4.6 Vulnerabilities and Attacks in ARP and RARP

Now we will study various vulnerabilities and attack in ARP and RARP.

Vulnerabilities in ARP

As discussed earlier to keep down the ARP traffic on a network segment, Ethernet hosts and switches keep an ARP cache usually consisting of a list of MAC and IP addresses. The system will use this information when initiating a conversation with another system. If the address is not in the table, the system will use ARP to determine the MAC address of the destination system. Switches use ARP tables to limit the traffic that a port receives to just the MAC address registered for that port.

Authentication is a basic concept of security and provides the means for identifying and verifying a user, process or program. It is the lack of authentication in ARP that makes many networks vulnerable to various attacks.

Any system can spoof a reply to an ARP request. Receiving system will cache the reply. It will overwrite existing entry for the source and add entry if one does not exist.

The major vulnerabilities lies in ARP are ARP broadcast. ARP cache entries can be modified, deleted or added by an unsolicited requests. These type of attacks are known as ARP cache poisoning. The tools which are used for the attacks on ARP are ARO0c, ARPpoison etc. ARP supports unsolicited requests. ARP try to update ARP tables on computer even that it is not solicited, causing events like ARP Posioning and MAC Spoofing.

Proxy ARP facilities can be manipulated to effect proxy redirection.Proxy ARP is typically used by network gateways and firewalls to respond to ARP broadcasts on behalf of other hosts.

Attacks in ARP

Due to various vulnerabilities, ARP is prone to many attacks. The spoofing, cache poisoning, man in the middle and flooding are the most frequently observed attacks on ARP. Some of the attacks are described below in detail.

- **ARP Spoofing:** In an ARP spoofing attack, the attacker listens on the LAN for ARP request broadcasts. When a broadcast is sent looking for the victim host, the attacker sends a forged ARP reply with its MAC address to the requesting party.

