ARP Cache Poisoning Fundamentals Explained

by Himanshu Arora http://www.thegeekstuff.com/2012/01/arp-cache-poisoning/

Suppose 'A' and 'B' are very good friends and 'A' shares all his secrets with 'B'.

Now if a guy 'C' comes in and fakes as if he is 'B'. Can you imagine what could happen? Yes, 'A' could tell all his secrets to 'C' and 'C' could misuse it.

In a layman's language, this is what we mean by ARP cache poisoning.

ARP poisoning may cause many serious networking problems and network administrators should know how this attack works.

ARP Protocol

Before Jumping on to the description of ARP cache poising, lets first refresh how ARP protocol works. ARP protocol consists of the following 4 basic messages:

1. ARP request : Computer 'A' asks on the network, "who has this IP?"
2. ARP reply : All the other computers ignore the request except the computer which has the requested IP. This computer, lets say 'B' says, I have the requested IP address and here is my MAC address.
3. RARP request: This is more or less same as ARP request, the difference being that in this message a MAC address is broad-casted on network.
4. RARP reply : Same concept. Computer 'B' tells that the requested MAC is mine and here is my IP address.

All the devices that are connected to network have an ARP cache. This cache contains the mapping of all the MAC and IP address for the network devices this host has already communicated with.

ARP Cache Poisoning Concept

ARP protocol was designed to be simple and efficient but a major flaw in the protocol is lack of authentication. No authentication was added to its implementation and as a result, there is no way to authenticate the IP to MAC address mapping in the ARP reply. Further, the host does not even check whether it sent an ARP request for which it is receiving ARP reply message.

In a layman's language, if computer 'A' has sent and ARP request and it gets an ARP reply, then ARP protocol by no means can check whether the information or the IP to MAC mapping in the ARP reply is correct or not. Also, even if a host did not send an ARP request and gets an ARP reply, then also it trusts the information in reply and updates its ARP cache. This is known as ARP cache poisoning.

So you can see that its easy to exploit this weakness of ARP protocol. An evil hacker can craft a valid ARP reply in which any IP is mapped to any MAC address of the hackers choice and can send this message to the complete network. All the devices on network will accept this message and will update their ARP table with new Information and this way the hacker can gain control of the to and fro communication from any host in network.

ARP Cache Poisoning Consequences

After a hacker sees a possibility of ARP cache poisoning, the attacker can use various attack techniques to harm or to gain control of the victim's machine. Lets' discuss some of them here:

1) Denial of service

A hacker can send an ARP reply mapping an IP address on network with a wrong or non-existent MAC address. For example, a fake ARP reply mapping the network's router IP with a non-existent MAC will bring down the connectivity of the whole network with the outer world as now any packet sent to IP of router will be sent to a machine with a MAC address that does not exist.

2) Man in Middle

As the name suggest, the hacker can make his machine sit right in between of the communication between your system and any other system on network. This way the hacker can sniff all the traffic to and from both the machines.

To achieve this suppose your machine is host 'A' and your network router is host 'B'. 'A' has IP-A and MAC-A, while 'B' has IP-B and MAC-B as IP address and MAC address respectively. Now, the hacker sends an ARP reply to the router mapping your IP (IP-A) with his machine's MAC address and another ARP reply to your machine mapping routers IP with his machine's MAC address. Now any message sent by your machine to router or from router to your machine will reach the hacker's machine. The hacker can now switch on the 'IP forwarding' feature on his machine which lets the hacker's machine to forward all the traffic to and fro to your machine and router. This way the hacker's machine sits right in the middle and can sniff or block the traffic.

3) MAC Flooding

For switches on network, MAC flooding is an ARP cache poising technique that is used. Many network switches when overloaded can start acting like a hub and start broadcasting all the network traffic to all the hosts connected to network. So a hacker can flood a switch with fake ARP replies and can make the switch to start behaving like a hub. In this role, the switch does not enable its 'port security' feature due to which it broadcast all the network traffic and taking advantage of this, the hacker can packet sniff the network.

ARP Cache Poisoning Mitigation Techniques

Poisoning ARP cache remotely is bit difficult as it requires either physical access to the network or control of one of the machines in the network. Since it's not always easy so ARP attacks are not frequently heard. Anyways, taking precautions is better than taking medicines. Network administrators should take care that these types of attacks do not take place. Here are a few mitigation points:

- For small networks, static ARP entries can be maintained. Static means unchanging, so as the name suggests these entries cannot be changed and thus any tries by hackers to change the mapping fails. This is good for small networks but not for big networks as mapping for every new device added to network needs to be done manually.

- For a large network, the port security features of network switches can be explored. Some features when turned on force the switch to allow only one MAC address for each physical port on switch. This feature makes sure that machines cannot change their MAC address and cannot map more than one MAC to their machine hence preventing attacks like ‘man in middle’.
- In general, some monitoring tool like ARPwatch can be deployed to get alerts when some malicious ARP activity takes place on your network.

To conclude, in this article, we studied the basics of ARP protocol, its loopholes, how these loopholes can be exploited and how they can be mitigated.