Research on Preventing ARP Attack Based on Computer Network Security

Mei Guo, Min Xiao* and Hui Xie

College of software and Communication Engineering, Xiangnan University, Chenzhou, 423000, China

*Corresponding author e-mail: xnxyxm@163.com

Abstract. The continuous development and wide application of computer technology are conducive to the realization of the sharing of social resources and information, and provide greater convenience for the development and improvement of all walks of life in society [1]. However, with the development of society, computer network security has also received more attention. Today, computer network security has become an important area of the computer network engineering technology. A major security threat to network security is the ARP attack. This paper describes the principle, working process, attack hazards, and performance of attacks after ARP. Protection against ARP attacks.

1. Introduction

ARP attack is the main threat to computer network security. How to protect computer network security and prevent it from being subject to ARP attack has become a problem that must be studied and solved for full network management.

2. ARP Principle

ARP is an abbreviation of Address Resolution Protocol. It is a protocol for determining the physical address of a host when it only knows the IP address of the host. The core idea of the ARP principle is to send a fake ARP reply to the target host, and make the target host receive the mapping pair between the forged MAC address and IP address in the reply to update the target host ARP cache.

Assume that host C is an attacker who implements ARP spoofing. Its purpose is to intercept the data exchanged between host B and host A. Host C already knows the IP addresses of A and B before implementing ARP spoofing. At this time, C sends an ARP packet to obtain the MAC address of host B, and then sends an ARP Reply packet to B. The source IP address is the IP address of A, but the source MAC address is the MAC address of host C. After host B receives the ARP reply, it updates the ARP cache according to the new IP address and MAC mapping pair. After that, when B sends a packet to A, the destination MAC address will use the MAC address of C. Therefore, the switch forwards the packet to the port where attacker C resides based on C's MAC address. In the same way, attacker C sends ARPReply to make sure that host A has the MAC address of host B as C's MAC address. While sending fake ARP Reply intermittently, attacker C turns on the routing function of the local host and forwards the hijacked packet to the correct destination host. At this time, the attacker is completely transparent to hosts

A and B. There will be no exceptions, but in reality the data packet is illegally intercepted by C, and attacker C becomes a "middleman." [2]

3. ARP Working Process

Assume that the IP address of host A is 192.168.1.1 and the MAC address is 0A-11-22-33-44-01; the IP address of host B is 192.168.1.2, and the MAC address is 0A-11-22-33-44-02. When host A wants to communicate with host B, the address resolution protocol can resolve host B's IP address (192.168.1.2) to host B's MAC address. The following is the workflow:

3.1. A host matches the MAC address

Host A identifies the IP address of host B to be accessed by identifying the information in the routing table. Subsequently, host a searches its own local ARP cache, looks for a MAC address matching host B in these caches, and then establishes a connection.

3.2. Through ARP Request

If host A does not find a mapping in the ARP cache, it will query the hardware address of 192.168.1.2 to broadcast the ARP request frame to all hosts on the local network. Source host A's IP address and MAC address are included in the ARP request. Each host on the local network receives an ARP request and checks whether it matches its own IP address. If the host findsThe IP address cannot be used directly for communication. This is because the IP address is simply the address of the host in the abstract network layer. If you want to send the datagram sent in the network layer to the destination host, it will be transmitted to the link layer and then converted into a MAC frame before it can be sent to the actual network. Therefore, no matter what protocol is used in the network layer, the hardware address must be used finally when transmitting data frames on the actual network link [3].

Since the IP address has 32 bits and the LAN hardware address is 48 bits, there is no simple mapping relationship between them. In addition, new hosts may be added on a network, or some hosts may be withdrawn. Replacing the NIC also changes the host's hardware address. It can be seen that a mapping table from the IP address to the hardware address should be stored in the host, and this mapping table must also be dynamically updated. Address Resolution Protocol ARP solves these problems well. That the requested IP address does not match its own IP address, it will discard the ARP request.

3.3. Add ARP cache

The ARP cache (or ARP table) is the key to the efficient operation of the ARP address resolution protocol. (If there are multiple ARP responses, the last one will prevail.)

