Protecting Your Network from ARP Spoofing-Based Attacks

By Josha Bronson

It’s 4:45 on a Friday afternoon and you’ve got to finish that report for your team and make your 5:30 dinner reservation. You sit down at your desk and log onto the corporate Web e-mail system. You ensure that you are using an encrypted HTTP connection to the remote server because the report contains highly sensitive strategic information. When you connect to the e-mail Web server you get a strange error message, something about a mismatched SSL key. Whatever, IT must be messing around again, you think. You click “OK” and enter your username and password, log on to the system, and send your report—all in time to make your dinner reservation.

There’s just one small problem: You’ve just been a victim of an ARP spoofing attack. Your username, password, and the report you sent were all intercepted by a hacker. “But I was using an encrypted and secure connection!” you protest. “My network is all switched, so you can’t watch any of my traffic!” you insist. These are just some of the assumptions that make ARP spoofing attacks so highly effective.

Understanding MAC and ARP

In order to understand how you can protect yourself from ARP spoofing–based attacks, you must understand some fundamentals about how systems on Ethernet-based networks communicate. The level of interconnection where ARP spoofing attacks occur is known as Layer 2, or the data link layer in the OSI network model.

The first component of Layer 2 communication is the MAC address. Every network interface in an Ethernet network is assigned a MAC, or Medium Access Control address, at the time the device is manufactured. The MAC address is used to uniquely identify every interface connected to an Ethernet network. Every Ethernet card manufactured has a unique address so that cards from any vendor can be interconnected on an Ethernet-based network without having to worry about address conflicts. MAC addresses are used by network equipment such as switches to route information to the correct port on which a destination machine resides. This MAC address–based routing eliminates the need to broadcast traffic on all ports, as a hub does.
Devices with connected interfaces on an Ethernet LAN use two methods for discovering other connected interfaces on the LAN: Address Resolution Protocol and Reverse Address Resolution Protocol, ARP and RARP, respectively. Without these protocols to perform this interface discovery, it would be necessary to manually input the MAC addresses and associated IP addresses into every machine for every interface on a LAN! This would be a daunting task considering the size and dynamic nature of most modern networks. ARP and RARP automate this process through a series of Ethernet frame broadcasts to detect other locally connected machines. This information is then stored so that traffic sent between systems on the LAN can be properly routed by interconnecting network devices.

How do ARP Spoofing-Based Attacks Work?

The key to ARP spoofing attacks lies in modifying the cached MAC and IP address pair information maintained by each system. The technique utilized to perform an ARP spoofing attack is sending false ARP broadcast notifications to devices on the local network. These false ARP spoofing messages trick network devices into delivering network data to incorrect switch ports, allowing the attacker to have information destined for a victim system on the LAN sent to the attacker’s port on the network device.

There are a variety of ways ARP spoofing can attack a network. One of the most effective and dangerous is the Man in the Middle, or MITM, attack. A MITM attack places the attacking system between the victim’s system and the local gateway for egress traffic, allowing the attacking system to “sniff” everything the victim sends and receives.

First the attacker tricks the victim’s system into incorrectly addressing Ethernet frames of its packets, and tricks the switch into sending the victim’s data to the attacker’s switch port. The attacker does this with a series of spoofed ARP messages, after which it is possible for the attacker to monitor the victim’s egress connections. However, because the victim’s system will not be receiving any data in response to its connection attempts all outbound network communications made by the victim system will fail.

In order to allow the victim to continue to send and receive data to remote systems, the attacker sends another set of false ARP broadcast frames. This set of forged messages incorrectly tells the victim’s system that information destined for remote systems should be sent to the attacker’s MAC address rather than to the gateway. The attacker’s system is now receiving the victim’s network data in duplex; that is, both outbound and inbound traffic.

Now for the final trick of the MITM: The attacking system forwards the traffic to the machines for which it was originally intended, in effect becoming an temporary gateway between the victim’s system and the true LAN gateway. The victim is still able to send and receive data to and from remote systems, but all of this data is transported through the attacker’s system.
The implications to security of being interposed between the victim and the gateway are severe. Any plain-text authentication information or communications, such as network passwords or e-mail, can be monitored by the attacker. Not only can attackers monitor network traffic, they can also modify it. Having the ability to edit the victim’s network data on the fly allows the attacker to alter communications from the victim’s system, perform MITM-based attacks during cryptographic key exchange, and carry out many other security compromises. For instance, by modifying traffic during the initial key exchanges of an encrypted Web session, the attacker can intercept and decrypt the victim’s traffic, even though the session still appears to be encrypted.

