Network Security - Homework

Sireesha Ponnaganti
801310488
18-SEP-2022

Question 1: The ARP protocol allows the network nodes to identify the mapping between IP address and hardware address dynamically. Now we assume that for the next generation Internet, some investigators propose to use static combination of IP address and Physical address, for example, if you know the next hop's IP address, you can use a function Func(IP) to calculate the MAC address. Please discuss the advantage and disadvantage of this proposal in the following aspects: (1) do we still need ARP? Why? 2) Can we still hardcode the MAC address into the hardware when it is manufactured? (3) If a computer just boots up and it needs an IP address, how can it reach the server and how can the server send the information back? Here we assume that the computer and server are on the same Ethernet.

Answers:

1.1

Yes, we need ARP to keep the communication happening between the MAC and the IP address. Because if any crash happens on a server, ARP will help to update the new MAC address and then the communication persists.

On the other hand, its complex to maintain the static IP address combination with the MAC address and also its not secure enough as the hacker can just track the system continuously with the help of MAC address.

1.2

Yes, we can still hardcode the MAC address into the hardware when it is Manufactured. But this might be more advantageous to the hackers that leads to ARP poisoning attacks where the hacker can just change their MAC address and enter into the network to get the static IP address.

1.3

If a computer just boots up and it needs an IP address, it can be done via broadcast mechanism where the computer(client) sends request to all the all the devices in the same network(Ethernet) with their IP address then the server look up and respond with the particular MAC address.

If the same scenario to be handled in unicast mechanism, we need an ARP table which store the cache and communicates the information.

Question 2:

A company is using IP based authentication to protect the computers behind the firewall. Only the web server and email server's IP addresses can reach the outside world.

Please use an example of ARP poisoning to illustrate how the malicious node can penetrate the firewall and reach out to surf the web pages.

Answer:

As the web server and Email Server IPs are the only way to enter the network, the hacker tries to enter the network by associating his IP address as the genuine IP address. To achieve this, he will change the MAC address of the system with the forged ARP request and acknowledging packets. Hence the genuine MAC address will be replaced with the hackers MAC address.

So with the help of ARP poisoning attack, the hacker will get the response from the targeted system and again the hacker will interact with the Original system. This way he will get all the information from the Web Server and the Email server. And then the hacker will penetrate to the firewall and gets the data history of the web server and all the emails. Thus the hacker will get the complete information of the webpages.

Question 3:

Read "RFC 1858 - Security Considerations for IP Fragment Filtering" at http://www.faqs.org/rfcs/rfc1858.html and write a half page summary to illustrate: (1) what are the security concerns discussed in this document? (2) what are the proposed approaches?

Answer:

The article demonstrates the IP fragment filtering, different types of attacks that occurs and the procedures to tackle these attacks. IP fragmentation means the IP divides to small chunks so that they can pass through the link easily compare to the full packet size. This happens as the Maximum transmission unit is less than the Original packet size. Once it reaches the destination, the host rearranges the packet to original shape. The issues and the security concerns with the Tiny Fragmentation attack and the overlapping Fragment attack and they ways to overcome the attack has been discussed as below.

The Tiny Fragmentation Attack mean the small chunks penetrating to the server. In the scenario of too small fragment that can be considered as a new fragment and this leads to a Denial of service attack. To overcome this attack, there should be some limitations imposed in a header that the minimum length(TMIN) of the header should be of the particular size, in any situation of the fragment with less than that size appears that should be ignored.

In the overlapping fragmentation attack, the hacker targets on the assembling IP packets. So the correct packet organization will never happens as the attacker keeps on sending the fragments that are duplicated, no sequence fragments and sending the forged rules to arrange the fragments back. This eventually leads the server overload and results the Denial of service attack. To overcome this, there should be an

inspection for the incoming packets that reaches a router, using the intrusion detection systems or firewalls and by using a proxy server.

References:

after academy(2020, February 7). What is ARP and how does it work?. https://afteracademy.com/blog/what-is-arp-and-how-does-it-work

Raspberry Pi(2019, April 7). WLAN MAC address changes at every reboot?. https://forums.raspberrypi.com/viewtopic.php?t=237623

Red Hat (2022, January 13). How to troubleshoot DHCP communication problems on your network. https://www.redhat.com/sysadmin/troubleshoot-network-dhcp-configuration

ATT&CK (2020, Oct 15) Adversary-in-the-Middle: ARP Cache Poisoning. https://attack.mitre.org/techniques/T1557/002/

Geeksforgeeks (2021, June 28) IPv4 Datagram Fragmentation and Delays. https://www.geeksforgeeks.org/ipv4-datagram-fragmentation-and-delays/