ARP makes a dynamic mapping between IP addresses and MAC addresses. That is, it caches an ARP table and associates the obtained IP address, it will be sent. Broadcast to find. With the use of the user, if the ARP table does nothing, it will become more and more bloated and slow, which reduces the efficiency of network data transmission. Therefore, each item in the ARP cache is set to have a lifetime, which is generally 20 minutes. , calculated from the time it was created, cleared when it is timed out, and if it is used again during the time period, the time is reset.

In addition, we can view the Arp table through the Arp command, as shown in Figure 1 below.

```
[windeal.li@dnixm ex7300-buildroot]$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.20.12            ether   00:18:7d:1f:e6:9c   C                     eth0
192.168.20.1             ether   e0:05:c5:73:03:ec   C                     eth0
192.168.20.22            ether   00:18:7d:1f:e5:ce   C                     eth0
192.168.20.13            ether   00:18:7d:1f:e5:b6   C                     eth0
192.168.20.21            ether   84:2b:2b:50:f2:b1   C                     eth0
[windeal.li@dnixm ex7300-buildroot]$
```

Figure 1. Checking ARP Tables through ARP Commands

The ARP table records some mappings between IP addresses and physical addresses. In the Arp table, we can see a Flags field with C, M, and P values:

C: indicates that the Arp entry is dynamically obtained through ARP request (general time is 20 minutes)

M: Indicates that the Arp entry is manually set.

P: indicates Publish, indicating that the ARP entry can be used to restore ARP requests from other hosts. (For ARP proxy)

3.4. Host B Reply Message

After receiving the message sent by host a, host B directly responds to the message through the MAC address.

3.5. Update ARP Cache

After host B replies to host A's message, host B's IP synchronizes the ARP update cache. The result of this cache is a lifetime, and the above process will be repeated after the lifetime expires. Host B determines that the MAC address is a prerequisite for host A to send a message.

4. Attack Hazard

The machine can modify the address translation table before the cache memory updates the table entry to implement the attack. The ARP request is sent in broadcast mode. It will also cause traffic redirection, and all data will pass through the attacker's machine. Therefore, there is a great security risk.ARP spoofing can cause the communication between the target computer and the gateway to fail. It will also cause traffic redirection, and all data will pass through the attacker's machine. Therefore, there is a great security risk. In the ARP virus, computers in the entire LAN attack each other. In other words, computers in the entire region have been affected. Computers with no problems will also be infected because of the related links.

5. POST-ATTACK Performance

The poisoning phenomenon of ARP spoofing Trojans is as follows: When using a local area network.IE browsers frequently make mistakes, and some common software problems occur [4]. If the LAN is authenticated through the Internet, authentication may suddenly occur, but it cannot be accessed through the Internet (the gateway cannot be pinged). After the machine is restarted or the command Arp -d is run in the MS-DOS window, Internet access can be restored.

ARP spoofing Trojan horses can successfully infect only one computer, which may result in the entire LAN not being able to access the Internet. In serious cases, it may even cause paralysis in the entire network. In addition to the intermittent occurrence of other users on the same LAN, the Trojan will also steal user passwords. Such as stealing QQ passwords, stealing various online game passwords and accounts to make money transactions, and stealing online bank accounts to do illegal trading activities, etc. This is a Trojan horse's usual trick, causing great inconvenience to users and a huge economy. Loss.

Based on this working characteristic of the ARP protocol, the hackers continuously send fraudulent ARP packets to the other computers. The packets contain duplicate MAC addresses with the current device.As a result, normal network communication cannot be performed. Under normal circumstances, there are two kinds of phenomena in computers that are attacked by ARP:

The dialog box “Conflicts between 0-255 hardware address of the machine and 0-255 address conflict in the network” pops up continuously.

The computer cannot access the Internet normally and there are symptoms of network interruption.

