Research of the ARP Spoofing Principle and a Defensive Algorithm

YANG LIU, KAIKUN DONG, LAN DONG, BIN LI
Department of Computer Science & Technology
Harbin Institute of Technology at WEIHAI
Harbin Institute of Technology at WEIHAI, No.2, WENHUA West Road, Weihai, Shandong, 264209
P.R CHINA
lyyl2322@126.com, dkk@pact518.hit.edu.cn, hitlan@126.com, libin@pact518.hit.edu.cn

Abstract: - During the network communication process, attacker carry on ARP spoofing by using the disadvantage of the ARP(Address Resolution Protocol) protocol, this phenomenon is seriously threaten the LAN security. This paper will introduce the commonly used ARP spoofing methods such as internal/external network sniffing, interception, malicious attack and so on. It presents the Matching IP method, Data monitor method, Echo time method, ARP response analysis method, software tools detecting method as well as the new method of ARP cache updating, using switching equipment to control and other strategy and presents the algorithm to keep ARP spoofing away and maintain network security.

Key-Words: - ARP spoofing, interception, monitor, MAC, sniffing, guarding algorithm

1 Introduction

In Ethernet, when both sides of communication is sending message they will need not only the network logical address but also the network physical address. So it presents a problem how to get the MAC address based on IP address, ARP protocol is used for processing this problem[1]. The ARP table will keep the reflection between the IP and MAC address and is updated unceasingly. The network attacker using several spoofing method to attack the network by the disadvantage of the ARP protocol and it has seriously threaten the network security, This paper has analyzed the spoofing method as well as detecting method in detail and presents an effective guarding algorithm.

2 ARP spoofing principle

ARP protocol is based on the mutually trust, it is a stateless protocol. The request way of ARP is by broadcasting, each host that does not receive the request can send out ARP response package randomly, when ARP buffer without authentication mechanism received the ARP response it will dynamic updating the cache directly, the above all provide the spoofing condition. ARP spoofing mainly gets following types:

2.1 Sniffing

Sniffing is that the attacker insert itself between the two communicating host to obtain the message, to prevent the communication halt the attacker will retransmit the message between the two hosts ceaselessly[2,3,4]. There are two kinds of sniffing: internal network sniffing and external network sniffing.

2.1.1 External network sniffing

When including a sub-subsection you must use, for its heading, small letters, 11pt, left justified, bold, Times New Roman as here.

Assuming host A and host B are in the same network and will communicate with each other, the host C is out of the network, Illustrated in Fig.1

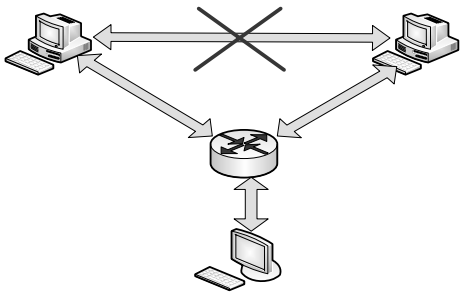

Figure.1 External network sniffing

If the attacker C wants to sniffing the communication content between host A and host B, it must pass the router. Considering the message survival time from inside net to outside net, the attacker modifies its TTL of IP grouping to make sure it has enough time sending out response package to the destination host. The host C send out

ARP response package to host A. The format of the package is as Table1:

Table 1 ARP response package send to host A

Source MAC address	Source IP address	Destination MAC address	Destination IP address
0C-1C-2C-3C-4C-CC	10.1.1.200	0A-1A-2A-3A-4A-AA	10.1.1.100

When host A receives ARP response package it updates buffer, after being spoofed host A send message to host B by the MAC address of attacking host C. ARP is a LAN(Local Area Network) protocol, for host is external network so host A can not send message to router, at this time host C will update the routing table of host A through ICMP(Internet Control Message Protocol), it send the message which should send to host B fist to router and then retransmit to attacker. So attacker realizes the sniffing by this process. So does host B

2.1.2 Internal network sniffing

Assuming that host A will communicate with host B, the attacker C will sniffing the content of the communication. Illustrated in Fig.2

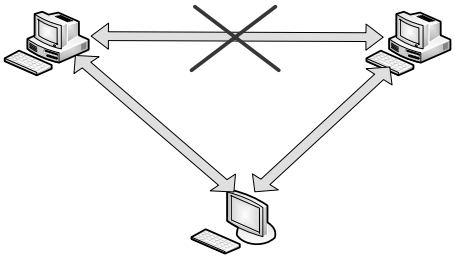

Figure.2 Internal network sniffing

Based on knowing the IP address the attacker C can get the MAC address of the host by collecting ARP request/response message or by the PING command of ICMP protocol. The host set NIC(Network Interface Card) as promiscuous state with retransmitting function[5,6,7]. The host C will carry on ARP Spoofing and send response package to host A. The format of the package is as Table 2:

Table 2 ARP response package send to host A

Source MAC address	Source IP address	Destination MAC address	Destination IP address
0C-1C-2C-3C-4C-CC	10.1.1.200	0A-1A-2A-3A-4A-AA	10.1.1.100

For the disadvantage of the ARP protocol, the host A will receive the response package constructed by host C and update the ARP buffer, to avoid spoofing failure, host C must send out ARP response package ceaselessly to keep proofing. With the same principle host C send out ARP response package to host B. The format of the package is as Table 3:

Table 3 ARP response package send to host B

Source MAC address	Source IP address	Destination MAC address	Destination IP address
0C-1C-2C-3C-4C-CC	10.1.1.100	0B-1B-2B-3B-4B-BB	10.1.1.200

The communication between host A and host B is interdicted by the attacker, the attacker can receive and retransmit the message of both sides without detecting.

