The application and analysis of network security technology

Na Wu
Nanchang institute of science & technology，China
35482278@qq.com

Keyword: computer;network security;technology;application

Abstract. In recent years, with the rapid development of computer technology and communication technology, the application of computer network is more and more popular, it has been penetrated into every field of human's working and living, such as daily work, finance, trade, shopping and so on, and it has been basically achieved networking. But at the same time, due to the openness of network, computer virus emerges in endlessly, network hacker's rampant activities letting human impossibly defend themselves effectively, network security suffered unprecedented threat. Therefore, realizing the vulnerability of computer network, finding the potential threat of network security, deepening the research of network security, and taking effective technology to ensure the security of computer network, is very important to protect human's normal working and living of modern society. So this paper analyzed and discussed the security technology and application of computer network.

The security threat analysis which computer network information faced

At present, the vast majority of domestic enterprises and units established related information system, and realized to make full use of all kinds of information resources. But with all walks of life information network system gradually forming, network information faced more and more security problem, such as hackers, malicious software and other attacks. A lot of information security technology have been researched and developed, used for protecting network information security, but there are still many problems, investigated its reason, mainly manifested in the following aspects:

(1) The vulnerability of computer network

The Internet is network which opening to around the world, all units or individual can conveniently transport and get all sorts of information on the Internet, the Internet gives the challenges to computer network security which has the characteristics of openness, sharing, internationality. At the same time, the related communication protocols used in information network, didn't have high safety performance, and it existed some safety problems, such as easy to suffer deceive attack, information manipulation, data capture and so on.

(2) The security problems which operating system existed

Operating system is the basic support software of computer network, it has provided a lot of management functions, mainly is the software and hardware resources of management system. Due to operating system software's own insecurity, and system open design's inconsiderate to leave flaw, left hidden danger of network security.

(3) The vulnerability of firewall

The firewall is made up by software and hardware equipment, it is a protective barrier constructed on the interface between intranet and extranet, to private network and public network, it is a combination of computer hardware and software, to set up a security gateway between the Internet and Intranet to protect the Intranet from the illegal users' invasion. But the firewall can only provide network security, and it can't guarantee the network absolute security, it is also very difficult to prevent internal attacks and viruses' invasion. With the development of technology, some crack methods also have made the firewall caused some hidden troubles, this is the limitation of the firewall.

(4) The attacks of computer virus

Computer virus has many characteristics, such as concealment, infectious, destructive, and so on,

© 2016. The authors - Published by Atlantis Press

it often as a normal procedure by hidden or disguised, with the start of computer program to run it. Computer virus realized to the operation of the network information by destroying and eavesdropping. Compared to other security threats, the overall threat level is bigger, with the slight effect is to affect the operating efficiency of the operating system, the heavy effect is to destroy the user's overall system data, and it is very difficult to be restored, so that to form irreparable damages.

(5) Other factors

The computer system's hardware and communication facilities are vulnerable to suffer the influence of natural environment, such as all kinds of natural disasters pose threat to computer network. It also has some accidental factors, such as power failure, left some loopholes in the software development process, to pose serious threat to computer network. In addition, bad management rules, imperfect regulations, errors in operation, malfeasance and so on, all will pose threat to the computer information security.

The main information security technology and application analysis

(1) Internet protocol security

As the next generation Internet protocol, the security of IPv6 is higher, enforcing compliance security agreement IPSec of Internet, it is made up by certification agreement, encapsulation security load, Internet key exchange protocol, namely, AH, ESP, IKE. IPSec can ensure IPv6 has higher interoperability and security performance, makes a wide range of security services to effectively implement the IP layer.

(2) Encryption and digital signature technology

The encryption technology as the most basic of network's security technology, at the same time, it is also the core of information security. The emergence of encryption technology provided the guarantee for the global e-commerce, so that it makes the electronic trading system possible which based on Internet. The password constitution includes single-key, double-key and mixed password. Among them, the single-key is the symmetric password; double-key is the asymmetric password; mixed password is the mixture implementation of single-key and double-key. At present, in the network information, the password techniques mainly adopt double-key and mixed password.

A. Public key cryptography

In order to strengthen the security performance of the public key cryptography, the length of public key $\geqslant$600bit. At present, RSA public key cryptography is based on Montgomery algorithm, excluding the existed mode of division, through the multiplication model and modulo subtraction at the same time, much improve the operation speed, are widely used. At the same time, some manufacturers successfully developed the elliptic curve public key cryptography which matched IEEEPl363 consistent standards, and successfully applied to the electronic government affairs, had strong confidentiality and high speed.

