Research on Security Issues and Protection Strategy of Computer Network

Min Zhu[1, a], Yong-jian Luo[1,b], Jun-qiang Yang[1,c] ， Ming-shun Xing[1,a] and Jing Zhao[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: Computer Network, Network Security, Security Protection System

Abstract: Development and improving and bringing very great impact to network of the network technology of the computer, the security question of the network has become one of the focuses of the social safety question of information. In this paper, through the analysis of computer network information security threats and protective factors conducted and presented as a basis for a common computer network information security and protection strategy, looking forward to provide useful lessons for our computer network and information security and protection reference, a series of questions such as security and depend ability existing to the network system of the computer, this text proposes some opinions from respects such as the importance, online security existing problem of the computer and precautionary measures of the online security of the computer, etc.， and has explained in detail, so that the masses of users strengthen safe precaution consciousness while using the computer network.

Theoretical Introduction of Computer Network Security

In essence, network security is information security on the network, which refers to the flow of network systems and data saved are not subject to accidental or malicious destruction, disclosure, alteration, the system for normal operation, the network service is not interrupted. Broadly speaking, all related to the network confidentiality, integrity, availability, authenticity and control technologies and theories related information are network security areas to be studied.

Using Physical Security Network is the premise of the entire network system security. Physical security is defined as the physical medium level of network storage and transmission of information security protection is essential to protect the network information security. Establish physical security architecture should consider three aspects: First, natural disasters and equipment failure (power, electromagnetic interference); the second is an electromagnetic radiation, take advantage of infiltration, traces of leakage; three are operational errors (hard disk formatting, line removal), accidental omission and so on [1].

Now Internet has become an indispensable part of our lives, the network had infiltrated into the commercial, financial, government, health care, research, education, and other social sectors, making the network has become in our lives can't be missing an important part. Internet, LAN, or even GPRS cellular communications, life always reflect the power of the network. With the development of the network, boosting the number of new industries, such as online games, online chat, online video download; at the same time, network media, e-commerce, e-government and other companies to bring more business opportunities. If the external and internal communication network, the machine is likely to internal network security threats, but also affect other systems on the same network.

Overall Design of Defensive System

With the evolving means of attack, relying on traditional firewalls, encryption and authentication and other means has failed to meet the requirements, monitoring and response aspects in modern network security system is becoming increasingly important, gradually becoming a network

security system in the building important part, not just a simple process of running protection network. With the rise in dependency on the network, hacking tools emerging, traditional network information security is far failed to meet people's requirements for information security, and the construction of network information security system has been welcomed by all [2].

From the above, we can see that the principle of attacks, prevent spoofing attacks are not the biggest difficulty lies against the server or switch the system itself, but also attack the source segment can be hidden in any one place, which means its hidden high the prevention and treatment of common attacks or viruses as a single or as the preventive effect from the network gateway from the server system is not very good. Therefore, we propose an attack prevention strategies need to simultaneously start a three-pronged: Computer system security reinforcement, MAC- mapping table management, and network illegal packet detection. Fig.1 shows the framework of attack defend system.

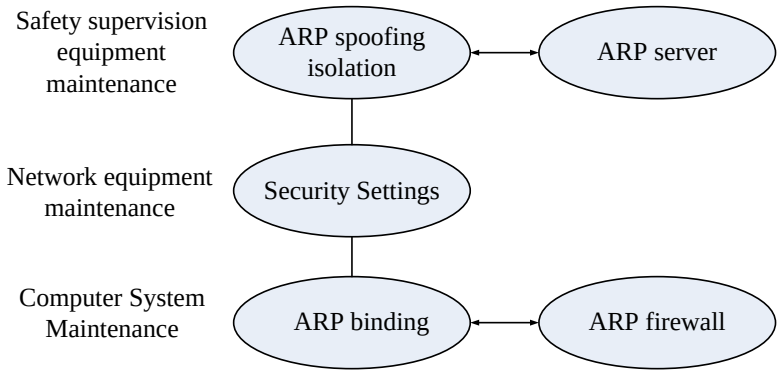

Fig. 1 The framework of attack defend system

System network port is connected to the switch mirror port to charge all packets, the system network interface into promiscuous mode, in order to meet the needs of multiple segments can be collected. Information system can be set to receive each data. System hardware platforms need to install multiple Ethernet ports for connecting the switch according to multiple routers under. Fixed system used to convert all dynamic static, thus effectively preventing the attacker to modify the entries. This method is relatively simple, as long as the device type in fixed command, the device will be the system converts all dynamic static [3].

Design Principles of Authentication Server

Authentication is a process of confirming a claimed identity. Authentication includes identity authentication and message authentication. The former is used to identify the users, and the latter is used to ensure the integrity and anti-repudiation of information communication parties. As openness and complexity of the network connection, authentication environments become more complex. Through a comprehensive analysis of network operation of various factors, authentication can be summed up under the network environment the following characteristics: Authentication means can't be achieved with single state; an attacker can tap authentication information of communication channel, intercept a legitimate user's identity and legal status impostor access network [4].

Therefore network authentication must be considered appropriate security means ,which are authentication integrity, non-repudiation of the information, replay attacks and transport security, also be considered to avoid the user's identity forgery, tampering, repudiation, posing, etc. authentication is the first hurdle of network security system, Authentication server includes two parts: control server and authentication server. The control server controls access and forwards packet for client requests; the authentication server completes the interaction between the client and authentication agent. Authentication Server stores decrypted private packet key RSA and user information, so its safety is very important. Fig.2 shows logical structure of the safety system.

