Design of LAN Security Analysis System Based on B/S Architecture

Wenzhi Zhu

Zhongnan University of Economics and Law, Wuhan, China

Keywords: B/S Architecture; Information Security; Development; Attack and Defense

Abstract: Network security is becoming more and more important in our life, because the rate of network using is getting higher and higher, and the demands and functions of the users are increasing. So, to adapt to the dangerous network environment, prevent information from being stolen, destroyed and used, it is essential to discuss our own understanding with our own practical development and our own learning in the process of learning network security.

1. Introduction

The era of networking has been irreversible, almost all walks of life are linked to the Internet to operate, publicize and develop, and enterprises that are not linked to the network will eventually be eliminated by the big trend. When we rejoice in the huge profits and profits brought by the Internet, various network security problems also give us a head start. At present, there are a wide variety of Chinese enterprises, wide range of operations, different types of business, and the threat of network security is uneven, but they are more or less vulnerable to hacker attacks, malicious code, data leakage and internal abuse, and the enterprise network environment is not optimistic. Not only is the enterprise suffering, the vast number of netizens are also increasingly being attacked, and the security of privacy and funds can not be guaranteed, and the persecution of network security events, such as information leakage and capital theft, has been frequently suffered. It is undeniable that the network is a double-edged sword. Therefore, we must attach importance to network security, and focus on building a network security protection system.

2. Various Threats to Network Security

Malicious code includes traditional computer viruses, Trojan horses, worms, logic bombs, script viruses, user level RootKit, core level RootKit and so on.

There are security vulnerabilities in the current operating system, especially the universality and operability of Windows, which make it the most insecure server operating system. There are Office vulnerabilities, browser vulnerabilities, II S vulnerabilities, SQL loopholes, code vulnerabilities and other application systems leak holes to constitute a major threat to network security. System vulnerabilities are the structural defects of the computer software system. In addition to the vulnerability repair, it is necessary to design the computer software system and reduce the number of loopholes in the system.

Internal users threaten illegal access to Internet, such as browsing websites such as yellow, violence, reactionary and so on, as well as clicks and mistaken attacks caused by spam and illegal mail links. At present, the spam in the network generally has computer virus and Trojan horse program. If the spam is spread and access to illegal links, it is easy to cause the computer to infect the virus and cause the computer system to be paralyzed.

3. Security Service Mechanism.

3.1 Encryption mechanism

This mechanism provides confidentiality of data or information flow and can be used as a complement to other security mechanisms. The encryption algorithm is divided into two types:

(1) symmetric key cryptosystem, encryption and decryption use the same secret key;

(2) asymmetric key cryptosystem encrypts public key and decrypts private key. The key management mechanism must be used in data encryption under network conditions.

3.2 Digital signature mechanism

A digital signature is a number of data attached to a data unit or a cryptographic transformation of a data unit that allows the receiver of the data unit to confirm the integrity of the data unit source or the data unit, and to protect the data and prevent the person from forgery. The digital signature mechanism consists of two processes: data unit signature and verification of the signed data unit.

3.3 Access control mechanism

The access control mechanism determines and implements access to the entity using the identified entity identity, the entity's relevant information or entity's capability.

3.4 Data integrity mechanism

Data integrity includes two aspects: first, the integrity of a single data unit or field, and the two is the integrity of data units or field sequences.

3.5 Authentication exchange mechanism

Identify the mechanism by which switches identify entity identity by exchanging information. This mechanism can use the following techniques: the sender entity provides authentication information (such as a password), the authentication of the recipient entity; the encryption technology; the features and attributes of the entity, etc.3.6. Communication service filling mechanism

The communication business fill mechanism can be used to provide various levels of protection against communication business analysis. This mechanism produces forged information flow and fills the protocol data unit to achieve a fixed length and limited traffic analysis. This mechanism is effective only when the information stream is encrypted and protected.

3.6 Routing mechanism

Routing can be dynamically predetermined to use only physically secure subnetworks, relay stations, or links; in detecting persistent operating attacks, the end system can indicate that the provider of network services is connected by different routes; data with certain security markup can be banned through some subnets by the security policy. A collaterals, relay station or link.

3.7 Notarization mechanism

This mechanism confirms the characteristics of data communication between two or more entities: data integrity, source points, endpoints, and time to send and receive. This guarantee is provided by notaries, the third party trusted by communication entities. In the detectable way, notary holds the necessary information to confirm. Notarization mechanism provides services, but also uses digital signature, encryption and integrity services.

4. Construction of Network Security Protection System

4.1 Set up a firewall

Firewall is an effective defense tool. On the one hand, it makes local systems and networks free from the threat of network security. On the other hand, it provides an effective way to access the outside world through the wide area network and Internet. Network firewalls isolate internal and external networks, access control strategies between internal and external networks (Internet), in order to prevent unpredictable, unlawful access or potentially destructive intrusion of Intranet resources.