6. ARP Attack Prevention Strategies

6.1. Double-binding measures

Double-tied is an IP-MAC binding method on both the router and the terminal. It can restrict the ARP spoofing, forging gateways, and intercepting data. This is a precautionary measure taken from the

principle of ARP fraud, and it is the most commonly used method. It is effective against the most common ARP spoofing. However, the disadvantage of double tying lies in three points: 1. Static binding on the terminal is easily destroyed by the upgraded ARP attack. An ARP-d command of the virus can completely disable the static binding. 2. It is time-consuming and laborious to do IP-MAC binding on the router, which is a tedious maintenance work. 3. Double tying only allows the computers and routers at the two ends of the network not to receive relevant ARP information, but a large amount of ARP attack data can still be sent out, and they must be transmitted on the internal network, which greatly reduces the transmission efficiency of the internal network [5].

Therefore, even though double tying was once the basic measure of ARP prevention, because of the limited prevention capability and management, it is now more and more limited.

6.2. ARP Personal Firewall

In some antivirus software, the function of ARP personal firewall is added. It binds the gateway on the terminal computer to ensure that it is not affected by the fake gateway in the network, so as to protect its own data from being stolen. The ARP firewall has a wide range of applications. Many people think that there is a firewall. ARP attacks do not pose a threat. In fact, this is not the case. Figure 2 below is the common personal firewall setup.

Figure 2. Personal Firewall

The ARP personal firewall also has a big drawback:

1, it can not guarantee that the bound gateway must be correct. 2, ARP is a problem in the network, ARP can forge gateways, but also intercept data, is a "double head strange."

Therefore, the ARP personal firewall does not provide a reliable guarantee. Most importantly, it is a measure that has nothing to do with network stability. It is personal, not network.

6.3. VLAN and Switch Port Binding

Dividing VLANs and switch port bindings to prevent ARP is also a commonly used defense method. The approach is to carefully divide VLANs, reduce the scope of the broadcast domain, and make ARP work in a small area, without having a large area of influence. At the same time, some network management switches have the function of MAC address learning. After the learning is completed, this function can be disabled to bind the corresponding MAC address and port. This prevents the virus from using ARP attacks to alter its own address. That is, the risk of intercepted data in ARP attacks is lifted. This method can indeed play a role.

However, the problem with VLAN and switch port binding is: 1. there is no protection for the gateway. 2. Each computer is firmly fixed to a switch port. This management is too rigid. 3. The cost of the entire switching network is greatly increased.

Because the switching network itself is an unconditional support for ARP operations, that is, its own loopholes may cause ARP attacks. The management means above it is not for ARP. Therefore, implementing ARP protection measures on existing exchange networks belongs to the shield of the child. And the complex operation and maintenance is basically a thankless task.

7. Conclusion

Through the analysis of the four universal ARP prevention methods in the article, we can see that there are problems with the existing ARP prevention measures. This is the reason why ARP has been thoroughly studied even though it has been studied for a long time, but it is still the reason why it cannot be completely solved in practice. All in all, it is difficult to prevent ARP attacks. Modifying the protocol is also unlikely. However, there are some jobs that can improve the security of the local network.

Acknowledgments

This paper is funded by Project of:

1. Scientific Research Fund of Hunan Provincial Education Department, Research on database storage performance optimization in virtualization, (No. 16C1498)
2. School level scientific research project of XiangNan Universit, Research on network security situation prediction based on data fusion, (No. 2017XJ16)

References

[1] Liu Yanqing. Development of Computer Network Technology and Analysis of Security Defense Strategy [J]. Digital Technology & Application, 2012, (5): 179.
[2] Zhou Weiping.A Brief Talk on Attack Principles and Prevention of Network Virus ARP [J]. Silicon Valley, 2011, (2).
[3] Xu Lin. Security Strategies for Preventing ARP Attacks in Computer Network Security [J]. Computer Disc Software and Application, 2013, (17): 164-166.
[4] Wang Baomin;Zhang Jinglin;Shi Zhibin.Present Situation and Countermeasures of Computer Network Security [A]; [C]; 2002
[5] Luo Xiaozhu.Analysis of computer network security management technology [A]; The development and application of network security technology conference proceedings [C]; 2002