2.2 Interception

Based on the internal/external network sniffing, if the attacker C camouflage host A and send wrong message to host B to intermit link, then host B can not communicate with host A, thus attacker can communicate with host A as host B to achieve the interception goal.

2.3 Malice attacking

The attacker sends response package to all the ARP request, it fill in the same inexistent MAC address in the response package cause that the host can not find the address of destination host[8,9], so the communication is stopped. The attacker send ARP response package with inexistent MAC address to the destination host, thus the destination host have to update the ARP buffer, the destination will lose its response package after receiving the message from other host and can not maintain the communication[10,11,12].

The attacker sends response package to all the ARP request, it fill in the same inexistent MAC address in the response package, this lead to a great deal of data flowing to the gateway and aggravate the load of the gateway causing network jam and cause communication interrupt.

3 ARP spoofing detecting

ARP spoofing has seriously threaten the network security, we can detect whether network gets ARP spoofing by detecting reflection between IP address and MAC address in local ARP buffer. Now there existing the several detecting methods as follows:

3.1 The method of Echo time

Usually, the hosts that carry on the ARP beguilement all establish the network card in mix pattern, the aggressor can obtain the correspondence

10.1.1.100
0A-1A-2A-3A-4A-AA

10.1.1.200
0B-1B-2B-3B-4B-BB

information of the man who was aggressed under this kind of pattern, so the system can give the network which doubted have the ARP beguilement behavior to send out a great deal of garbage, according to judge Echo time of the host inside the net, the normal system's Echo time response little change, because of wanting to handle a great deal of garbage information, so carrying on the ARP beguiling system, the Echo time will change greatly.

3.2 The method of IP matching

When host receives the ARP request, it will check the IP address in the request frame and IP address of the host, if they are the same there may be other host spoofing. The host can also send out request package to check its IP address periodically, if the IP address received is the response frame of host IP address there also maybe other hosts spoofing.

3.3 The method of ARP answer analysis

According to the mechanism of ARP spoofing, aggressors who want to maintain cheat, have to send out the report text of the ARP beguilement repeatedly and continuously. The system can wiretap the report text inside the net, if the system detected lots of frames which without the ARP answer, it can examine the existence of the ARP beguilement.

3.4 The method of data frame detecting

Although the spoofing ARP response package does not leave the address of the attacker, the ARP response frame contains the address of the attacker. In the normal condition the source MAC address and destination MAC address in the head of the frame should match the ARP message in the data package of frame, if not the spoofing maybe exist.

3.5 The method of software examination

Using the software tools to check the relation ship between IP address and MAC address such as Enthereal, NetWatch, NETCM, ARPwatch etc[9].

4 Guard against ARP spoofing

4.1 ARP cache updating method

For the ARP protocol receiving ARP response and updating the cache without ARP request, this has create the ARP spoofing condition, so we can formulate the ARP cache updating rules. It stipulate that the sequence of receiving ARP protocol is fist sending out ARP request then receiving the matching ARP response package, these non-response or non-matching response package will be deleted, this can prevent the ARP spoofing efficiently.

4.2 Configure the static ARP cache

One important precondition of ARP spoofing is that the ARP cache is dynamically changed, if the network manager makes a registration of IP address and MAC address and prevent the dynamically ARP cache updating. When the spoofing ARP response to the host it can not update the ARP cache, so it can not achieve the goal of spoofing. But the expense is bigger and easy mistaking.

4.3 Controlling with switching equipments

Using the switchboard can make the physical of network into subsection, and bind the IP address with the MAC address statically, the switchboard will compare the source address to the port report of the source address information when a port received the message, if changes occurred, then forbids automatically to the port until the conflict solved. Making use of the insulation function of the router, make the ARP beguilement can't across the net segment to attack the server.

4.4 Information encryption

Based on the ARP spoofing theory, Sniffing is difficult to be checked. If both of the communication side encrypted the message, even though the message was caught by the attacker it can not get the useful message without the decryption algorithm, so it guarantees the network transmitting security.

4.5 Checking the ARP cache periodically

The network manager catch the ARP request and the ARP response periodically, check the reliability of the ARP response, Taking turns periodically, check the reflection between the host's ARP cache IP address and the MAC address.

5 The guarding algorithm for ARP spoofing

The ARP spoofing is usually through modifying the ARP request/response package or updating the ARP buffer to achieve spoofing,

The above guarding methods against the ARP spoofing have their limit, so we present a kind of arithmetic against the ARP spoofing. This arithmetic via the received ARP request/response to restrict the modification to the ARP cache, it can

prevent spoofing effectively which has already passed the confirmation.

