DOI : 10.3745/JIPS.2009.5.3.131

Principle of and Protection of Man-in-the-middle Attack Based on ARP Spoofing

Guo Hao* and Guo Tao*

Abstract: Man-in-the-middle attack is used wildly as a method of attacking the network. To discover how this type of attack works, this paper describes a method of man-in-the-middle attack based on ARP spoofing, and proposes a method of preventing such attacks.

Keywords: *Man-in-the-middle attack, ARP Spoofing, Session Hijack*

1. Introduction

The Man-in-the-middle mode of attack consists in capturing and modifying the data between two or more network hosts. [1] When a hacker runs a man-in-the-middle attack, victims' data are monitored and changed at free by this transparent man. Methods of man-in-the-middle include the following:

1) Packet Capture. This attack mode intercepts sensitive information such as the user's name and password. [1] It is harmful to cleartext or low enciphered messages.
2) Packet Modify. This attack mode modifies intercepted data packets, and then sends them to the aim host.
3) Session Hijack. This Attack mode takes over sessions between hosts, and then masquerades as the legitimate host.

In this article, we show the principle and activities of man-in-the-middle attack based on ARP spoofing, and propose some advice on how to prevent or avoid such attacks.

2. Principle of the ARP Spoofing

It is a key that an attacker inserts himself into the communications tunnel. ARP spoofing is commonly used in the Ethernet. It is common knowledge that the MAC determines the address in the Ethernet rather than in the IP. We can translate from the IP to the MAC using the ARP protocol. If the Data Link Layer does not know the MAC address of the target IP, it will broadcast an ARP request to every host in the LAN. Only the host which has the target IP will return an ARP response to the source host, including its MAC. In order to increase the efficiency of address conversion, there is always what is known as the ARP cache (i.e., the MAC records) in the memory of every host. The ARP cache is a dynamic record, and can be used to store the latest IP-MAC records.

For most operating systems, when receiving an ARP response, they will update their ARP caches whether they have sent an ARP request or not. As such, the ARP is a stateless protocol. ARP spoofing takes advantage of this characteristic.

The principle of ARP spoofing is to send an ARP response consisting of fake IP-MAC Records to target the host, which will update the ARP Cache and send data packets to the specified host after receiving the fake response. [2]

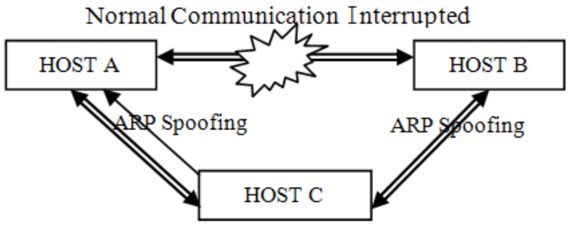
3. Principle of Man-in-the-middle Attack Based on ARP Spoofing

Three steps are necessary for a complete Man-in-the-middle attack based on ARP spoofing.

To use ARP spoofing, the Attacker inserts himself in the center of two legitimate hosts, at which point the communication between the two legitimate hosts will be broken, changing it into: A ⟷ C ⟷ B

The data frame between the two legitimate hosts is intercepted, and filter or alter the data frame in case of need.

The intercepted data frame is transmitted in order to maintain communication between the two legitimate hosts durative.



C is a “transparent trunking”

Fig.1. ARP Spoofing Attack

Manuscript received March 9, 2009; accepted June 9, 2009.

Corresponding Author: Guo Hao
* College of Science, Taiyuan University of Technology, Shanxi, China (feiyu_guo@sina.com, guotaolink@vip.163.com)

3.1 Inserting Attacker into the Communication Tunnel

In The first stage of an attack, the attacker inserts himself in the center of communication between two legitimate hosts. So, we exploited the ARP spoofing technique by sending a fake ARP response to both host A and host B, making them update their own ARP caches. The ARP response sent to host A should be (host B' IP – host C' MAC), and that sent to host B should be (host A' IP – host C' MAC). Thus, host A will regard host C' MAC as host B' MAC, while host B will regard host C' MAC as host A' MAC. While communicating between host A and host B, a data frame will be sent to C. Because the ARP Cache is dynamic update, the fake ARP response will fail in a given period of time. As such, we needed to send a fake ARP response to Host A and host B time-lapse.

