Analysis and Design on the Security Management Technology of the Confidential LAN

Haiyan Liu[1, a], Jiankang Yang[1, b] and Zeng Zhang[1, c]

[1]Department of Information Communication, the Army Academy of Armored Forces, Beijing 100072, China.

[a]lhy940@163.com, [b]health_y@163.com, [c]Zhangzeng9999@163.com

Abstract. On the basis of analyzing the security threats faced by hosts in a confidential LAN and the existing security measures, this paper designs a security management and control system for the network access control of LAN hosts. Based on the working principle and implementation details of the ARP protocol, this system realizes such functions as host registration, illegal host identification and illegal host disconnection, etc. The experimental tests show that this system can manage and control the network access behavior of LAN hosts.

Keywords: Confidential LAN, ARP, Intranet Security, Perimeter Security.

1. Introduction

The security threats faced by a host in LAN can be divided into two categories: penetration of attacks coming from the external network and threat posed by the internal hosts. Among them, threats from the intranet mainly refer to the attacks from other hosts on the same LAN and the intentional or unintentional misuse of the host's users. At present, many organizations have their own intranets, some of which are physically isolated from the Internet, and others use firewalls, filter routers or other technical means to connect to the Internet as to prevent malicious attacks from Internet. Perimeter security measures provide a certain degree of security for organizations. While, the statistics show that more than 80 percent security breaches coming from intranet, either intentionally or unintentionally. So intranet based technologies and measures are the key to the security of the LAN hosts.

The main security problems in LAN hosts can be summarized as follows [1, 2].

(1) Illegal access to the network. A host that does not belong to the network is connected to the LAN of an organization. Since it is not under control of the regular management, it may lead to information leakage, malicious code infections, or even damages to the various systems on the intranet. This kind of access is the most dangerous security threat of intranet.

(2) IP spoofing. A host counterfeits other host's IP addresses, engages in malicious acts without being tracked. Some internal users with malicious intention wish to not only access the resources of the whole network, but also not be responsible for their own actions, such as pseudonymous attacks, stealing information, interfering with information system on the network, etc.

(3) Illegal Extra-Connection. An internal host connects the external network through other channels. Because it evades the network monitoring of the internal network as well as the security filtering of the perimeter defence, it may not only cause internal information leakage, but also introduce external attacks and malwares.

(4) Using illegal removable devices on internal hosts. For example, using a removable storage device may threaten the host's information security by physically copying data, while using a serial port or a wireless port may provide an additional information transmission channels.

2. Security Measures Used in Confidential LAN

In order to protect the security of intranet hosts, many security management methods have been developed. According to where they are deployed, the existing LAN security measures can be

classified into three categories [2, 3], that is perimeter protection, network monitoring and host protection, as shown in Fig. 1.

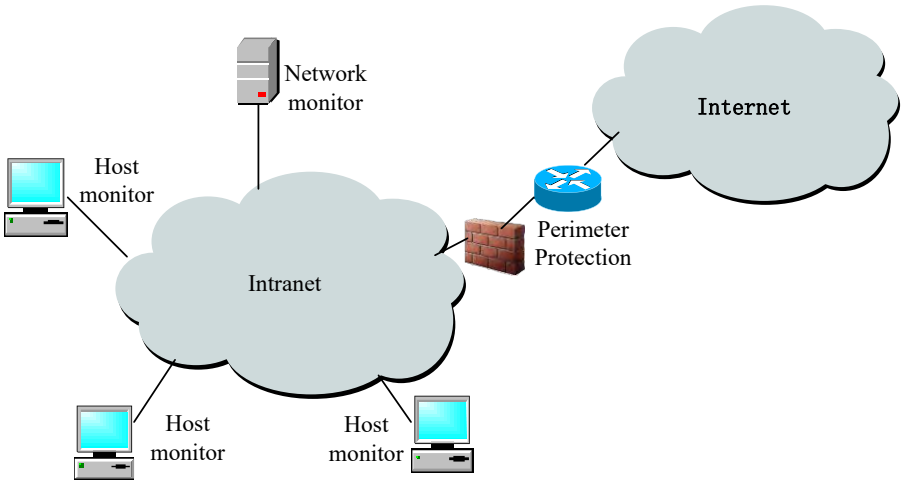

Fig. 1 Typical techniques used in a confidential LAN

(1) Perimeter protection

Perimeter protection refers to taking measures at the network boundary between the intranet and the external network to cope with the threats from the external network. Perimeter protection measures can be divided into physical isolation and logical isolation.

Physical isolation means that the internal network is completely separated from the external network at the boundary. Physical isolation breaks the way for outside attackers to utilize the network vulnerabilities to intrude, thus ensuring the security of the internal network. While at the same time it loses the convenience of communication, resource sharing and network collaboration brought about by the external network.