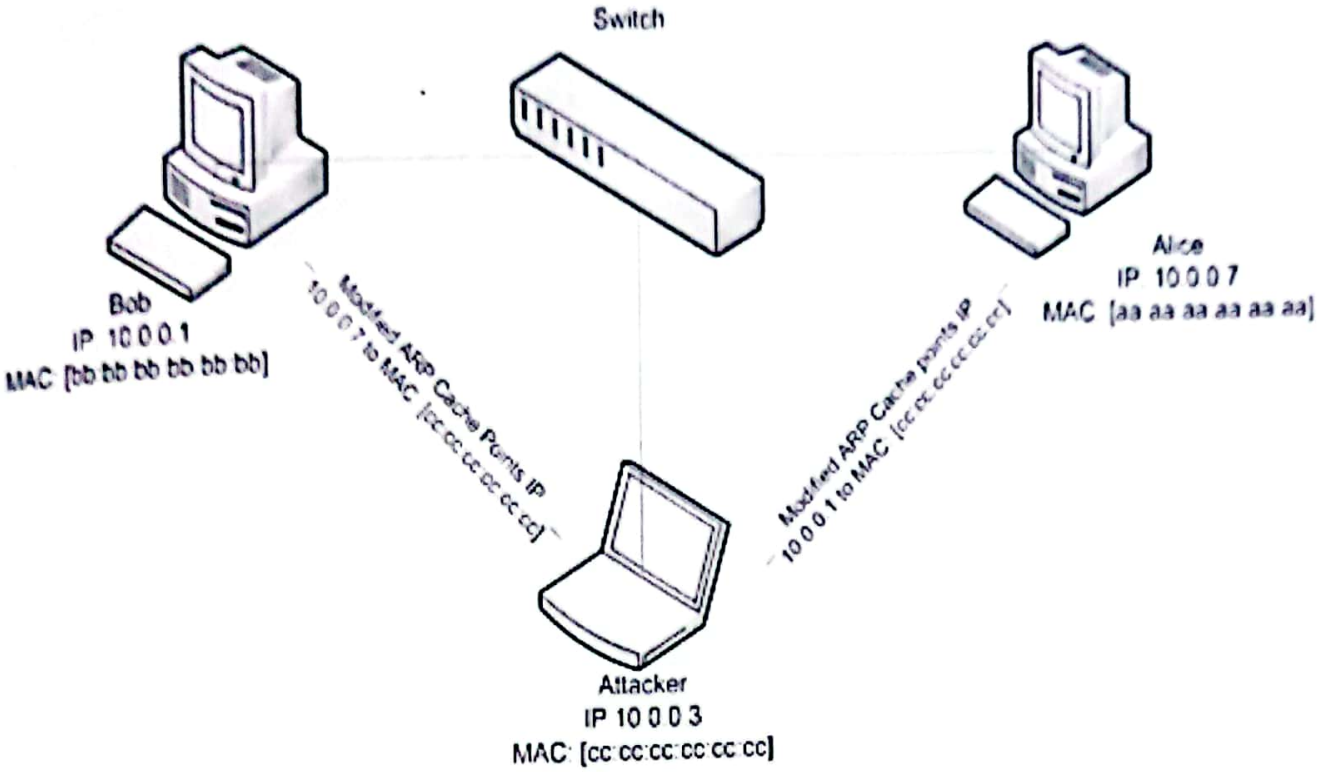

Fig 4.6 ARP Spoofing Attack

There are several security tools that allow or are based on ARP spoofing methods. Tools like arpspoof facilitates the interception of network traffic normally unavailable to an attacker. arpsend sends an IP ARP request or reply packet containing fields you specify. This is a diagnostic tool intended for use by network administrators.

- **MAC Flooding:** MAC flooding is an attack against switches. Switches have a type of cache table called Content-Addressable Memory (CAM), which is populated in most cases through transparent bridging. CAM tables basically record the port to MAC address pair so that the switch can intelligently forward packets meant for a target to the physical port that the target is connected to. The CAM tables, however, have limited memory space reserved for them. When flooded with thousands of bogus ARP packets, devices run out of memory. Once the CAM table is overflowed, any subsequent frames must be flooded to all of switch's ports, temporarily causing the switch to function similar to a hub. The attacker can then eavesdrop on the flooded packets. The behavior of a switch with overflowed CAM table depends on the vendor and the version of the operating system. Also, in certain cases, the attacked switch may simply fail, causing a denial-of-service on the LAN.
- **Man-in-the-Middle Attack:** When a "man-in-the-middle" attack (MiM) is performed, a malicious user inserts his computer between the communications path of two target computers. Sniffing can then be performed. The malicious computer will forward frames between the two target computers so communications are not interrupted.

The attack is performed as follows

where X is the attacking computer, and T1 and T2 are targets

X poisons the ARP cache of T1 and T2.

- T1 associates T2's IP with X's MAC.

- T2 associates T1's IP with X's MAC.

- All of T1 and T2's IP traffic will then go to X first, instead of directly to each other.