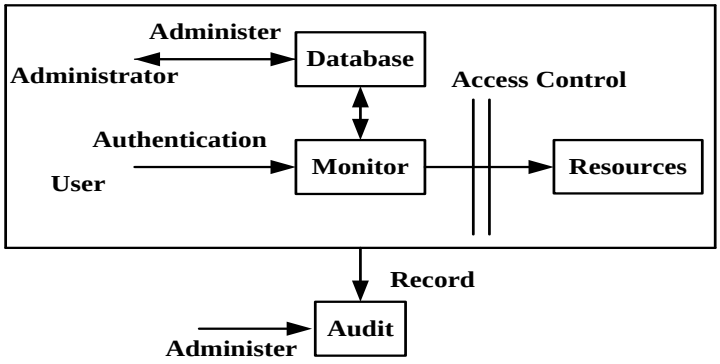

Fig.2.The Logical structure of the safety system

Before users access to network system, identity authentication system access the monitor determines whether users can access based on user identity and authorization database a resource. The user should be authorized by the security administrator to configure the database as needed. Audit in accordance with auditing system records the user's request and set behavior, while a non-real-time intrusion detection system in real time whether the intrusion. Access control and audit system relies on the "Information" of the authentication system, which is the identity of the user.

Protection Strategy of Computer Network Security

The network has brought us convenience, and the network information security issues. This will be based on the current computer networks, computer management explained the content classification, and analysis of the current computer network information security issues, propose appropriate protection strategies [5]. Towards a secure operating system, codes don't not belong to their own operating system must not become a secure operating system, because the system there is any backdoor or flaw that are unknown. The use of open source operating system is a good option, we use cropped Linux. Authentication server application develops with ANSI-C standard. Fig.3 shows the network structure of authentication server.

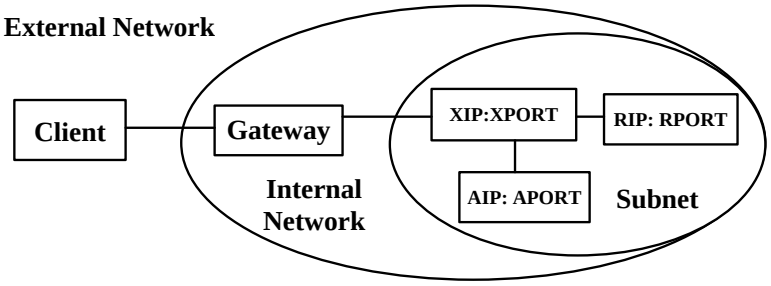

Fig. 3.The network structure of authentication server

XIP:XPORT represents network address and port of control server; RIP: RPORT represents the network address and port number of server which provides resources services (such as providing services for the HTTP port number is 80, FTP port number is 21, TELNET port number is 23) .AIP: APORT represents the network address and port of authentication server. Network divides into three parts: the external network, internal network and protected subnet. A firewall is the software between the computer and the network it is connected is located. The inflow and outflow of all computer network communications have to go through the firewall. Firewall network traffic flowing through it to scan, this can filter out some of the attacks, in order to avoid its being executed on the target computer firewall can also turn off unused ports, but it also prohibits a specific port out of communication blockade Trojans. Finally, it can block access from a particular site, thus preventing all traffic from unknown intruders, largely to protect the security of the network.

Data backup is the so-called useful files on the hard disk, the data are copied to another place such as mobile hard disk, etc., so that even if your computer is connected to the network being

attacked destroyed, as it has been backed up, so do not worry, then the desired file and copy the data back to it. Good data backup is one of the most direct and most effective measures to solve data security issues. Data encryption is the basic process of the original plain text files or data processed by an algorithm, making it unreadable piece of code, often referred to as "cipher text", it can only be entered after the corresponding key to shows that the contents have been through such a way to protect data from being illegally stolen, read the port.

The emphasis on network security, information technology solutions, but also must make great efforts to strengthen the use of network management personnel, pay attention to management and implementation, as many insecurities precisely reflected in the organization of the management or staff job entry, use, etc. side and, which in turn is a fundamental problem of computer network security must be considered. So, to take a practical approach, strengthen management, establish chapter formed to enhance security awareness of internal staff. In short, there are a lot of measures to address security alone one or several of them are very difficult to solve network security problems. In concrete work still needs full and multi-level security measures to maximize the safety and reliability of the network system, and the network system is more secure service for everyone to make a detailed network based on the actual situation.

Conclusions

With the continuous development of the network, computer network information security and protection is also beginning to be a widespread concern and attention. In this paper, along with the rapid development of network, the network information safety is becoming more and more attention. Based on the analysis of network information safety factors, and then put forward kinds of common computer network information safety protection strategy, and the development of the network information safety was prospected and formed the network information safety protection system. This means that the use of a certain kind of protective measures alone can’t ensure that the network information security, we must use a variety of comprehensive protection strategy, set director of public companies, in order to establish a network of information security protection system. Therefore, we protect the network information security have to be very careful to minimize the possibility of hacking, protect the security of network information.

References

[1] Testa Bridget Miatz. Zig Bec: Remote control euphoria [J]. Telecommunications (Americas Edition), 2004, 38(10): 10-11.

[2] AbadCL, Bonilla Ra. An Analysis on the Schemes for Detecting and Preventing ARP Cache Poisoning Attacks.27Th International Conference on Distributed Computing Systems Workshops, Toronto, Oct, 2007: 60.

[3] Matthew Connolly Mobilizing the Library’s Web Presence and Services：A Student-Library Collaboration to Create the Library’s Mobile Site and iPhone Application[J]. The Reference Librarian, 2011 (52):27-35.

[4] Daniel Chudnoy. A Mobile Strategy Web Developers Will Love[J]. Computers in 1ibraries，2010(5): 24-26.

[5] Brian T. John stone. Boopsie and Librarians: Connecting Mobile Learners and the Library [J]. Library Hi Tech News, 2011(4) N: 18-21.