Research on Security Issues Based on CAN LAN

Yu-yang Du[1, a], Hai-yan Zhao[1,b], Jing Zhao [1,c], Hui Li[1,a] and Huai-jun Zhou[1,a]

[1] Department of Network service, Xi'an Communication Institute, Xi'an 710106, China

[a]51375908@qq.com, [b]813086903@qq.com, [c]583822272@qq.com

Keywords: CAN LAN, Security Policies, Network Security Technology

Abstract: With the rapid expansion of the rapid development of computer network technology and network coverage, network security issues are increasingly complex and outstanding looks up. In this paper, we have the analysis of the CAN security situation, put forward the principle of network security policy-making process to be followed, clearly a number of network security policy are also pointed out to build a more complete network security solution ideas. For the current CAN security issues, we discuss the principles and methods of the CAN network design process involved in the security system, and propose specific means for the CAN technology features. Meanwhile, we have researched and explored the characteristics and design of school network management, combined with the existence of the local area network insecurity, indicated security needs of the network, and to developed appropriate the security policy of network.

Theoretical Introduction of CAN LAN Security

The construction of CAN LAN will provide digital high-reliability and high-performance network infrastructure services on one platform for the whole school teaching, research, administration and service work are based on information technology and network, so that teachers and students , researchers and administrative staff can most easily achieve the exchange of information and sharing of resources for collaborative work, improve the construction of network, which is conducive to enhance the level of school education and social competitiveness.

Now network virus and network security has become a major hazard vulnerability LAN stable operation. The construction of network security system is actually the process of lasting confrontation between the intruder and anti-intruder. People are trying to build a dynamic network security protection system is dynamic + static defense, passive + active defense even fight, the concept is a complete security management + technology. Ensure the LAN normal and efficient operation, the development of a well-conceived and effective network security strategy is very important. In the LAN planning and design process, the main security issues that should be considered are: physical security, unauthorized access, denial of service attacks, computer viruses and so on [1].

Conducting local network system security design should follow the following principles: the principle of needs, risks, costs balance analysis. The main principle of consistency refers to the development of secure off-line structure must be consistent with the security needs of the network. Principle of ease, security measures need people to do, if the measures are too complex for people too high, reducing the security itself. We should ensure that the measures adopted should not affect the normal operation of the system. Principle of adaptability and flexibility, security measures must change with the network performance and security needs change, easier to adapt, but it also can be easily modified to meet the needs of future upgrades. It is a very important aspect to prevent attacks from the current network construction.

Requirements Analysis of Network Security

At this stage, the theme of the network architecture has been formed, but with the further increase of the network service requirements, but also in the operation of a comprehensive solution to the problems, so as to provide more comprehensive services [2]. Fig.1 shows the requirements analysis of network security.

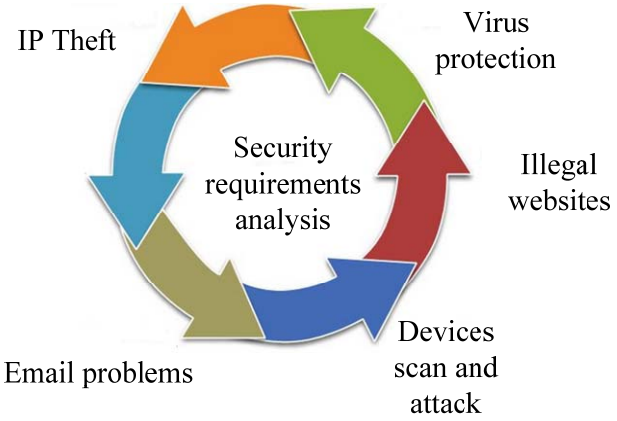

Fig. 1.The requirements analysis of network security

There are thousands of internally connected to the computer, computer application is a legitimate part of the IP address of the application through the normal way, but the reality is that not all schools have requested the computer IP address, fraudulent use legitimate IP address of others, it will cause conflicts within the network address, a serious impediment to the legitimate user's normal use. Firewall system development related technology is relatively mature, the firewall system is very strong, but this is only for external protection only, it is for internal protection almost can't afford to make any difference. Unfortunately, under normal circumstances, there is 70 percent of the attacks from the LAN internal staff. Since the user's security concept weak some people with ulterior motives and online, will give the network users to send some bad content Email letters, and sometimes carry a wide variety of viruses. So, how to prevent the problem letters into the network Email system is also a problem to be solved.

Sometimes there will be some users of the network servers and network devices to scan and attack, causing the network is heavily loaded, causing the server to refuse to provide services, or cause network can't provide normal service. For some reactionary or unhealthy sites, should be prohibited in the network users to access through the network. The rapid development of Internet makes network operators to become a social fashion, but also for the rapid spread of viral infections and viruses from passing between the network cause system crashes, network paralysis, pose a serious threat to network services, resulting in huge losses. So, how to make safer, preventing the network from virus attacks, become the network is an urgent need to solve the problem [3].

Network Security Technology

Firewall is mainly used for data access network restrictions, the system provides access control and centralized security management to prevent unsafe access to data and services. Traditional firewalls using packet filtering or packet filtering technology work in the seven models in three-tier network. With the application of new technologies such as flow filtration, current firewall policy deployment can have the application layer, including the use of network firewalls can achieve divide the DMZ, NAT address translation functions. Currently firewall technology can be divided into three categories according to achieve: packet filtering firewall, application proxy, station detection firewall [4].

VPN (Virtual Private Network) will be physically distributed in different locations in the network backbone via a public Internet connection, especially to form a virtual subnet. Depending on its capabilities, VPN can be divided into remote branch offices to implement the Internal Security interconnected Intranet VPN and secure interconnection with other partners Extranet VPN. Meanwhile, VPN technology also provides data encryption authentication technologies such as multiples in different places of the Internet security provided technical assurance. VPN tunneling technology used mainly, encryption technology, key management techniques and technology user and device authentication. Fig.2 shows the CAT workflow of system.