Logical isolation means that there are physical links between the internal network and the external network, but it uses firewalls, filter routers or other control measures at the border to control the access between the internal network and the external network. If the filter rules are set reasonably and properly, illegal access from outsiders to the internal network can be prevented, while at the same time legitimate access are permitted. However, the management and control policy as well as the implementation technique is very important, and the firewall or router themselves always become the target of intrusion.

(2) Network monitoring

In this approach, an intranet management and control server is placed in the intranet, which is responsible for the management of the behavior of all the intranet hosts. The content of management includes the registration of intranet hosts, the detection of illegal activities such as private connection of foreign hosts and spoof of addresses etc. Next sections will design and implement a LAN management and control system which belongs to this kind of measurement.

(3) Host monitoring

In this approach, the monitoring software is installed on each host of the intranet which monitors in real time any illegal activities on the host. Illegal activities of a host include the use of external devices, install or uninstall a software, etc. The former refers to using some removable device such as a USB storage device, CD-ROM, serial-parallel port device, wireless ports device, etc. Some kinds of software are crucial to security, such as virtual machine software, remote management software, etc. because they can provide some new information transmission channel. Since some malicious code may be installed without notice of the users, so any install or uninstall of some software should be logged and audited. Host monitoring can also detect any illegal out connection of a host. By sending detection packages to outside network, it can detect whether there is a network channel that bypasses the internal network management and control and perimeter protection measures.

3. Design of a Security Management and Control System

In this paper, a security management and control system is designed for the confidential LAN, which monitors as well as controls the network access of all the hosts on the LAN. The system consists of three main components: legal host registration, illegal host identification and illegal host processing. The legal host registration is further divided into scanning registration, manual registration and registration editing. Next section will give the details of this design.

(1) Scanning registration

The management and control system continuously sends broadcasted ARP request packet to the hosts within the specified range, requesting the MAC address of a target host. After receiving the request, the target host packs its IP and MAC addresses into ARP reply packet and sends back. The system then extracts the IP and MAC information from the response packet. After being confirmed by the administrator, these results can be stored in the registered host database.

(2) Manual registration

The administrator manually inputs the IP address and the corresponding MAC of the specified host and adds it to the registered host database.

(3) Registration editing

Administrators modify or delete the existing information in the registered host database.

(4) Illegal hosts identification

The management and control system sends ARP request packets regularly and scans the online hosts in the intranet. The scanning results are compared with the information stored in the registered host database to determine whether it is normal. If the corresponding relationship between an IP and MAC changes, it is further determined whether there is an external host or the internal host counterfeited its IP address.

(5) Illegal hosts processing

To the illegal hosts, the management and control system will counterfeit some ARP packets, make it disconnect from the network. Due to the inherent aging mechanism of the ARP caches, this deceiving process should be done continuously before being manually stopped.

4. Implementation of the Security Management and Control System

Since it is needed to construct specific packets, capture and parse the contents of received packets, So *WinPcap*[4] development package is used. At the same time, *vs.net* is used to develop the main control program and *Access* is used to store the registered host database. Next section will illustrate the implementation of some key functions.

4.1 Implementation of the Database

A table named *RegHosts* is created in the database. The fields of the tables include *IpAddr*, *MacAddr* and *Regtime*, which store the IP address, MAC address and registration time of the host separately. The illegal host tables *OutHosts* include *MacAddr*, *IPAddr* and *IllegalType* fields, which store IP address, MAC address and illegal type respectively.

4.2 Implementation of Scanning Registration Module

The scanning registration module is realized by multi-threading mechanism. The main thread is responsible for sending broadcasted ARP request packets to hosts within a specified range, which contains its own IP address an, MAC address, as well as the IP address of the target host to be requested. The main codes for constructing a broadcasted ARP requesting packet and sending it is as follows:

```
EthernetHeader eh; //Ethernet frame head
Arpheader ah; //ARP request packet had
struct pcap_pkthdr * pkt_header;
const u_char * pkt_data;
memset(eh.DestMAC, 0xff, 6); //Destination of the frame is the broadcast address
memcpy(eh.SourMAC, local_ip_mac, 6);//source of the frame is the system itself
memset(ah.DestMacAdd, 00, 6);    //the MAC to be requested is set to zero
memcpy(ah.SourceMacAdd, local_ip_mac, 6); //the source MAC
```

```
for (int i = startip; i <= endip; i++) {//to each host in the specified range
    ah.DestIpAdd = htonl(i);    //destination IP address
    memset(sendbuf, 0, sizeof(sendbuf));
    memcpy(sendbuf, &eh, sizeof(eh));
    memcpy(sendbuf + sizeof(eh), &ah, sizeof(ah));
    if (pcap_sendpacket(adhandle, sendbuf, 42) == 0) ...//send the frame
}
```

