CSE 406

Computer Security Sessional

Report on Project No. 1

ARP Cache Poisoning with Man in the Middle Attack

Submitted by-

Raihan Rasheed

Student ID. 1605062

Lab Group. B1

Project Group No. 2

Level 4 Term 1

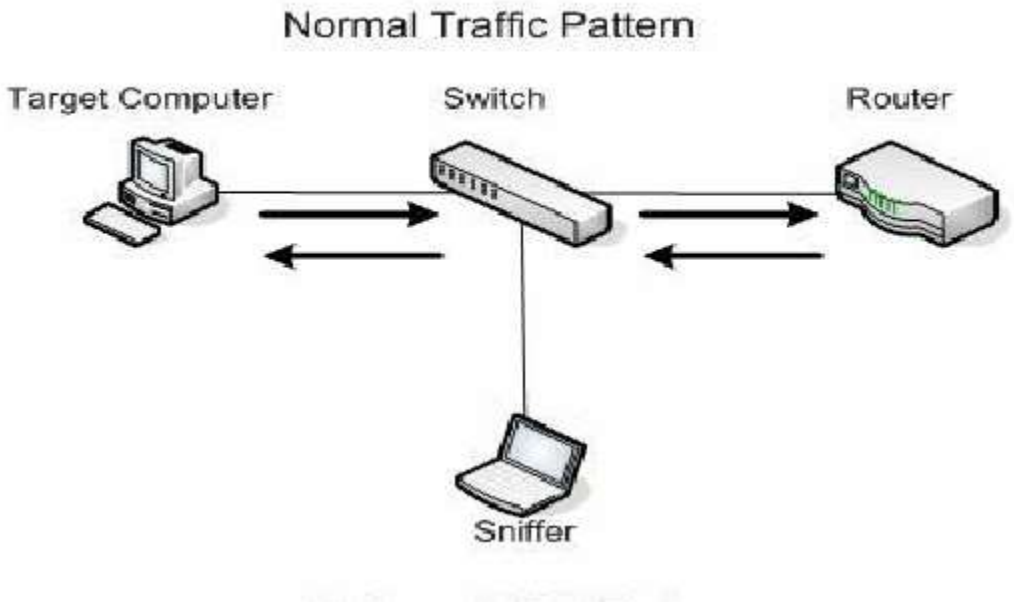
Department of CSE, BUET

Definition of the attack

ARP spoofing, ARP cache poisoing, or ARP poison routing, is a technique by which an attacker sends (spoofed) Adress Resolution Protocol (ARP) messages onto a local area network. Generally, the aim is to associate the attacker's MAC address with the IP address of another host. This host can be host computer on this network or it can be the default gateway to other networks.

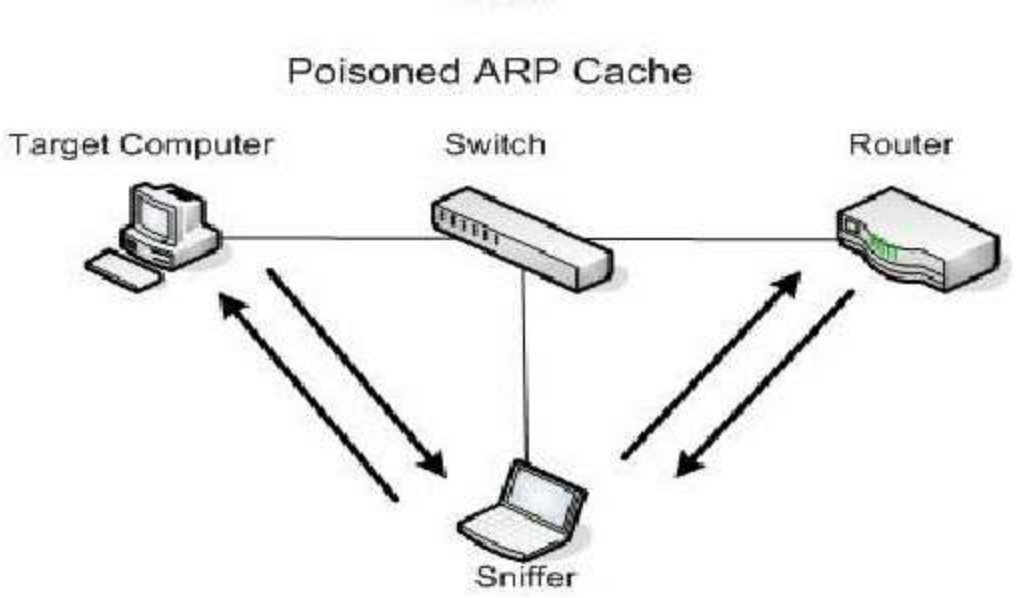
If attacker is successful, then any network traffic meant for that IP address would be sent to the attacker instead of the machine that uses that IP address. This allows attacker to intercept data frames on a network and then attacker can perform all sort of things such as modify the traffic, or stop all traffic. This attack is often used as an opening for other attacks, such as man in the middle or session hijacking attacks. The attack can only be used on networks that use ARP, and requires attacker have direct access to the local network segment to attacked.

