2012 IACSIT Hong Kong Conferences
IPCSIT vol. 29 (2012) © (2012) IACSIT Press, Singapore

Implementation of ARP Protection Software Based on Windows NDIS

Shin-Shung Chen [1+], Yu-Wei Chen [2] and Tzong-Yih Kuo [3]

[1] Dept. of Information Management, China University of Technology
[2] Graduate Institute of Information and Logistics Management,
National Taipei University of Technology

Abstract. With the proliferation of LAN technology, malicious users on an Ethernet LAN can easily monitor and intercept network communication using ARP spoofing tools. An expensive hardware solution to this problem is to change all the switches. Moreover, existing ARP protection software has limited functionalities because the intrinsic weakness of Ethernet LAN security is well known and exploited by malicious hackers. In this paper, we develop filter software based on Windows NDIS, which can filter ARP packets on NIC drivers. The proposed software focuses on LAN protection against ARP spoofing packets, and it identifies malicious programs conducting ARP attacks on the application layer. It can improve the ARP protection capabilities of current ARP protection software and reduce hardware costs. We have shared the source code and provided free software downloads at openfoundry.org. We conduct tests to show that the software can provide effective protection against ARP spoofing and LAN attacks.

Keywords: ARP spoofing, security threat, ARP protection.

1. Introduction

Ethernet is a long-established widespread network technology. Any computer can re-route all the LAN traffic through itself, allowing it to monitor and alter any data sent to or received from any other machine on the network. ARP spoofing techniques (such as ARP Trojan, man-in-the-middle, and denial-of-service attacks) are well known within the hacker community, and many easy-to-use tools have been developed by malicious hackers. ARP spoofing is a security threat that cannot be ignored. Several known ARP-based attacks can severely compromise the confidentiality of sensitive data. Although ARP spoofing attacks and defenses have been known for years, countermeasures are rarely implemented. Thus, ARP poisoning is an interesting attack vector that can be further exploited in the future. The active exploitation of such attacks shows that we cannot afford to ignore network layer vulnerabilities [1].

2. Related Work

In previous studies, researchers extracted the characteristics of ARP spoof protection mechanisms. Puangpronpitag et al. [2] proposed a dynamic ARP spoof protection system (DAPS) that is implemented as a gateway for monitoring ARP packets in order to prevent ARP spoofing. Tripunitara & Dutta [3] proposed a middleware for filtering ARP packets. Their approach is similar to ours; however, they implemented the middleware on Sun Solaris, and they did not consider the solution to denial-of-service attacks using ARP spoofing on gateways. He [4] described the architecture of a personal firewall based on Windows Network Driver Interface Specification (NDIS); however, it has not been implemented practically thus far. To block ARP attacks, Cisco Systems developed Dynamic ARP inspection (DAI) [5] and Identity-Based Networking Services (IBNS) [6] for Layer 2 switches; these mechanisms ensure that only valid ARP requests and responses are forwarded. However, such solutions require hardware changes to all Layer 2 switches on a LAN; hence, they may be prohibitively expensive for small businesses. On the other hand, software

[+] Corresponding author. Tel.: +886-2-29313416 ext.2138; fax: +886-2-29334853.
E-mail address: shein@cute.edu.tw

approaches to ARP spoof protection involve the binding of the gateway IP and MAC address. Although the software is referred to as ARP protection software, it focuses on preventing the interruption of network services by ARP attacks. It does not consider a PC on the LAN as a potential ARP attacker. Therefore, all PCs on the LAN should be considered for protection against ARP spoofing.

3. Software Architecture

We designed ARP filtering software based on application and NIC drivers in order to implement an ARP firewall using middleware. The software was developed using Windows NDIS; a filtering middleware was used to drop ARP spoofing packets and to identify the malicious program sending ARP spoofing packets on Windows systems. Figure 1 shows the difference between the middleware and the application software of the implemented ARP software.

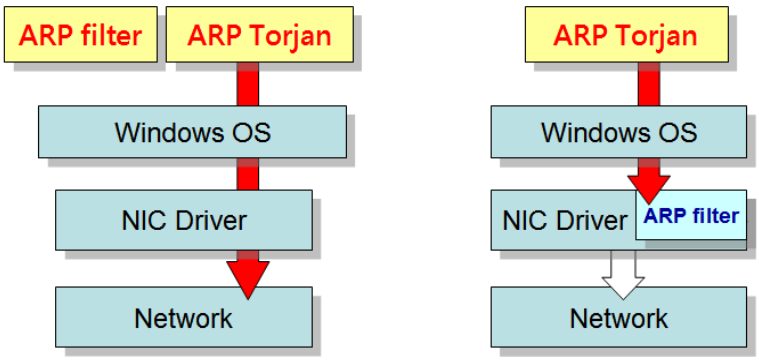

Fig. 1: Difference between ARP application software and NDIS filter middleware.

