ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 3, pp: (10-15), Month: July - September 2021, Available at: www.researchpublish.com

UNION CATALOG PROTOCOL MODEL SUGGESTION TO DETERMINE ADVERSARIES AND SOLUTION DEPICTION FOR WIDE RANGE NETWORKS

Dr.A.Senthil kumar[1]

[1]Assistant Professor, Department of Computer Science, Tamil University, Thanjavur

Abstract: **In general, Network computers to communicate with one another need to know their own Internet Protocol (IP) address. More often, the initial node or the sender broadcasts the request for Ethernet address and eventually the target computer replies. Internet Protocol (IP) address is in particular is resolute by the Ethernet address and mapping the constraints are implemented through Address Resolution Protocol (ADDRESS RESOLUTION PROTOCOL (ARP)) which is the main focus of this paper. Conditioned through the usage of IP to the Ethernet address (IP, EAD) pairwise approach is utilized normally but this model suggests a novel approach, where a node can be determined true or false can be identified by sharing the union-catalogue content sharing occurs from the start node to the terminal node configured in the network. The IP to Ethernet address mapping would later be stored in an ADDRESS RESOLUTION PROTOCOL (ARP) Cache for some time duration, after which the process is repeated. Since ADDRESS RESOLUTION PROTOCOL (ARP) is susceptible to ADDRESS RESOLUTION PROTOCOL (ARP) poisoning attacks, initially the mechanism is unicasted initially and later on scalable to other nodes depending on the organizational needs. Pairwise deployment in the bandwidth enriches the packet detection approaches also when this model can be enhanced according to other user's needs. This paper initially proposes the concept of Address Resolution Protocol (ADDRESS RESOLUTION PROTOCOL (ARP)) and Dynamic Host Configuration Protocols (DHCP), ADDRESS RESOLUTION PROTOCOL (ARP) slaughtering implementation where a node gets polluted is determined, and framing a data model to store the contents of various nodes. The research further includes the sample procedure to frame the constraints and concludes by providing a prodigious solution to identify the adversaries in a network and enriches the security need of user or any organizational support.**

Keywords: **catalog, packet, address, host, media access control, address resolution, timing attack.**

1. INTRODUCTION

Nodes in networks are attached to use a network interface card that has with a unique physical address called as MAC address (or 48-bit Ethernet address). A computer cannot use MAC address alone to communicate to others in a network. No two cards would have the same address since such network card manufacturers get the card numbers from a central authority that would assign only unique MAC addresses. This can very well avoid MAC address convicts. These cards know nothing about the IP address of the computer. The data link layer hardware does not understand the IP addresses. It only understands the physical address or MAC address. In the following sections, the initial section provides the working architecture of Address Resolution Protocol with its sketch followed by Dynamic Host Configuration Protocols. The third section narrates the ADDRESS RESOLUTION PROTOCOL (ARP) slaughtering by its procedure implementations.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 3, pp: (10-15), Month: July - September 2021, Available at: www.researchpublish.com

Fourth section frames the data model to show the union catalogue suggestions along with the original specifications. When all individual nodes of this model shares their packet, any adversary who maps with the initial known specification could not know the logic depicted with the novel approach. Hence packets shared based on union-catalogue model provides concrete security over networks. The nodes are limited in the beginning can be enlarged further depending on the organizational costs whom configure the network.

2. THE ADDRESS RESOLUTION PROTOCOL (ARP)

When an incoming packet intended for a host machine on a particular local area network arrives at a gateway, the gateway asks the ADDRESS RESOLUTION PROTOCOL (ARP) program to find a physical host or MAC address that matches the IP address. The ADDRESS RESOLUTION PROTOCOL (ARP) program looks in the ADDRESS RESOLUTION PROTOCOL (ARP) cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine. While the conversion takes place in the node logically, subject to time stamping, there occurs a chance to intrude into the node by polluting the mapping. So, in addition to the initial mapping another union catalogue model similar to original conversions is used in this research to identify the node and determine the adversary based on the original mapping compared with this novel union catalogue model. Address Resolution Protocol (ARP) which is defined in RFC 826 standard is used to map the IP addresses onto the data link layer MAC address. Consider the following sketch on interconnected networks.