The receiving thread captures ARP reply packet based on *winPcap*, parses the packet to extract IP address and MAC address. The process of receiving and extracting is described as follows:

```
if ((res = pcap_next_ex(adhandle, &pkt_header, &pkt_data)) >= 0) {//capture a packet
    if (*(unsigned short *)(pkt_data + 12) == htons(ETH_ARP)) {// a Ethernet frame
    ArpPacket *recv = (ArpPacket *)pkt_data;      //the ARP head
    if (*(unsigned short *)(pkt_data + 20) == htons(ARP_REPLY)) { //ARP reply
        strIp.Format("%d.%d.%d.%d",recv->ah.SourceIpAdd & 255,
        recv->ah.SourceIpAdd >> 8 & 255,recv->ah.SourceIpAdd >> 16 & 255,
        recv->ah.SourceIpAdd >> 24 & 255); //extract the IP address
        for (int i = 0; i < 6; i++) Mac[i] = *(unsigned char *)(pkt_data + 22 + i); //extract MAC
        strMac.Format(_T("%02x-%02x-%02x-%02x-%02x-%02x"),
                Mac[0], Mac[1], Mac[2], Mac[3], Mac[4], Mac[5]);
        ……}}}
```

When displaying the scanning result, the receiving thread uses the message mechanism to synchronize with the displaying thread.

```
pDlg->PostMessage(RECV_ARP, (WPARAM)(LPCTSTR)strIp, (WPARAM)&mc);
WaitForSingleObject(hPauseHandle,INFINITE);
ResetEvent(hPauseHandle);
```

When the administrator stops the scanning, the receiving thread should be terminated at the same time, and then add all the host information displayed in the list to the registered host database.

The manual registration module provides the input interface of IP address and MAC address, and then adds it to the *RegHosts* table in the database. If there is already some information about that MAC address in the database, the original information will be overwritten.

4.3 Implementation of Illegal Hosts Identification Module

After the monitoring function is started, the system sends serious of ARP request packets regularly. At the same time, the monitoring thread is started to continuously capture the ARP packets, and the IP/MAC addresses in the packets are compared with the information stored in the registered host table to detect whether there are some new hosts or the IP/MAC corresponding relationship has changed. The process flow of listening threads is shown in Figure 3. This monitoring process will continue regularly until it is stopped by the administrator.

4.4 Implementation of the Illegal Hosts Processing Module

To deal with those illegal hosts, ARP spoofing technology is used to make the target host disconnect from intranet. Since the ARP cache of the host will refresh automatically after 2 minutes, so this system uses a timer. As long as it does not receive the cancel command, it will send the package to the malicious host regularly to prevent the malicious host from automatically refreshing its ARP cache.

After the malicious host is selected and the dealing command is started, the timer is started. When the processing is stopped by the administrator, the timer is terminated. In the timer procedure, forged ARP reply packets are constructed and sent to the selected host. The process of constructing ARP reply package is similar to that in section 4.2, but the source IP address is the gateway's address while the source MAC address is the address of the management and control system.

5. Summary

The ARP protocol is a necessary protocol for frame transmission in a LAN. This paper designs a security management and control system based on the principle of the ARP protocol. By sending ARP requests and capturing the response packets, it can discover all the hosts connected to the LAN network. By the pre-registration and the realtime scanning mechanism, it can find out the hosts

unregistered or those with the counterfeited IP. By using ARP deception method, it can make the illegal hosts disconnect from the LAN. Deployed on a centralized server, this system can manage and control the access of all the hosts on the LAN. Because of the limitation of its location, this system could not detect or control the illegal outreach and illegal use of peripherals. To achieve these kinds of protection, it is necessary to set up some detection functions on the host.

References

[1]. Liu Haiyan, Yang Zhaohong, Huo Jinghe. On the Detection and Analysis Techniques of the Intranet Security. COMPUTER ENGINEERING &SCIENCE. Vol.31 (2009) No.9, p.11-35.

[2]. Lin Congjie. Research on Risk Analysis and Security Strategy of Secret-related LAN. Electronics World. 2014(17), p.173-174.

[3]. Zhang Di，Chen Weiliang, Wang Bo. Analysis of Computer Network Security Technology Based on LAN Environment. Network Security Technology and Application. 2018.07. p.20-22.

[4]. Winpcap manuals. https://www.winpcap.org/docs/default.htm. 2018.05.