The following diagram shows a typical ARP spoofing scenario along with an example of the ARP spoofing messages that the attacker sends out to redirect traffic.

There are many tools that will automatically perform most of this complex process, making ARP spoofing trivial for the clever attacker. (See Appendix A for a list of software that performs ARP spoofing–based attacks.)
Detecting ARP Spoofing Attacks

So now that we understand how ARP spoofing–based attacks work, how can we detect them? Due to the dynamic nature of the modern LAN and the automatic configuration of the ARP and IP pair information, detecting an ARP spoofing–based attack is difficult. The best approach is to enable software that monitors the ARP/IP pair combinations for machines on a given LAN. Such software can be configured to notify network or security administrators if any suspicious changes occur on the network, such as a broadcast ARP packet advertising a new MAC address for the LAN’s gateway. (See Appendix B for a list of some of these tools.) Some operating systems will also log messages when changes occur in the gateway MAC address. Unfortunately many operating systems provide no built-in method to automatically monitor and log ARP modifications.

Protecting Against ARP Spoofing Attacks

The ARP spoofing attack is highly effective because it takes advantage of an inherent weakness in the design of a core network protocol. The only real solution is an enhancement of the method of interface discovery for Ethernet networks. There is work being done in this area, but implementation is years away.

There are some methods that network and security administrators can take to limit their exposure. The first is to implement software to monitor LAN segments for suspicious ARP traffic. This ensures that in the event of an attack the proper mitigation measures can take place. The second is to segment your network. This can be accomplished by separating out subnets, using virtual LANs (VLANs) and router-based broadcast access control to limit the exposure of hosts to ARP spoofing–based attacks. A host that is on a separate subnet or isolated VLAN can not use an ARP spoofing–based attack against a host not on the same subnet or VLAN because the routing devices will drop the broadcast packets, thwarting the attempted spoof. The third method is to hard-code the important MAC/IP pairs into mission critical machines, so that an attacker cannot modify them. Some network switch devices allow static configuration of MAC/IP pair information for each port on the device; this prevents an attacker from tricking the switch into redirecting traffic to the wrong switch port.

Last and most important is to educate users about what ARP spoofing is, the telltale signs of being under an ARP attack, and to whom to respond. For instance, if any messages about mismatched keys during an encrypted communication such as HTTPS or SSH occur, the communication must be terminated immediately and a network administrator notified.
Separate, Educate and Mitigate

By taking these few preventive measures, you can greatly reduce the effectiveness and mitigate your exposure to ARP spoofing–based attacks. Until next-generation network protocols that utilize more secure local host discovery are implemented, ARP spoofing is going to be a threat to every TCP/IP LAN. Every network and security administrator should be familiar with how these attacks work, how to detect them, and the steps to take to prevent their effectiveness.

> Appendix A: ARP spoofing tools
  - ettercap  http://ettercap.sourceforge.net/
  - ae-gateway http://packetstormsecurity.nl/UNIX/security/ae-gateway.tar.gz
  - arpspoof http://monkey.org/~dugsong/dsniff/

> Appendix B: tools to monitor ARP traffic
  - Arpwatch  http://www-nrg.ee.lbl.gov/

> Appendix C: references and resources
  - ARP RFC 826
  - RARP RFC 903
  - IP of Ethernet RFC 894
  - TCP/IP tutorial RFC 1180

About the Author

Josha Bronson is a Research and Development Engineer for Foundstone Labs. Responsible for the development of many open source security tools, Josha has helped numerous companies develop software to protect enterprise networks against digital security attacks. Additional areas of expertise include penetration testing, secure software development, and security policy design and implementation for networks around the world.

Prior to Foundstone, Josha held positions in the security research and development industry focusing on automated remote vulnerability and application assessment. He was also responsible for the discovery and release of multiples security advisories for products from Microsoft, Cisco, Oracle and many others. He has appeared numerous times on television and radio programs to discuss information security. Josha holds CCNA and RHCE certifications. Josha can be reached at joshabronson@foundstone.com.