Two Methods for Active Detection and Prevention of Sophisticated ARP-Poisoning Man-in-the-Middle Attacks on Switched Ethernet LANs

Kenan Kalajdzic, Center for Computing Education, Bosnia and Herzegovina

Ahmed Patel, Universiti Kebangsaan Malaysia, Malaysia, and Kingston University, UK

Mona Taghavi, Universiti Kebangsaan Malaysia, Malaysia

ABSTRACT

This paper describes two novel methods for active detection and prevention of ARP-poisoning-based Man-in-the-Middle (MitM) attacks on switched Ethernet LANs. As a stateless and inherently insecure protocol, ARP has been used as a relatively simple means to launch Denial-of-Service (DoS) and MitM attacks on local networks and multiple solutions have been proposed to detect and prevent these types of attacks. MitM attacks are particularly dangerous, because they allow an attacker to monitor network traffic and break the integrity of data being sent over the network. The authors introduce backwards compatible techniques to prevent ARP poisoning and deal with sophisticated stealth MitM programs.

Keywords: *ARP Poisoning, Digital Forensics, Intrusion Detection & Prevention, Man-in-the-Middle Attacks, Protocols, Security*

INTRODUCTION

Although every machine on the Internet has one (or more) IP (Internet Protocol) addresses, these cannot be used for sending and receiving packets at the hardware level. IP addresses are administratively assigned logical addresses and are thus not understood by the network hardware. Nowadays, most computers are attached to a Local Area Network (LAN) through a network interface card (NIC) that only understands physical addresses. For instance, every Ethernet NIC ever manufactured comes equipped with a 48-bit physical Ethernet address. In order to avoid address conflicts, manufacturers of Ethernet NICs are assigned unique blocks of physical addresses by a central address allocation authority to ensure that no

DOI: 10.4018/jdcf.2011070104

two NICs will ever have the same address. NICs send and receive frames based solely on 48-bit Ethernet addresses, without any knowledge of the IP protocol.

Network applications, on the other hand, use IP addresses for communication, so a fundamental question now arises: How does an IP address get mapped to the physical address, such as an Ethernet address? The protocol which gives an answer to this question is called ARP (Address Resolution Protocol) and defined in RFC 826 (Plummer, 1982). It is implemented and run in almost every machine as an essential component of communication in *open* wide and local area networks to ensure unique identification of the network interface cards such as those encountered in Ethernet LAN environments. ARP provides a mechanism to translate logical network addresses into physical Media Access Control (MAC) addresses which are required for the exchange of packets on a local area network.

ARP is a stateless protocol designed without security in mind, which makes it an ideal means for launching DoS and MitM attacks on a LAN. By sending spoofed MAC addresses in ARP reply packets, a malicious host can poison the ARP cache of other hosts on the local network and thereby easily redirect network traffic.

To mitigate the danger of ARP-based attacks on local networks, multiple techniques have been proposed to detect and prevent attacks by malicious hosts. Detection of ARP poisoning is usually performed by specialized network tools, such as *arpwatch* (LBNL Network Research Group), or Intrusion Detection Systems. Carnut and Gondim (2003) and Trabelsi and Shuaib (2007) proposed delegating the detection to specialized detection or test stations with digital forensic capabilities.

For prevention of ARP-based attacks, a simple solution consists of using static ARP entries in the ARP cache. This solution, however, does not scale well especially in heterogeneous networks with dynamic IP addressing. Other solutions include use of cryptography for authenticating ARP traffic (Bruschi, Ornaghi, & Rosti, 2003; Goyal & Tripathy, 2005; Limmaneewichid & Lilakiatsakun, 2011; Lootah, Enck, & McDaniel, 2007), artificial intelligence (Trabelsi & El-Hajj, 2007), or hardware support for dynamic ARP inspection (Cisco Systems, 2009; Ortega, Marcos, Chiang, & Abad, 2009).

We have developed two methods for detection and prevention of ARP-poisoning-based MitM attacks. For simplicity and convenience, we call these Method1 and Method2, respectively. Our motivation was to find ways to cope with increasingly sophisticated MitM attack tools, while still maintaining backward compatibility with existing ARP implementations. Our methods feature several important advantages compared to the aforementioned approaches:

- We avoid the use of specialized computers as helpers in the attack detection process. While these solutions may be among the simplest to implement, delegating detection to a particular test computer or LAN switch makes them a single point of failure. Our methods also do not rely on special network devices, but address detection and prevention of ARP poisoning in the most common and usual network settings.
- Our methods do not use cryptography. Despite the fact that cryptographic functions generally help in preventing ARP poisoning, they require a special infrastructure and modifications of various components in the entire network. With our methods, it is possible to implement detection and prevention of ARP poisoning on any host in the network independently of other computers.
- Instead of relying on artificial intelligence and heuristics in detecting ARP poisoning through anomaly analysis, both our methods make use of active IP probing, which helps in an unambiguous detection of Man-in-the-Middle attacks.