B. Hash-function

In regard to put forward the SHA collision and cracked theory of SHA-1, reduced the calculated amount which SHA-1 had cracked, to a great extent, it affected the assessment of the Hash function safety status and design in the future. At the same time, due to the crack of MD5 and SHA-1, letting the existed theory foundation of digital signature suffer questioned, to bring a great threat to digital signature method which is using.

C. Quantum cryptography

Quantum cryptography technology adopted the quantum mechanics law, to allow the both users have private random number string, to represent a single quantum sequence information of digital string, and through the bit value to receive information, to ensure no communications eavesdropping. Once it occured eavesdropping, communications will be finished, and generated a new key.

(3) Firewall technology

The firewall technology is a set of organic combination between hardware and software, is a effective mean to control internal and external network access, can ensure the Intranet to operate

safety and stablely. The firewall technology provided access control and information secrecy for users, possessed the advantages of simple operation and high transparency, while keeping the original, on the basis of network application system function, the maximum met the user's network information security requirements, widely respected by the users.

At present, from the perspective of the technology which firewall used, there are mainly three types: packet filter technology, agent service technology and condition monitoring technology. The packet filter firewall technology is the application of the filter principle and technology, checked the network outside to the inside network packets to flow, at the same time, to limit the gateway firewall. And agent service firewall technology, the major role is in the application layer, through transfering the application services from external network to internal network, to control the application layer services effectively. When internal network can not accept the direct request which applied by external network node, the service request will be accepted only for the agent pattern.

The firewall technology as one of the network information security technology, with simple operation and strong practicability, is widely used. But restricted by its characteristic, lack the active response of the dynamic and complicated attack means, only processing the static security defense, unable to safeguard against all external attacks can be effectively prevented. Some higher levels computer hackers can turn over the firewall, to achieve the attack purposes. At the same time, the firewall can't stop the internal attack. Therefore, in order to realize network security, need process the data encryption, strengthen internal network’s control and management.

(4) Intrusion detection techonology

Intrusion detection technology is a technology for testing some abnormal phenomena, when found the abnormal phenomenon, intrusion detection technology could send out corresponding alarm to remind human. Within computer network, some unsafe behaviors and measures could be detected by this technology.

(5) Biological recognition technology

Biological recognition technology is one kind of solution which depended on the body's physical characteristics to authenticate. Due to the human’s body characteristic has the characteristics not to be copied, the security system of biological recognition technology has greatly improved than the authentication mechanism of traditional sense. The body's biological characteristics including fingerprints, voice, face, the retina, and so on, amoung these characteristic, fingerprint received continuous attention with its incomparable uniqueness, stability and reproducibility.

The comprehensive application of network information security technology

Based on the specific analysis of current main network information security’s technology and application, can build a full range of network information security protection system, to realize integrated application of network information security technology which has all kinds of different function. In this system, it had some different specific network information security technology, applied to different levels of network information security requirements, to process security protection of more layers and broader ranges, to realize the whole communication security of the network system. The overall network security protection system is made up by network security evaluation system, safety protection system and network security service system. According to the integrated application of network information security technology which have different functions, can build a full range of safety protection system, to realize the safe protection of whole process network communications group, effectively enhance the reliability and security of network information.

Conclusion

Along with the continuous improvement of computer communication technology, information system has gradually turned into the most important ways for enterprises and units to realize information exchanged. Mastering the shortcomings and security threats in the course of information systems, can help users to set up security strategy with high feasibility, to indeed promote the security performance of information system. At the same time, the network information security system is not only a single security technology which only works on a particular aspect, but is a variety of security technologies which effects on different aspects, is a more complex system. This system includes people's composition, and technical composition, is not a simple accumulation of security technology such as anti-virus, firewall, encryption, and intrusion detection, but is a whole upgrading and optimization treatment from system to application. At present, about the network information security technology, upgrading is in the stage, new technology constantly being developed. But affected by various factors, new technology will exist some loopholes inevitably, it also need to update and perfect timely. In addition, because the technology such as computer virus, computer crime is regardless of national boundaries, therefore must organize a sufficient international cooperation, to jointly cope with the problems of increasingly rampant computer crime and computer viruses.

References

[1] Qianli Zhang. The new technology of network security. People's posts and telecommunications press, 2003.

[2]Haifeng Liu, Lei Yi. The analysis of impact factors and precaution for computer network information security [J]. Information security and technology, 2013 (8).

[3]Chun Liu. Network intrusion detection model which based on the combination algorithm selection feature [J]. Computer and modernization, 2014 (8).

[4]Chenggong Shan. The study of security technology and development trend which based on computer network information [J]. Electronic technology and software engineering, 2013 (23).

[5]Guozhi Lu. A new introduction to e-commerce [M]. Peking University Press.2005