Research on Computer Network Security Anti - attack

Liu Zheng Liang [1, a], LAI MIN[2, b]

[1]Gannan Medical University, Ganzhou City, Jiangxi Province

[2]Gannan Medical University, Gan zhou City, Jiangxi Province

Keywords: Network Security, Anti- Attack, ARP Defense System

Abstract: With the continuous development and improvement of computer technology in practical application, the computer network security requirements are gradually improved, and the understanding of information security connotation is continuously extended. It has expanded from the original information security integrity and reliability to the integrity and non-repudiation of information. Information security began to prevent, detect and evaluate security theory and technology. The network can't make it exposed to many dangerous effects, suffering from various types of adverse factors of attack, how to strengthen the prevention of computer networks more security and reliability has become an important issue we are discussing, based on the importance of computer network security The development of common network attack mode and mechanism, and the development of effective security prevention and control strategies, encryption strategy, to enhance the long-term security services of computer networks have a positive and effective role in promoting.

Theoretical Introduction of 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.

The expanding range of computer communication is in far beyond the jurisdiction of the local area network. Therefore, the data in transit is vulnerable to attack. On the entire data communication networks, data protect measures must be taken to include the communication itself confirmed the legitimacy and ensure the legality of the communication data in two ways. A network running, its large amount of data and information are stored in the host or terminal, external memory, how to prevent unauthorized users access is essential. Core ARP attacks is to send fake ARP response to the target host, and the target host receives the response mapping between IP and MAC forged, and thus updates the target host cache. [1].

In the actual computer network security management will often appear ARP attacks, such as IP address unauthorized use of the phenomenon, which not only affect the normal use of the computer network, but also due to address unauthorized use tend to have a higher authority, the enterprise unit caused a lot of economic losses and potential safety hazards, anti-ARP attack has become an important research field of computer network security. Physical security precautions are protected by computer systems, network servers, and other computer-related hardware facilities, mainly to prevent these hardware systems are subject to natural and man-made damage. In order to form a good physical security environment, the need to determine the user's identity, the use of authority, etc., to build an electromagnetic compatibility work environment, while the need to prevent the computer control room theft, destruction of the emergence of behavior.

Common Computer Network Attacks

Virus attacks for computer networks mainly refer to computer program instructions or code data that are artificially inserted into a process that can break down the computer's integrated functions and thus affect its normal use and can spread the virus by self-replicating. Although the types of

computer viruses are rich and varied, they all have some common characteristics, namely, fast propagation, high degree of concealment, comprehensive destructive and latent, and so on. At the same time, the mountain has different personality characteristics [2].

System vulnerabilities mainly refer to the computer software, hardware or protocol in the specific implementation or security policy in the construction of the shortcomings, so that an attacker can be unauthorized in the system through the vulnerability to access and damage. The foundation of building a computer network is TCP / IP protocol, which usually puts the efficiency first in the implementation process, and the security of the network system is not limited, which will inevitably lead to an increase in the amount of code, IP protocol operation efficiency of the service, the agreement in its own design process contains a large number of unsafe attributes. Although the computer network omnipotent, but the lack of effective security policy protection, due to the complexity of the configuration, the error rate is high, it is easy for hackers to find the vulnerability of the attack, these computer network can become lawless elements mainly steal and deceive the object.

In the computer network system, the spoofing attack mainly uses the TCP / IP protocol mentioned in the previous article. If the attacker uses the disguised identity to communicate with the attacked host, and sends the request to it, it will cause the system host to produce the wrong response operation even determines the attacker as a trusted object. At this point, the attack the main body can be posing, deceptive means to obtain the host trust into the central system, and reserve the back door for subsequent attacks, stealing use. According to different deception, counterfeit way, we can be divided into IP spoofing, e-mail spoofing, DNS spoofing and the source of mountain deception [3].

The Requirements Analysis of Defense System

The client is responsible packets received intercept capture ARP packets sent if it is going to be data extraction, and data detection, and if you find a local test fails, put the extracted data to the server and waits server response data. An IP address corresponds to a MAC address, in favor of the host within the network spoofing occurs when the easy management, due to the correspondence between the network IP address and MAC address list has been fixed, and it makes the operation to capture spoofing packets and implementation can be more easily. According to the characteristics of ARP virus hazards and communicate with users concluded the following functional requirements [4]. Fig.1 shows the requirements analysis of defense system.

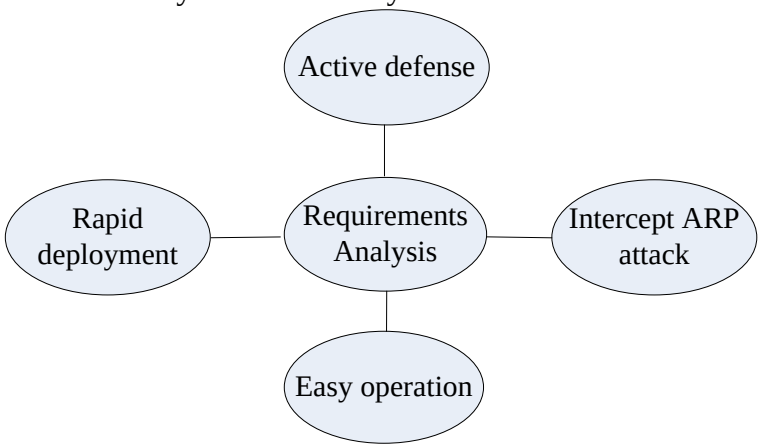

Fig. 1.The requirements analysis of ARP defense system

ARP defense system capable of rapid deployment, without changing the existing network topology: Such access device, you can continue to open networks. No need to install client software, we can solve the ARP attack and collect multiple network segments, a plurality of the ARP communication, in physical space permitting, to collect multiple routers under ARP communication. We can adapt to a variety of network environments, such as manually assign IP, automatic song Indian allocation of IP, can adapt to the frequent changes in network and IP hosts. It is easy to

operate, non-professionals, after simple training immediately after the operation: the research found that many enterprise network managers is non-professional, the situation is particularly serious in the various colleges and universities. Pinpoint ARP attack packets: you can distinguish between normal communication and ARP attack.