3.2 Intercepting a Data Frame

Once host C had been inserted into the communication tunnel between hosts A and B, and at the same time that the data frames of hosts A and B were being sent to C, we were able to set a network card for host C as a promiscuous mode for capturing data frames. Next we need to filter or alter the data frame including special keywords in accordance with the demand. After altering some data in protocol layer, the check sum may need to be recalculated.

3.3 Transmitting Data Frame

In order to maintain the communication of the two legitimate hosts durative, host C must transmit the intercepted, altered data frame and target the MAC address of the data frame must adjust to the real MAC address of host A or B.

4. Design and Implementation of the Attack System

4.1 Experimental Environments

Hosts A, B and C are located in the same network segment in the 100M Switching Ethernet. Hosts A and B are legitimate, but host C is a Man-in-the-middle attacker. With regard to the configuration of the operating system, the IP and the MAC address of the three hosts are shown in Fig. 2.

4.2 Design and Implementation

Based on an analysis of the principle of man-in-the-middle attack through ARP spoofing, as mentioned above, we divided the attack system into three modules: the ARP spoofing module; the intercepting data frame module; and the forwarding data frame module.

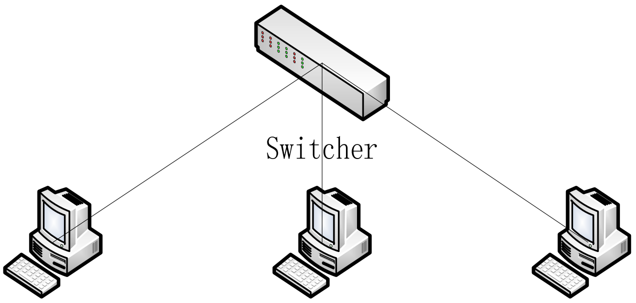


Fig. 2. Configuration of the Hosts

1) ARP Spoofing Module:

This Module is used to carry out ARP Spoofing on the legitimate hosts A and B. In the experiment, we found that the validity time of the ARP Cache is about 90s. To guarantee the durative of the spoofing, we need to send a fake ARP response to Host A and B time-lapse, and set the cycle time as 90 seconds.

2) Intercepting the Data Frame Module:

This module is used to intercept the data frame from hosts A and B, and then filter or modify the data frame according to the established rules. This module is the core of the attack system, whose operational mode will influence the effect of the whole attack.

3) Forwarding the Data Frame Module:

This module is used to forward the intercepted data frame in order to keep the communication between the two legitimate hosts durative, while making attacker C more covert. When forwarding the data frame, we need to replace the destination MAC address with the host's true MAC address.

The system is written by Visual C++6.0 and WinPeap3.0, and tests and debugs on Windows 2000 Pro SP4.

4.3 Results of Analysis

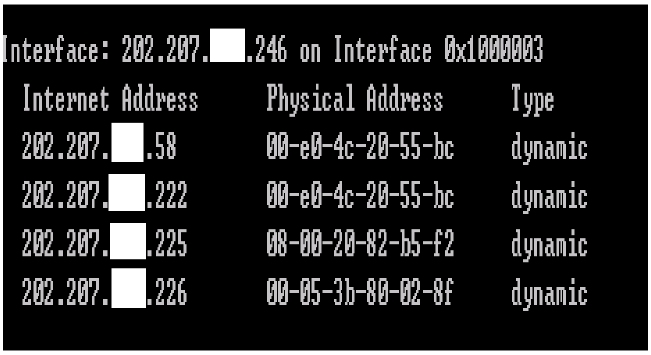
Through some special protocols testing - such as ICMP, HTTP, FTP, Telnet and UDP between hosts A and B, Attacker C intercepted and transmitted the entire data frame between hosts A and B successfully, thus accomplishing a man-in-the-middle attack.