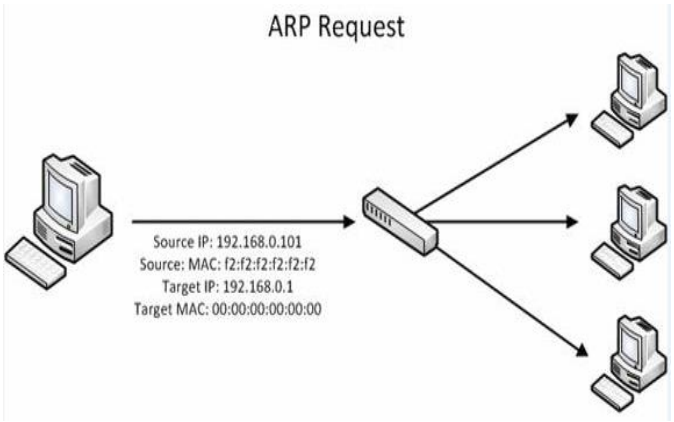

Figure 1: Interconnected networks

Each computer on LAN has been shown with an IP address andMAC address. Two computers (A and B) on LAN1 have IP address, MAC address pair as [IP- A, MAC- A] and [IP- B, MAC- B] respectively. Similarly, two computers on LAN3 (C and D) have IP address, MAC address pair as [IP- C, MAC- C], [IP- D, MAC- D]. For instance, a query to DNS would return the IP address of the user A, IP-A. It then frames a packet with IP B in the destination field and passes it to IP layer to transmit. The IP layer sees that the address is on the same network. But it needs to find B's MAC address. To find that it broadcasts a packet asking, "Who own IP address IP B?". This broadcast would reach on all computers in LAN1. Only computer B would respond with its MAC address MAC B. Thus ARP works by this request and reply approach. ADDRESS RESOLUTION PROTOCOL (ARP) replies from B, it stores that IP to- MAC address mapping of B in a local cache. So if in a short period of time, if A wants to communicate with B, it refers to the local ADDRESS RESOLUTION PROTOCOL (ARP) cache, eliminating a second broadcast. Usually, A would include its IP-to-MAC address mapping in the ADDRESS RESOLUTION PROTOCOL (ARP) packet, thus informing B of its mapping. In fact all machines on LAN1 can enter this mapping information on A into their ADDRESS RESOLUTION PROTOCOL (ARP) cache. An-other optimization is to have every computer broadcast its mapping when it boots, in the form of an ADDRESS RESOLUTION PROTOCOL (ARP) looking for its own address. To allow for changes in mapping, especially when network card breaks down, and is replaced with a new one, entries in ADDRESS RESOLUTION PROTOCOL (ARP) cache should time out after few minutes. The time required to cache by the ADDRESS RESOLUTION PROTOCOL (ARP) must be considered for security reasons. Hence any adversary can try to impact within the cache time. So, assuming timing constraint with a packet can provide periodic security to get rid from false packet injection or timing attacks. The next section includes Dynamic Host-Configuration Protocol (DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)) that is mandatory for network identifications for nodes.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 3, pp: (10-15), Month: July - September 2021, Available at: www.researchpublish.com