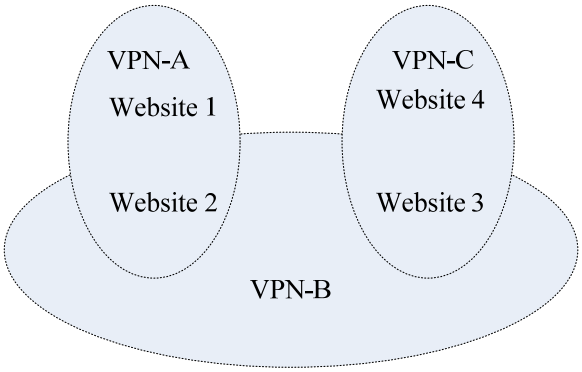

Fig.2.The CAT workflow of system

Intrusion Detection System (IDS) is defined as "behavior, security logs, or audit data, or other information obtained from the network can operate the system detects intrusion or intrusion attempt." Intrusion detection systems on the network only alarm unsafe operation after interaction with the router or firewall, the data can also be blocked. However, since the accuracy of the passive system and the identification of IDS are not high, so there are still many problems in use. Intrusion Prevention System (IPS) technology uses the rules of conduction, and immediately block when the attack was found. Moreover, it is able to perform some of the application layer access policies, to attack from a normal port for effective protection.

Development of Network Security Policies

LAN security threats may come from the network outside, which may also come from within the network. Therefore, when the security policy of LAN is designed, we should take safety precautions on LAN borders against external invasion and attack. Meanwhile, we should make security access control on the LAN internal infrastructure equipment. LAN security policy-making process, the following elements are usually considering [5]. Fig.3 shows the network security policy.

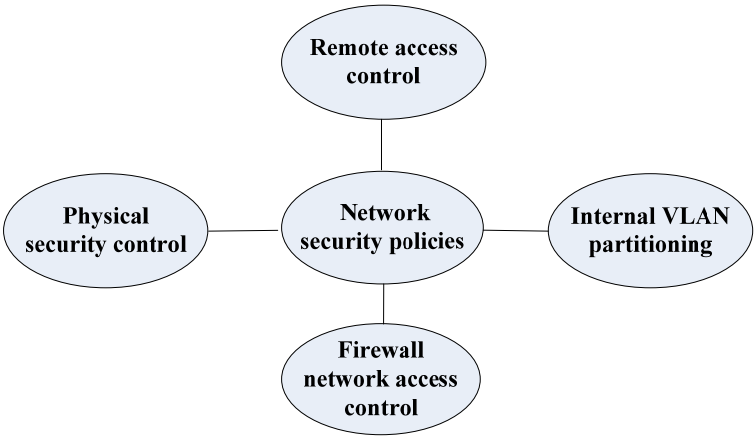

Fig. 3.The network security policy

Physical security control strategy. Physical security controls are controls on the existing physical infrastructure, security, physical equipment and physical access. Physical security control strategy should include: All rooms must be built or rebuilt in accordance with the relevant safety standards; management responsibilities and clear operating authority administrators and operators; all network infrastructure equipment must be connected redundant power supply. Firewall network access control policy. For the safety and security of the intranet hosts, set the demilitarized zone (DMZ) on the firewall, shielding the internal network, disable external network users to connect to the internal network; only http and pop and other limited services to external users; internally Network general to provide users with http, FTP, SMTP, BBS, News and other Internet services, as well as intranet multimedia and audiovisual services.

We divide the principles adopted internal VLAN port + VLAN division based on IP addresses, all unused switch ports constitute a VLAN, VLAN support switching equipment, all port has a

default VLAN number. All access control port switching device constitutes a VLAN, the role of the port access control on the switch is used for network management. Remote access server ports, is a weak link in the LAN security. The main security policies we have adopted are: restrict remote access to the appropriate calling number; choose the appropriate authentication method for remote access to authenticate users; restrict remote access to the user's operation of the Telnet server, record the use of dial-up users, and regularly to be checked.

Conclusions

With the popularization of the network, the security issues have become increasingly prominent, CAN facing information leaks, damage the integrity of the business and the illegal use of refuse and other security threats. In this paper, we have discussed the security requirements of CAN, security technology, security management, etc. and explore the CAN security policy. The current status of network is discussed, as well as the requirement analysis and designing of system function, and we have given some useful suggestions on selection of the communication technique, project construction of total network. The CAN security flaws are reviewed to explain security flaws caused due to a variety of network security issues, which further put forward various possible and necessary security policies in order to ensure the safety of the CAN and normal operation.

References

[1] Jakob Vlietstra. Dictionary of Acronyms and Technical Abbreviations[M]. Springer,2006.

[2] Zhao P, Cao Xw, Luo P. Attack on Radius Authentication Protocol. Process of the ICCT 2003, IEEE, 2003; 1: 208-212.

[3] Zouheir Trabelsi, Khaled Shuaib. A Novel Man-in-the-Middle Intrusion Detection Scheme for Switched LANs. International Journal of Computers & Applications. 2008, 30(3):234-243

[4] Biju Issac. Secure ARP and secure DHCP protocols to mitigate security attacks. International Journal of Network Security. 2009, 8(2):107-118.

[5] Seung Yeob Nam, Dongwon Kim, Jeongeun Kim. Enhanced ARP: Preventing ARP Poisoning-Based Man-in-the-Middle Attacks. Communications Letters, IEEE. 2010, I4 (2):187-189.