Fig. 3 shows the ARP cache of host A after ARP spoofing. It shows that host B (202.207.aaa.58)'s MAC address was adjusted to host C (202.207.aaa.222)'s MAC address.

Fig. 4 shows the data frame, which was intercepted and transmitted by the man-in-the-middle attacker C interposed between hosts A and B.

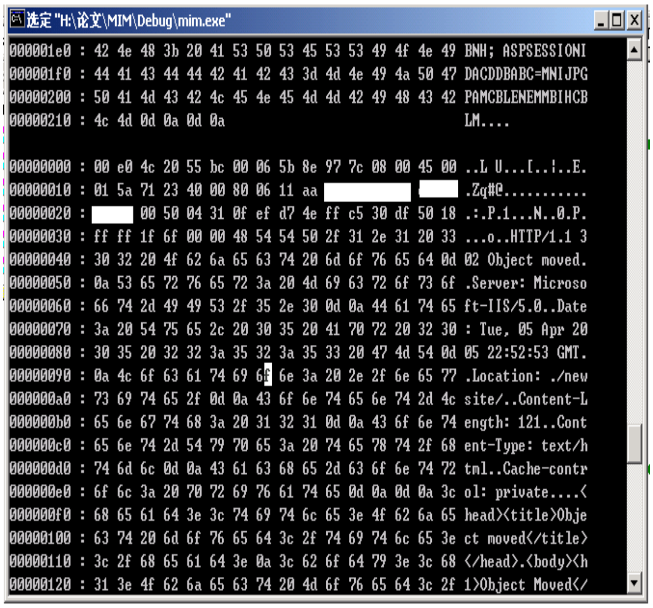
The problem with the experiments:

1) Because attacker C intercepts and transmits the data frame between hosts A and B, the communication time must be prolonged. Take Ping for example: when



```
Interface: 202.207.[redacted].246 on Interface 0x1000003
  Internet Address      Physical Address      Type
  202.207.[redacted].58       00-e0-4c-20-55-bc     dynamic
  202.207.[redacted].222      00-e0-4c-20-55-bc     dynamic
  202.207.[redacted].225      08-00-20-82-b5-f2     dynamic
  202.207.[redacted].226      00-05-3b-80-02-8f     dynamic
```

Fig. 3. Host A's ARP Cache after ARP Spoofing



```
000001e0 : 42 4e 48 3b 20 41 53 50 53 45 53 53 49 4f 4e 49 BNH; ASPSESSIONI
000001f0 : 44 41 43 44 44 42 41 42 43 3d 4d 4e 49 4a 50 47 DACDDBABC=MNIJPG
00000200 : 50 41 4d 43 42 4c 45 4e 45 4d 4d 42 49 48 43 42 PAMCBLENEMMBIHCB
00000210 : 4c 4d 0d 0a 0d 0a                               LM....

00000000 : 00 e0 4c 20 55 bc 00 06 5b 8e 97 7c 08 00 45 00 ..L U...[..¦..E.
00000010 : 01 5a 71 23 40 00 80 06 11 aa [redacted] [redacted] .Zq#@..........
00000020 : [redacted] 00 50 04 31 0f ef d7 4e ff c5 30 df 50 18 .:.P.1...N..0.P.
00000030 : ff ff 1f 6f 00 00 48 54 54 50 2f 31 2e 31 20 33 ...o..HTTP/1.1 3
00000040 : 30 32 20 4f 62 6a 65 63 74 20 6d 6f 76 65 64 0d 02 Object moved.
00000050 : 0a 53 65 72 76 65 72 3a 20 4d 69 63 72 6f 73 6f .Server: Microso
00000060 : 66 74 2d 49 49 53 2f 35 2e 30 0d 0a 44 61 74 65 ft-IIS/5.0..Date
00000070 : 3a 20 54 75 65 2c 20 30 35 20 41 70 72 20 32 30 : Tue, 05 Apr 20
00000080 : 30 35 20 32 32 3a 35 32 3a 35 33 20 47 4d 54 0d 05 22:52:53 GMT.
00000090 : 0a 4c 6f 63 61 74 69 6f 6e 3a 20 2e 2f 6e 65 77 .Location: ./new
000000a0 : 73 69 74 65 2f 0d 0a 43 6f 6e 74 65 6e 74 2d 4c site/..Content-L
000000b0 : 65 6e 67 74 68 3a 20 31 32 31 0d 0a 43 6f 6e 74 ength: 121..Cont
000000c0 : 65 6e 74 2d 54 79 70 65 3a 20 74 65 78 74 2f 68 ent-Type: text/h
000000d0 : 74 6d 6c 0d 0a 43 61 63 68 65 2d 63 6f 6e 74 72 tml..Cache-contr
000000e0 : 6f 6c 3a 20 70 72 69 76 61 74 65 0d 0a 0d 0a 3c ol: private....<
000000f0 : 68 65 61 64 3e 3c 74 69 74 6c 65 3e 4f 62 6a 65 head><title>Obje
00000100 : 63 74 20 6d 6f 76 65 64 3c 2f 74 69 74 6c 65 3e ct moved</title>
00000110 : 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 68 </head>.<body><h
00000120 : 31 3e 4f 62 6a 65 63 74 20 4d 6f 76 65 64 3c 2f 1>Object Moved</
```

