ciphertext, when the information reaches the destination by the recipient using the corresponding key decrypt ciphertext data recovery becomes readable in plain text. Objective data storage encryption technology to prevent data in the storage areas of compromised, can be divided into the ciphertext storage and access control in two. The former general is to convert additional passwords, encryption modules, etc. on the locally stored files are encrypted and digitally signed by encryption. The latter is the user's entitlements, privileges and restrictions to be reviewed to prevent unauthorized users from accessing data or unauthorized access to legitimate user data. 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. There are many digital signature algorithm, which is the most widely used: Hash signature, DSS signatures and RSA signatures. Digital signature implementations generally have the following forms: 1) general 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 the information. 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. 3) with symmetric encryption algorithms for digital signatures. Encryption and decryption keys used for this method is generally the same, even if the difference may also be easily made of any one of them derive another. In this algorithm, encryption and decryption keys used by both sides to be kept secret. Since the calculation speed is widely used in a large number of database file encryption, such as the RD4 and DES. 4) the recipient non-repudiation digital signature. This method not only prevents repudiation of the sender can be prevented deny the recipient, relatively high demand for communications applications. But this method of encryption and decryption too many times, affecting the efficiency of data transmission. 5) Based on the time stamp digital signature. Of this method of introducing the concept of a time stamp, reducing the number of data encryption and decryption, also reduces the profile encryption and decryption time, and ensure reliability of data transmission, security, and the sender, the recipient of all non-repudiation By improving data encryption, decryption and transmission efficiency, more suitable for high data transmission requirements of the occasion.

Digital signature technology as an important information security technology, and its applications are increasingly widespread. With the rapid development of computer networks, digital signature technology in many areas of the proposed new application requirements. Currently used in some special occasions demand special purpose digital signatures is gradually growing. Such as anti-failure signature (Fai-lstop) will prevent an attacker has sufficient computing resources; blind signature (Blind Signature) will be more widely used in elections and digital currency agreements; and group signature (Group-oriented Signa-ture) in a large-scale group purchasing online will play a more important role, will significantly reduce the cost of e-commerce transactions, greatly improve the efficiency of transactions.

Network Information Security System

With the evolving attack methods, traditional to rely on firewalls, encryption and authentication and other means has failed to meet the requirements, status monitoring and response links in the modern network security system is becoming increasingly important, it is gradually becoming the Construction of Network Security System an important part of not only a simple process operation protection network, the network also includes a safety assessment, and the use of security technology after service system

Conclusion

Network information security is a constantly changing, fast update field. This means that simply

using a certain kind of protective measures can not guarantee the security of information networks, we have comprehensive use of various protection strategies, set director of public companies, with each other, in order to establish the network information security protection system. Therefore, we protect the network information security must be very careful to minimize the possibility of hackers to protect the security of network information.

References

[1] Peng Xiaoming. cope with the rapid development of computer network security technology to explore [J]. Silicon Valley, 2009 (11): 86.

[2] Li Yong. Computer network security and prevention [J] Bengbu School Education, 2009 (1): 30-31.

[3] Lin Jingna. Computer Network Security and Defense [J]. managers, 2009 (11): 335.

[4] Lu Peng. Computer Network Security and Protection Strategy of [J]. Silicon Valley, 2009 (12): 62-63.

[5] Wang Yongzhong. Computer network management technology and its application [J]. Science and Technology Information Review, 2007 (1): 188 – 189.