When all PCs on a LAN are deployed, ARP spoofing tools (such as NetCut, CAIN) will not be executed. There is no good reason to allow ARP spoofing for PCs on a LAN, in a security policy. The ARP protection software function prevents ARP spoofing packets from being sent over the network, thereby protecting other PCs on the LAN. By conducting an ARP scan on the LAN and obtaining the spoofing packet from the PC address information, the attacker PC can be identified by the man-in-the-middle attack. Figure 2 show an example of such an attack using ARP spoofing.

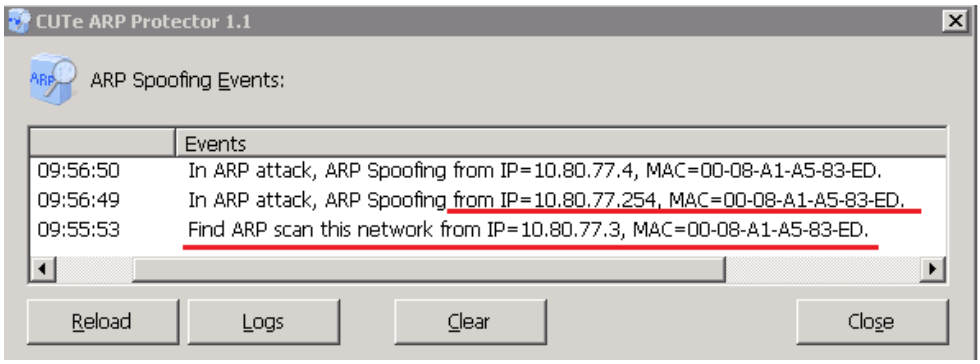

Fig. 2: Example of man-in-the-middle attack.

The NDIS architecture can filter any protocol on the network; however, we only filter ARP requests and reply packets on the LAN for performance evaluation. While an executed program calls the NIC driver to send an ARP packet, it checks whether the source MAC address and IP address are actual addresses. The NIC driver receives an ARP packet from the Ethernet network, the software checks whether the source MAC address and IP address match with the gateway information, and time is assigned at the PC start-up stage, when most malicious programs are executed. Figure 3 shows our middleware for detecting ARP spoofing packets.

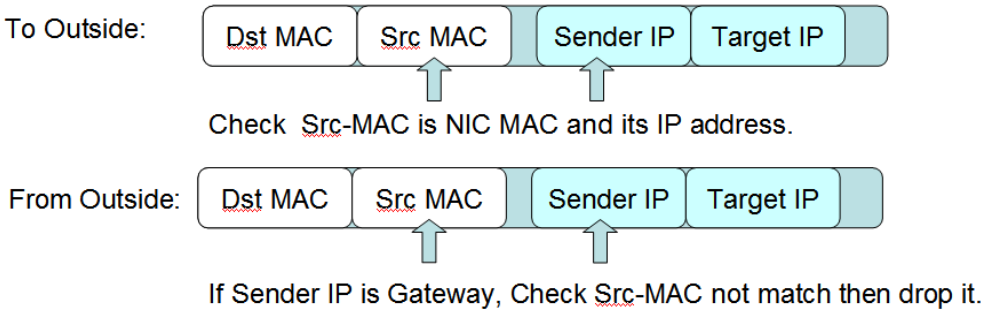

Fig. 3: ARP packets filtered by NIC driver.

The ARP spoofing software sends ARP spoofing packets to the victim PC and gateway device. The command "ARP –S [MAC-address] [IP-address]" does not serve the purpose of ARP spoof protection on Windows OS. The ARP denial of service (DoS) software (NetCut 2.0.8) will send an ARP request for spoofing to the gateway at one-second intervals. To fight DoS by ARP spoofing, we send an ARP reply packet to the gateway every second until no ARP spoofing packets are detected on the LAN. In order to detect the ARP attacker, the software listens to all ARP request packets on the LAN, and by scanning from the same source IP address, it identifies the attacker PC and triggers an alert in real time.

4. Implementation

We use Windows Driver Model (WDM) technology developed and implemented as ARP protection software on Windows OS (XP /Vista /7 /Server 2003/ 2008). It is shareware that can be executed on a 32/64-bit Windows system, and it is named CUTe ARP Protector. The source code is available at openfoundry.Org [7]; it can be downloaded to provide a secure environment on a LAN. We use the spoofing tools CAIN and NetCut to evaluate the effectiveness of this software. It is shown that the software can provide protection against ARP spoofing and DoS.