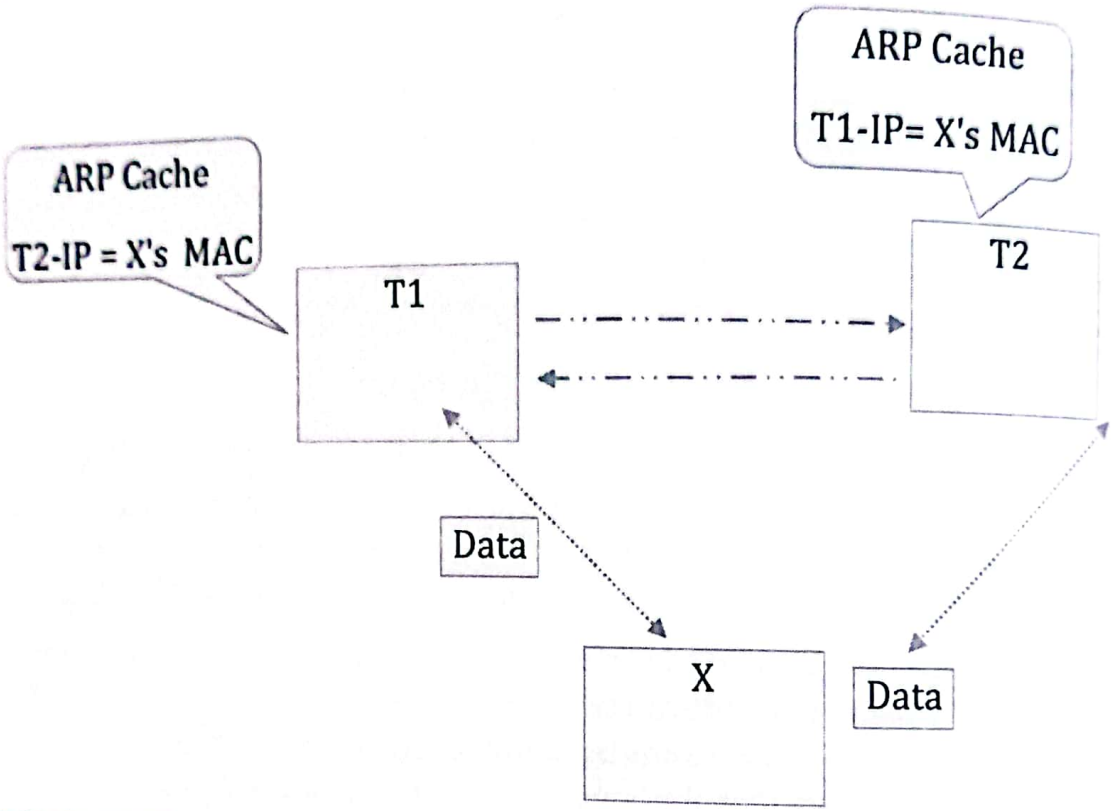

Fig 4.7 Man-in-the-Middle Attack

We consider that computers and routers/gateways can be poisoned. All Internet traffic for a host could be intercepted with this method by performing a MiM on a target computer and the LAN's router.

- **Port Stealing:** In port stealing, the attacker crafts ARP replies using the victim's MAC address as the source and its own address as the destination. When the switch receives the packet, it associates the attacker's port to the victim's MAC address. Any subsequent packets intended for the victim now go to the attacker. In order to allow the victim to continue receiving packets, the attacker must broadcast an ARP request for the victim's MAC address immediately following the interception. Upon receiving the request, the victim responds with an ARP reply, which then updates the switch's CAM table back to the original state. This process can continue as long

as the attacker wishes. The process obviously must happen extremely quickly in order to minimize delay. In fact, it is common for some packets to be lost. Any packet that is intercepted, however, can be used to the attacker's advantage thus this attack method should not be ignored. Port stealing is effective even when victims use static ARP tables or other mechanisms meant to thwart ARP cache poisoning attempts.

- **ARPoison:** ARP cache poisoning seeks to update the victim's ARP cache table with forged information. But because the original ARP request is heard by everyone on the LAN, including the legitimate host that the requestor is looking for, the attacker must win the race condition. The race condition, however, is insignificant since most operating systems simply use the most recent ARP reply to update their cache tables. As long as the attacker repeatedly advertises his MAC as that of the target, the victim's cache table will be overwritten in most cases.

The steps for ARP poisoning are:

1. Attacker selects two target nodes on the same local subnet (for example, a client and the gateway).
2. Attacker sends gratuitous ARP packets to the local node with the IP address of the default gateway but the attacker's MAC address.
3. Attacker sends gratuitous ARP packets to the default gateway with the IP address of the client node but the attacker's MAC address.
4. Attacker starts filtering IP packets so that only those coming from the local client node and local gateway targets are intercepted; this is necessary so that the attacker can differentiate traffic from the victim and other Internet-bound traffic

Arpoison is a simple command line tool by Steve Buer that constructs an ARP REQUEST or REPLY packet using the specified hardware and protocol addresses and sends it out the specified interface.

```
arpoison -i <device> -d <destIP> -s <sourceIP> -t <targMAC> -r <srcMAC> [-a] [-n
number of packets] [-w time between packets]

-i Device e.g. eth0

-d Destination IP address in dotted decimal notation.

-s Source IP address in dotted decimal notation

-t Target MAC address e.g. 00:f3:b2:23:17:f5

-r Source MAC address

-a Send ARP REQUEST

-n Number of packets to send

-w Time in seconds between packets
```

If you have physical access, MAC addresses for the target systems can be found using ifconfig on UNIX and ipconfig on Windows. Otherwise a simple ping from the LAN segment of the victim will return the MAC address as part of the packet. Sniff the packet using tcpdump or some other utility and you have your MAC information. Additionally the MAC address of ff:ff:ff:ff:ff:ff can be used to broadcast to all hosts on the local network segment.