Firewalls are designed to operate only for access control software, without other devices, with relatively few defects and security vulnerabilities; in addition, the firewall improves the login and monitoring functions and can be managed specifically; moreover, the security management of the

main engine of the entire intranet becomes a firewall to the firewall. The safety management makes the safety management more convenient and easy to control. It is one of the most effective tools to realize the network security strategy, and it is also the first gateway to control the access of external users to the intranet. Therefore, the construction of network security protection system should first strengthen and improve the firewall.

4.2 Installation of the necessary antivirus software

A good safety protection system should not only protect and detect beforehand, but also effectively eliminate virus infection. The firewall can effectively prevent the virus from invading, but can not eliminate the virus completely. When the computer is poisoned, it needs special antivirus software to clear it, so it is necessary to install a variety of antivirus software on the computer. The antivirus software generally has broad-spectrum anti-virus ability. It can kill more than 90% virus, small black, worm and back door. It can find and eliminate the corresponding computer virus, malware and Troy Trojan horse. It has many functions, such as real-time monitoring of computer, scanning and clearing virus, automatic updating virus library and so on. Installing anti-virus software on computers plays a very important role in protecting network information security. Based on this understanding, the network anti-virus software should be actively applied in the software system of the grating machine, so as to quickly kill and kill computer viruses.

4.3 Resolutely resist the use of computer pirated software or hardware.

Because of the high price of current software and hardware, ordinary Internet users and small and medium enterprises usually choose to buy pirated software and hardware in order to save cost, so the equipment itself belongs to the vulnerable object. Even if the high level security protection technology is adopted, it is still vulnerable to the attack of the black guest or the virus. The purchase of pirated software or hardware not only makes the user's computer at high risk, but also seriously offends the copyright protection law of our country, while some businesses in order to reduce the price of computers attract customers, and usually install pirated software without the user's knowledge. Faced with this series of violations, relevant departments should actively supervise and formulate effective laws and regulations, and increase sanctions and penalties. For the users themselves, we should also enhance the awareness of resistance to piracy, not to be too small, not to be too cheap to buy irregular computers and software, to ensure that the initial stage of the use of computers is in a state of safety and health, which will greatly reduce the probability of the virus invasion and the attack by the black guest.

4.4 Good habit of backups of information and information

When your computer has a virus, it will affect the normal operation of the system, or even cause the system to be completely paralyzed. The task and meaning of backup is to recover a system that is available immediately, simply and reliably after the disaster happens. This is often the case, we do not hurt the loss of a computer, we are heartache in the information inside, the information in this can not be repeated again, maybe we spent a few years of blood, it is our precious memory. The manpower, material and financial resources that we want to restore to such a material is so great that we are in despair. Backup can be done as long as a safe host can be destroyed before it can be destroyed, so that the loss can be minimized.

4.5 Improve network security management system

In the face of the vulnerability of network security, in addition to increasing the security service function and improving the security and secrecy measures in the network design, it is necessary to make great efforts to strengthen the security management of the network. The network security management system consists of three parts: legal management, system management and training management.

Legal management has mandatory constraints on the main behavior of the information system, and has a clear management level. System management is the formalization and concretion of legal

management, the interface of law, regulation and management object, and training management is the premise to ensure the security of information system.

5. Summary

Finally, what I want to say is that network security is closely related to everyone, and every one of us should participate in the construction of network security environment. In peacetime, we should pay attention to the temptation to resist bad information, do not browse malicious web pages, do not download malware, supervise network information security and report unlawful information in time. At the same time, we should also learn some simple protective measures, such as backup, installation of antivirus software, and timely antivirus; in addition, in order to destroy the security of other people's network, Shame, even with this technology, it should be used in a suitable and active place, rather than a fluke, that it is a thing to show off to be a hacker, and we are not aware that we are on the way to the law. As a programmer, we should have our own principles, consciously maintain network security, and create a healthy and upward network environment for everyone.

References

[1] Yizheng Chen, Fujian Tang, Yi Bao, Yan Tang, *Genda Chen. A Fe-C coated long period fiber grating sensor for corrosion induced mass loss measurement[J]. Optics letters, 2016, 41(10):2306-2309.

[2] Du X, Chen L, Huang D, Peng Z, Zhao C, Zhang Y, Zhu Y, Wang Z, Li X, Liu G. Elevated Apoptosis in the Liver of Dairy Cows with Ketosis[J]. Cellular Physiology & Biochemistry, 2017, 43(2):568-578.

[3] Fernandes, S.L., Gurupur, V.P., Sunder, N.R., Arunkumar, N., Kadry, S. A novel nonintrusive decision support approach for heart rate measurement[J]. Pattern Recognition Letters, 2017.

[4] Jennifer W. Chan, Yingyue Zhang, and Kathryn E. Uhrich. Amphiphilic Macromolecule Self-Assembled Monolayers Suppress Smooth Muscle Cell Proliferation[J]. Bioconjugate Chemistry, 2015, 26(7):1359-1369.

[5] Stephygraph L R, Arunkumar N, Venkatraman V. Wireless mobile robot control through human machine interface using brain signals[C]// International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials. IEEE, 2015:596-603.