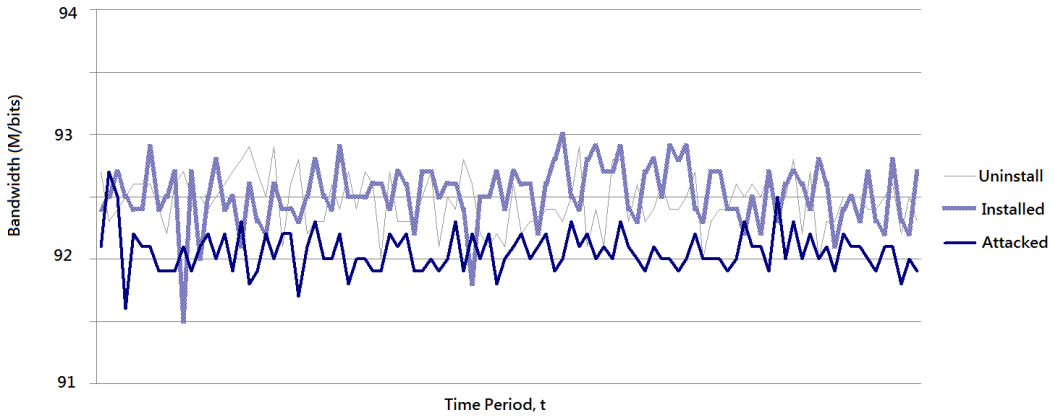

Fig. 4: Network performance on three schemes.

Figure 4 shows the performance of the software on three schemes (software not installed, software installed, and ARP attack with software installed) with 100 executions. The iPerf.exe software was used, and the network performance on Windows OS was analyzed. The average values for the three schemes (software not installed: 92.46 M/bits; software installed: 92.52 M/bits; Attacked: 92.06 M/bits) indicate that there is virtually no difference in performance between the cases with and without software installation; there is a 0.5% bandwidth loss in the case of an ARP attack because we send one ARP reply packet to the gateway device at one-second intervals. Thus, software using NIDS for ARP filtering involves low costs.

We carry out the ARP DoS attack test using NetCut (version 2.0.8) on different Layer 2 network devices. The results show that the software can effectively provide protection against ARP DoS attacks; however, the network transmission will be interrupted on some devices, which we attribute to the difference in their ARP cache sizes. The testing parameters using NetCut are listed in Table 1.

Table. 1: Network transfer rate on different devices

Device	Model	ICMP send / lose	Receive Rate
Switch	Cisco Catalyst 2948	618/0	100%
Switch	D-Link DES-1228	640/14	98%
Switch	D-link DES-1005D	648/0	100%
HUB	ASUS 8 port GX 1008B	605/13	98%

5. Implementation

In this paper, we implemented Windows-NDIS-based protection software that can provide protection against ARP spoofing. The software can be easily deployed from the viewpoint of security and network management. It can isolate ARP spoofing issues on a LAN. In addition, it has an ARP attack fight-back function. It can monitor and detect potential attackers in real time, and it can inform the network manager to carry out further processing. We believe that it can be modified with enhanced capabilities in the future; hence, we have shared the source code and published the software details at openfoundry.org. [7]

6. Acknowledgements

Our work is funded by National Science Committee of Taiwan (ROC), and the number of the Project is NSC 99-221-E-163-004.

7. References

[1] B. Zdrnja, "Malicious JavaScript Insertion through ARP Poisoning Attacks," *IEEE Security & Privacy*, Vol. 7, 03, pp. 72-74, May/June, 2009.

[2] S. Puangpronpitag, and N. Masusai, "An efficient and feasible solution to ARP Spoof problem," *Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology, 2009.* ECTI-CON 2009.

[3] M.V. Tripunitara, and P. Dutta, "A middleware approach to asynchronous and backward compatible detection and prevention of ARP cache poisoning," *Proceedings of the 15th Annual Computer Security Applications Conference.* (ACSAC '99), Dec. 1999.

[4] H. Chaokai, " Design and implementation of a personal firewall Based on NDIS Intermediate Drivers," *Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007.* SNPD 2007. Eighth ACIS International Conference, July 2007.

[5] "ARP Poisoning Attack and Mitigation Techniques," Cisco Systems, Inc. http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white_paper_c11_603839.html

[6] "Introduction to IEEE 802.1X and Cisco Identity-Based Networking Services (IBNS)," Cisco Systems, Inc., Apr. 2009.

[7] "CUTe ARP Protector," Openfundry.org., http://www.openfoundry.org/of/projects/1687