Intercept ARP attack: the system kernel level to intercept external fake ARP packets to protect the system against ARP spoofing, ARP attacks affect maintain smooth network and communications security; monitoring ARP cache. Automatic monitoring of the local ARP cache table, if found to be tampering with the MAC address of the gateway malicious programs; network antivirus necessary complement to the overall solution, the system only found responsible for blocking the attack, but does not involve the work of clearing the virus. We should be initiative to maintain communication with the gateway, the gateway advertise the correct MAC address, in order to maintain smooth network and communications security; tracing the attacker. After the discovery of aggressive behavior, according to the ARP packets in the data to lock the attacker IP address; ARP virus designed to kill. According to ARP virus signatures to scan for viruses; ARP cache protection. Prevent malicious tampering with the local ARP cache program

The Overall Design

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 ARP attack prevention strategies need to simultaneously start a three-pronged: Computer system security reinforcement, MAC-ARP mapping table management, and network illegal packet detection [5]. Fig.2 shows the framework of attack defend system.

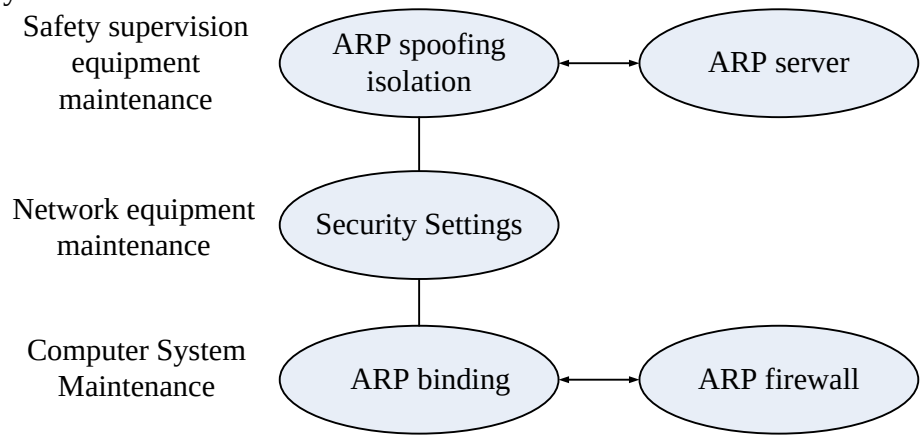

Fig. 2.The framework of ARP attack defend system

System network port is connected to the switch mirror port to charge all ARP 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 ARP, 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 ARP.

Network data, files, passwords and other information, in the transmission and storage process, the need for encryption means to improve the security level of information protection. Encryption prevention measures should be an important supplement to the access control precautions. For the openness of computer networks, it is easy to simplify the key management, facilitate digital signature and verification, and improve the efficiency of data encryption. You can use the electronic password technology, Algorithms and conventional cryptographic means to prevent unauthorized

access to users and malware placement. Specific methods of various means of comprehensive protection system are: setting a static MAC to IP mapping table, and prevent hackers refresh static conversion table. The network security relationship should not be established on the basis of the IP or MAC based on the trust relationship should try to build on the IP + MAC. Use MAC address management server. Isolate untrusted domains using a firewall internal network machines packet transmission. ARP cache on periodic polling hosts. Using ARP detection tools to detect illegal broadcast data frames on the network.

Conclusions

In recent years, all kinds of network attacks have become an increasingly prominent problem at the same time. Computer network security has become an important area of computer network technology currently exploring. In order to improve the reliability, confidentiality and completeness of computer network information effectively, we must proceed from the all-round and multi-angle research direction, deepen the understanding of the various risks and threats in the computer network, and develop different types of network attacks Effective anti-attack strategy, information encryption strategy and access control, public key strategy, can really make the computer network system to play a full application advantages and long-term service value. We need a variety of network attacks, including physical security precautions, access control precautions, improve the level of computer network security, and ensure that the computer network can operate in a relatively safe environment.

References

[1] CHEN Shan. Design of virtual reality roaming system based on Street View map service [J] .Computer & Digital Engineering, 2015,13 (6): 1121-1124.

[2] Tang Feifei, Automatic identification of martyrdom panorama interface smart home system controlled [J], Modern electronic technology, 2013, 36 (2): 32-35.

[3] Ouyang Pan, Li Qiang, Lu Xiuhui. Study and Implementation of Virtual Campus Development Based on Unity3D [J]. Modern Electronics Technology, 2013, 36 (4): 19-22.

[4] Xiao Jun, Huo Chao. Optimization of Virtual Mall Roaming System Based on 3DS MAX and VRP [J]. China Electronic Commerce, 2013, 11 (2): 61-62.

[5] YU Li-chao, ZHANG Xian-feng. Design and implementation of online virtual solar system roaming system based on Web-GL [J]. Computer and Information Technology, 2015, 23 (1): 49-53.