- **Denial of Service:** The Address Resolution Protocol (ARP) requests are legitimate and essential for the operation of the network. However, ARP can be used in more than one way to exploit the vulnerability of a computer system or a network. Some of the security attacks involving ARP can cause Denial of Service (DoS) attack by sending a massive amount of ARP requests to a victim computer and tying up its resources. Updating ARP caches with non-existent MAC addresses will cause frames to be dropped. These could be sent out in a sweeping fashion to all clients on the network in order to cause a Denial of Service attack. This is also a side effect of post- Man in Middle (MiM) attacks, since targeted computers will continue to send frames to the attacker's MAC address even after they remove themselves from the communication path. To perform a clean MiM attack, the target computers would have to have the original ARP entries restored by the attacking computer.ARP can also be used to create Denial of Service attack by sending a victim computer's outgoing data to a sink by the technique of ARP cache poisoning. Other ARP based attacks can result in unauthorized sniffing of packets or hijacking of secured Internet sessions. The Denial of Service attacks due to ARP storms can also be caused by worms such as code red due to their rapid scanning activity [6,7]. The worm initiated ARP storms have been commonly found in networks with high numbers of infected and active computers and servers. In ARP storm, an attacked victim which may be a gateway or a server, may receive a

constant flow of ARP requests from attacking computers in the same sub-network, and this ties up not only the network bandwidth but also the processing resource of the victim computer.

Cloning: MAC addresses were intended to be globally unique identifiers for each network interface produced. They were to be burned into the ROM of each interface and not be changed. Today, however, MAC addresses are easily changed. Linux users can even change their MAC without spoofing software, using a single parameter to "ifconfig", the interface configuration program for the OS. An attacker could perform a Denial-of-service on a target computer, then assign themselves the IP and MAC of the target computer, receiving all frames intended for the target.

Vulnerabilities in RARP

Most of the vulnerabilities in RARP lie because of lack of access control mechanism. The other most important vulnerability is because of broadcast based nature of RARP. This feature is invitation to the hackers to trap RARP broadcast request and manipulate using spoofing and masquerading techniques.

RARP Attacks

There are two key forms of spoofing that employ RARP to carry an attack against a higher layer host configuration protocols. One of the forms is BOOTP/DHCP server hijacking and other is client spoofing which are explained below.

- **Server Hijacking or Masquerading Attack**

  In this attack, a hacker may appropriate an existing DHCP service or install or configure a DHCP server to populate DHCP clients with erroneous configuration information. This may include erroneous IP, gateway, and routing, name server NETBIOS or domain information and could result in clients being redirected to a hacking proxy as part of man in the middle attack. The attack is shown in figure 4.8

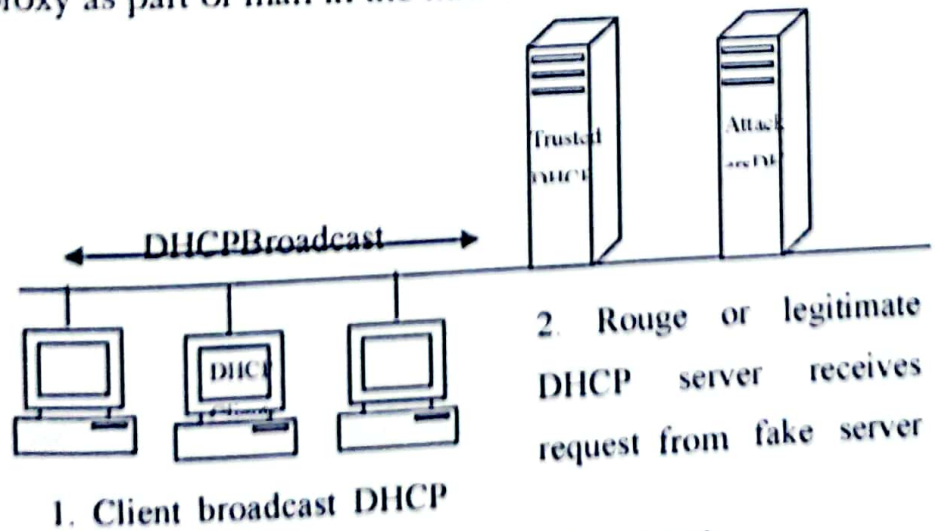

Figure 4.8 Masquerading Attack

- **Client side spoofing Attacks**

  This kind of attack involve establishing a DHCP Client on a network that utilizes DHCP to either gain a presence on the network or produce TCP/IP configuration data.