Fig. 4. Intercepted Data Frame

it is a matter of direct communication between host A and host B, the time of communication is less than 10 milliseconds. After launching a man-in-the-middle attack, that time is increased from 10 to 16 milliseconds.

2) When the volume of communications between host A and host B increases, or when the handling ability of attacker C is diminished, a 'lost frame' phenomenon will occur.

The key to the solution of the above problems consists in improving the data frame interception arithmetic, in increasing the efficiency of interception, and in reducing the filtering time.

5. Precautionary Measures

1) Encrypting Communication Content

The encryption of communication content can help to deal with man-in-the-middle attacks effectively. An attacker cannot read or alter the encrypted content, even if he has succeeded in intercepting the communication data.

2) Binding to Switch Port

If every switch port is bound with only an MAC address, man-in-the-middle spoofing will be restrained effectively.

3) Setting a Static ARP Cache

If a static ARP cache is set and the IP-MAC records are edited manually, the Host will not be able to update the ARP cache even if it receives an ARP response.

6. Conclusion

In this article, the author describes a method of man-in-the-middle attack in detail, and proposes some precautionary measures for preventing such attacks. Man-in-the-middle attack, one of the most important means of network attack for a hacker, consists of various attack modes, including a strong characteristic of concealment, and thus can cause great harm. It is too difficult to solve the problem thoroughly in a short time, so this mode of attack is likely to go on posing a threat to computer security for some years yet. That being the case, the study of this subject has considerable practical significance.

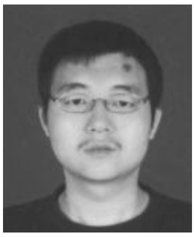
References

[1] James Stanger, *CIW Security Professional Study Guide [M]*, Peking: Publishing House of Electronics Industry, 2003

[2] Zheng Wenbing and Li Zhongcheng, "*An Algorithm Against Attacks Based on ARP Spoofing [J]*", Journal of Southern Yangtze University , 2003, 2(6):576-578

[3] Sean Whalen, "*An Introduction to ARP Spoofing [EB/OL]*",http://packetstormsecurity.org/papers/protocols/, 2001

[4] *"Windows Packet Capture Library Online Document [EB/OL]"*, http://winpcap.polito.it/docs/ , 2004



Guo Hao

Guo Hao, Ph.D. Candidate, Lecturer. He received the BS and MS degrees in Computer Science from Taiyuan University of Technology in 2003 and 2008, respectively. He worked at science college of Taiyuan University of Technology since 2004. His research interests are in area of nature language processing, Chinese information processing, semantic web, ontology and QA system (Question and Answering System).

Guo Tao

Guo Tao, Ph.D. Candidate, Lecturer. He received the BS and MS degrees in Computer Science from Taiyuan University of technology in 2001 and 2008. He worked at network center of Taiyuan University of Technology since 2001. His research interests include mobile network, mobile broadcasting and wireless communication technology.