The development environment of the algorithm is Vc++6.0, WINPCAP and MFC Classes. On the lower level it use WINPCAP catching package mechanism, after catching a package by WINPCAP then analysis its structure, the structure of its frame head is as follow:

```
struct ether_header
{ u_int8_t ether_dhost[6];
// Destination MAC address of data frame
u_int8_t ether_shost[6];
// Source MAC address of data frame
u_int16_t ether_type; };
```

The algorithm is described by natural language and C language

```
if(ntohs(ether_protocol->ether_type)==0x0806)
//ARP packet
void ARPRequest ()
{ GetIpNetTable() //read  ARP cache
 if(have MAC-IP mapping)
{if( in ARP cache IP==arp_protocol ->arp_source_ip_address )
        {Send_ARP_Response();}
else if(have the same MAC and in ARP cache source IP != arp_protocol->arp_source_ip_address)
{if(ether_protocol-> ether_shost !=arp_protocol-> arp_source_ethernet_address)
 {  Droppacket();
NoSetIpNetEntry();
//didn't refresh ARP cache;}
 else
{use arp_protocol->arp_source_ip_address
 obsequent resolution MAC of sender;
     if(requester's MAC==arp_protocol->
     arp_source_ethernet_address)
      {        SetIpNetEntry();
       // refresh ARP cache
      Send_ARP_Response(); }
   else
      {  Droppacket();
        NoSetIpNetEntry(); }}}}
      else if （haven't MAC-IP mapping）
       {if(ether_protocol->
          ether_shost!=arp_protocol-
            >arp_source_ethernet_address)
        {  Droppacket();
          NoSetIpNetEntry();}
         else
         { use arp_protocol->arp_source_ip_
              address obsequent resolution MAC
              of sender;
          if(requester's MAC==arp_protocol->
           arp_source_ethernet_address)
                { SetIpNetEntry();
                  Send_ARP_Response();}
           else
                {  Droppacket();
                 NoSetIpNetEntry();  }}}}
                 void ARPResponse ()
{The processing is just as ARPRequest ()}
```

6 Conclusion

The aggressor usually makes use of the ARP protocol's " stateless " characteristics to carry on the ARP beguilement, and cause great harm to the security of networks, the examine method and prevention strategies of the ARP Spoofing that I mentioned before have different scope and limitations, this article by a guard against deception algorithms, the algorithm can be achieved to prevent functional efficiency is not satisfactory, and random algorithms to consider acceding to the future efficiency of algorithms. To fundamentally solve the ARP Spoofing is more difficult, it needs to consider integrate the technology and the management in the actual network environment to minimize the risks posed by ARP Spoofing.

References:

[1] J. Lach, "Sniffing local network and its detecting", *Studia Infor-matica*, Vol.2, No.24, 2003, pp. 289-296.

[2] Chin, Tan Saw, Singh Y P. Single-hop wavelength assign- ment using an ant algorithm in WDM MESH network .*WSEAS Transactions on Computers*. Vol.5, No.7, 2006, pp. 294-300.

[3] Wenbing Zheng, Chenzhong LI, "AN Algorithm Against Attacks Based on ARP Spoofing", *Journal of Southern Yangtze University(Natural Science Edition)*, Vol.2, No.6, 2003, pp. 167-1696.

[4] Z. H. Tian, B. X. Fang, B. Li, et al. Avulnerability-driven approachto active alert verification for accurate and efficient intrusion detec-tion. *WSEAS Transactions on Communications*. Vol.4, No.10, 2005, pp. 1002-1009.

[5] Qinghua Deng, Songqiao Chen, "ARP Spoofing and Countermeasures", *Microcomputer Development*, Vol.8, No.14, 2004, pp. 215-217.

[6] W. Richard Stevens, *TCP/IP Illustrated(Volume1:The Protocols)*, Addison-Wesley, 1994.
[7] G. Malkin, *ARP Extension-UNARP*, RFC 1868[S], Nov, 1995.
[8] Mohd Dani Baba, Nurhayati Ahmad, et al., PERFORMANCE EVALUATION OF TCP/IP PROTOCOL FOR MOBILE AD HOC NETWORK. *WSEAS Transactions on Computers*, Vol.5, No.7, 2006, pp. 1481-1486.
[9] Mohamed G. ouda, Chin-Tser uang, "A secure address resolution protocol ",*Computer Networks*, Vol.1, No.41, 2003, pp. 57-71.
[10] V. Ramachandran, S. Nandi, "Detecting ARP spoofing: An active technique ", *LECTURE NOTES IN COMPUTER SCIENCE 3803*, 2005, pp.239-250.
[11] J. Koo, et al, "Evaluation of network blocking algorithm based on ARP spoofing and its application", *LECTURE NOTES IN COMPUTER SCIENCE 3480*, 2005, pp.848-855.
[12] K. Kwon, S. Ahn, "Network security management using ARP spoofing", *LECTURE NOTES IN COMPUTER SCIENCE 3043*, 2004, pp. 142-149.