- **DHCP Starvation Attack**

  A DHCP server dynamically assigns IP addresses to hosts on a network. The administrator creates pools of addresses available for assignment. A lease time is associated with the addresses. DHCP is a standard defined in RFC 2131. A DHCP starvation attack works by broadcasting DHCP requests with spoofed MAC addresses. A DHCP starvation attack works by broadcasting DHCP requests with spoofed MAC addresses. This scenario is achieved with attack tools such as gobbler, which looks at the entire DHCP scope and tries to lease all the DHCP addresses available in the DHCP scope. This is a simple resource starvation attack, similar to a SYN flood attack. The attacker can then set up a rogue DHCP server and respond to new DHCP requests from clients on the network. This might result in a "man-in-the- middle" attack.

4.7 Defense Mechanisms

In this section we elaborate the different defense techniques for ARP.

- **Preparation**

  The best defense is to know the system. If your network is static or has few changes, then it makes sense to include MAC/ARP information in the network design and documentation. A small DMZ with limited servers should have a fairly static ARP/MAC footprint, and alarms should set off if a new MAC address is visible within the subnet, or is mapped to a differing IP address. Keep in mind that most IDS systems do little to monitor or alert on suspicious ARP traffic. Even SNORT lists ARP as a protocol they intend to monitor in the future. Additionally, monitoring a network for ARP/MAC changes will have its own share of false positives as network cards are swapped out, or dual NIC configurations change, etc.

- **Host Hardening**

  ARP tables on systems can be statically mapped usually using the arp -s command. However, different versions of operating systems have different respect for this static mapping. Even with a static mapping, some systems have been reported to accept gratuitous ARPs and overwrite the static mapping. Some systems will allow ARP to be completely removed from the Ethernet interface and rely solely on static ARP tables. Static mapping should be tested with your target OS for durability during ARP attacks.

- **Switch Hardening**

  Like many switches, Cisco's IOS offers protection against ARP attacks. IOS has a command called: Set Port Security. Enabling this feature will restrict the switch such that only one default MAC address is allowed per physical port. This command allows one to configure the action that will take place upon a hardware address change. By limiting the number of hardware addresses per port to one, a host cannot change his hardware address on the fly or try to map multiple MAC addresses to route traffic out one port. This will not analyze the MAC/IP table and take action during changes. It will not have any affect on DNS spoofing. An attacker could use this as a denial of service tool by forcing hardware address changes on a host.

- **Identification**

  ARP attacks are difficult to discover. They can appear as ephemeral network disturbances, or widespread denial of service. Access to a particular system's ARP information is usually only available by logging into the system and querying the ARP cache. Operating systems are usually quiet about their ARP cache and do nothing to report on changes made in ARP cache are suspicious or not. Network sniffers can help pinpoint ARP shenanigans, but often require much filtering to get useful data.

- **ARPWATCH**

  Arpwatch contains functionality designed to monitor the IP/MAC table and record changes via syslog and email. This is a very simple and straightforward piece of software that can be easily run on any Linux system.

RARP Attacks Defense Mechanisms

From a defensive point of view, countermeasures for RARP related attacks are options to higher level protocols such as DHCP and BOOTP.

- Static IP address: Manually assigning IP addresses to clients can significantly improve network security. But this solution is increasing the administrative workload. This is the reason other option of security are more popular.
- Monitoring: Use of ARP monitoring tools, such as arpwatch will provide security against masquerading attacks. Monitoring of network traffic may provide you information about the fake DHCP/ BOOTP Servers present on the network.
- DHCP/BOOTP MAC Controls: Many BOOTP/DHCP implementations support the configuration of MAC address controls as a form of access control. Servers that support MAC controls will only accept connections from clients that are configures in the local MAC database.

- Port Level Security: Implementation of port level security may impede an intruder's ability to connect a system to an available data port or tap into a network and obtain a legitimate IP address on that network.
- The methods used to mitigate MAC address spoofing attack may also prevent DHCP starvation by using the DHCP snooping feature. You can limit the number of MAC addresses on a switch port, a mitigation strategy for CAM table flooding, to mitigate DHCP starvation attack. Other features on the Cisco Catalyst switch, such as IP source guard, may also provide additional defense against attacks.

4.8 Conclusion

The network interface layer is the lowest layer in the TCP/IP network model stack. The network interface layer is the basis of all networks. The goal of this layer is to provide reliable communications between hosts connected on a network. This particular layer has several unique security vulnerabilities that can be exploited by a determined adversary. This chapter discusses functionality of all the protocols of the layer various attacks, mitigations, best practices.