Topology Diagram



As previously stated, this attack requires attacker have direct access to the local network. In the figure above we can see sniffer (attacker) is connected with the same switch where target computer performs its normal communication with a router. This router can be the default gateway or gateway to a particular network.

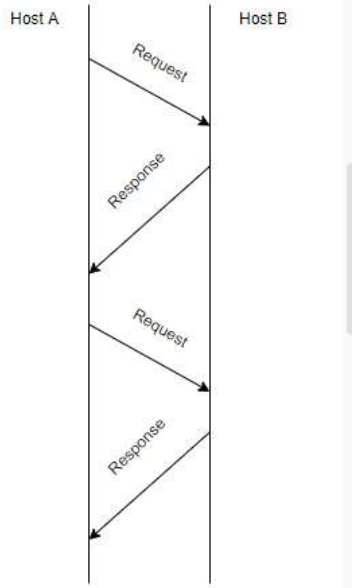
Before sniffer starts attacking the expected behaviour of this network is that target computer communicates back and forth with router via a network switch where target computer, router and attacker are connected. Then after successful attack the communication flow becomes like below -



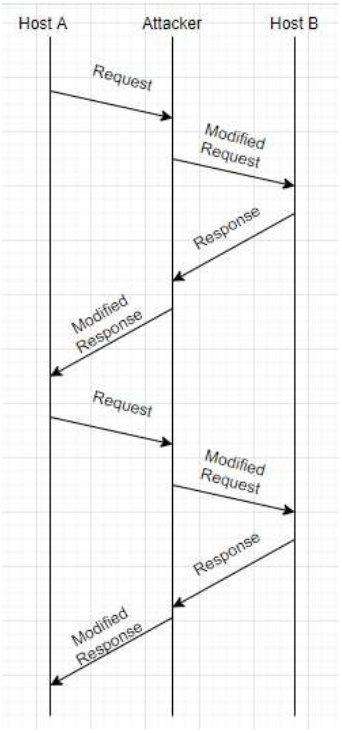
After the arp cache of both target computer and router is poisoned all the communication that is happening between target computer and router goes between the sniffer. Hence the sniffer computer gets opportunity to read data between target computer and router. Even the sniffer can modify the communication as intended or can completely hijack the session if desires.

Timing Diagram and Attack Strategy

In the figure drawn in the right-hand side we can see the normal network flow where Host A sends requests and gets back response from Host B. Both Host A or Host B can be gateway server or just a normal machine who wants to communicate with the other one.



When the attacker poisons the cache of both Host A and Host B it can now seat between both of these hosts to sniff what they are sending each other and if wishes the attacker can modify those packets as well. In order to create this situation. We have to poison both ARP caches situated in Host A and Host B. In Host A's ARP cache we are going to place Host B's IP address with Attacker's MAC address and inside Host B's ARP cache we will map Host A's IP address with Attacker's MAC address so that both of them send their message to attacker when they actually want to send message between themselves. So how we will modify ARP message and poison cache of Host A and Host B will be discussed on next sections.



Frame Details

ARP protocol works between various link layer and network layer protocol. Hence the size of an ARP message varies depending on the size of link layer and network layer address sizes. So, we are going to represent the structure of ARP message assuming it works with ipv4 network layer and ethernet data link layer. Here is a good time to mention the fact that, ARP is a data link layer protocol. So, ARP message structure shown below will go as a payload of Ethernet frame like IP packet. But it is does not work across networks hence its not network layer protocol.

Internet Protocol (IPv4) over Ethernet ARP packet

Octet offset	0	1
0	Hardware type (HTYPE)	
2	Protocol type (PTYPE)	
4	Hardware address length (HLEN)	Protocol address length (PLEN)
6	Operation (OPER)	
8	Sender hardware address (SHA) (first 2 bytes)	
10	(next 2 bytes)	
12	(last 2 bytes)	
14	Sender protocol address (SPA) (first 2 bytes)	
16	(last 2 bytes)	
18	Target hardware address (THA) (first 2 bytes)	
20	(next 2 bytes)	
22	(last 2 bytes)	
24	Target protocol address (TPA) (first 2 bytes)	
26	(last 2 bytes)	

ARP message shown above consists of total 28 bytes indexing from 0 to 27. We are assuming network layer address is IPv4 hence 32 bits or 4 bytes. Similarly, we are assuming link layer mac address is 48 bits or 6 bytes.

First two information stored are HTYPE and PTYPE indicate link layer protocol number and network layer protocol number respectively. In our case HTYPE would have 1 as its value denoting Ethernet link layer protocol and PTYPE value would be Ox0800 denoting IPv4 protocol at network layer.

Next two information HLEN and PLEN denotes address length in bytes for link layer and network layer respectively. For us that would be 6 and 4.

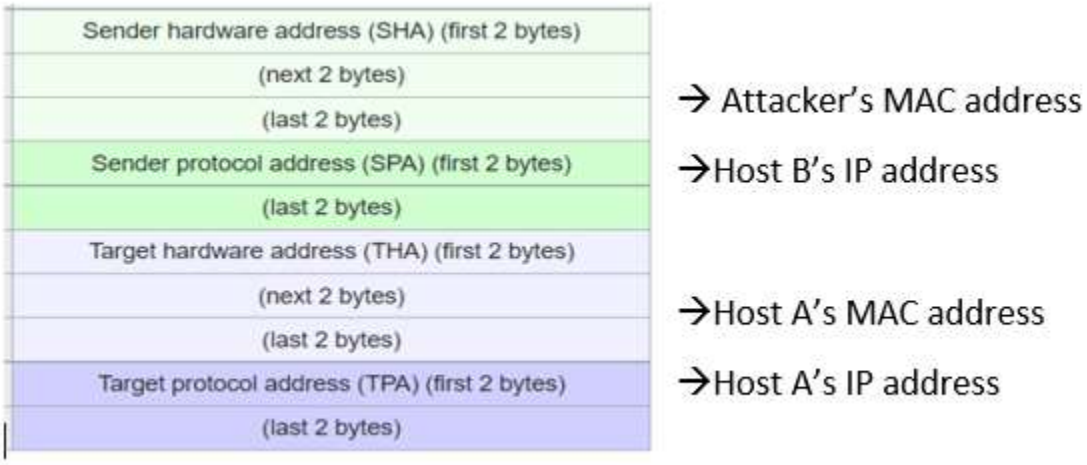
Operation field stores the type of ARP message being sent. 1 for request and 2 for reply.

The next 4 fields are important to us. Here we are going to make our modification actually. First two field is Sender Hardware Address (SHA) and Sender Protocol Address (SPA) that holds sender's MAC address and IP address respectively. Final two fields are concerned with receiver's information. Receiver's MAC address is placed on Target Hardware Address. In ARP request this field is ignored as it is not known at that time. Receiver's IP address is placed on Target Protocol Address.

Modification of ARP Message

In last section we studied different fields of ARP message. We are going to modify a ARP message in a way that it helps to store wrong information in victim's ARP cache.

Below is our proposed modification-



Here instead of sending attacker's IP address to Host A we are going to send Host B's IP address with attacker's MAC address.

We are going to send similar ARP message to Host B as well where we are going to put attacker's MAC address and Host A's IP address in sender information fields.

If we continue this process after a while and send this spoofed ARP message Host A and Host B will have poisoned cache throughout all of their communication time.

Justification

In last section we saw how are we going to modify ARP message fields so that Host A and Host B get wrong information about the MAC address where they want to send their frame. As we are going to keep sending ARP response with miss-information time after time Host A and Host B will never get correct IP address to MAC address mapping in their ARP cache. Hence they will continue to send their requests and responses to attacker and our attack will be successful. We hope that based on theories discussed in this report we will be able to demonstrate this attack in due time.