3. THE DYNAMIC HOST- CONFIGURATION PROTOCOL (DHCP)

DHCP stands for 'Dynamic Host Configuration Protocol' and is a way by which networked computers get their TCP/IP networking settings from a central server. Dynamic Host Control Protocol (DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)) is defined in RFC 2131 and 2132. It is an extension of BOOTP, the previous IP allocation specification. It allows manual and dynamic IP address assignment to computers that requests for that. DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) server is not reachable by broad-casting from a different network. Hence a DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) relay agent is needed to forward the DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) DISCOVER broad-cast packet from a newly booted machine. It is send as a unicast transmission to the DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) server (which may be on another network) by the relay agent. The relay agent usually keeps the IP address of the DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) server. Thus the relay agent is for relaying packets between servers and clients. This makes the DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) server handle the subnet that has no server available and thus there is no need to setup a server per sub-net. To keep track of the duration of IP address assignment, a DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) server uses the concept of leasing. As mentioned before, the DYNAMIC HOST CONFIGURATION PROTOCOL(DHCP) server assigns IP addresses automatically from a pool of IP addresses. If a compute leaves the network 'abruptly' and does not return the IP address that it was using, that IP address is lost for any further assignment. As a precaution to that, assignment of IP address is only for fixed duration of time, called 'leasing'. Just before the expiry of the lease, a computer should request the DYNAMIC OST CONFIGURATION PROTOCOL (DHCP) server for renewal. Otherwise, that IP address cannot be used further. The following sketch depicts the DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) working architecture in a network configuration as:

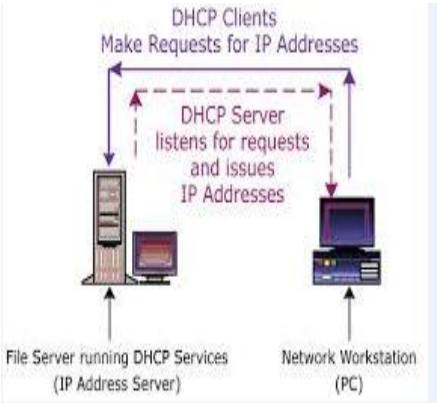

Figure -2 Dynamic Host Configuration Protocol (DHCP) Working Architecture

A DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) client may receive offers from multiple DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) servers and can accept any one of the offers; however, the client usually accepts the first offer it receives. Addition- ally, the offer from the DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) server is not a guarantee that the IP address will be allocated to the client. The server usually reserves the address until the client has had a chance to formally request the address. The client returns a formal request for the offered IP ad- dress to the DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) server in a DHCPREQUEST broad- cast message. The DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) server confirms that the IP address has been allocated to the client by returning a DHCPACKunicast message to the client. The formal request for the offered IP address (the DHCPREQUESTmessage) that is sent by the client is broadcast so that all other DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) servers that received the DHCPDISCOVER broadcast message from the client can reclaim the IP addresses that they offered to the client. If the configuration parameters sent to the client in the DHCPOFFER unicast message by the DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) server are invalid, the client re- turns a DHCPDECLINE broadcast message to the DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) server. The DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) server will send to the client a DHCPNAK denial broadcast message, which means the offered configuration parameters have not been assigned, if an error has occurred during the negotiation of the parameters or the client has been

slow in responding to the DHCPOF- FER message (the DYNAMIC HOST CONFIGURATION PROTOCOL(DHCP) server assigned the parameters to another client) of the DYNAMIC HOST CONFIGURATION PROTOCOL(DHCP) server. Meanwhile, an adversary can echo on the request of the DYNAMIC HOST CONFIGURATION PROTOCOL(DHCP) client and may inject false packet to the server. So here also security provisions must be implemented to avoid intrusions. The next section provides the attack occurrence and the novel approach of Union catalog provision that determines the attack and depicts the user an alarm to know the attack occurrence and solution to get rid from it.

4. ARP SLAUGHTERING AND SAMPLE PROCEDURE

Step 1: INITIALIZE NODE 1 AND NODE 2 WITH AN ADVERSARY SAY NODE3 SAY N3

Step 2: ASSUME NODE 3 WITH FALSE PACKET (IPHEADER, MAC1, EAD)

Step 3: NODE1 SENDS FILES TO NODE 2 I.E SHARING TAKES PLACE

Step 4: INJECT FP (IPHEADER1, MAC, EAD1) INTO NODE1 USING REQUEST R1

Step 5: INJECT FP (IPHEADER2, MAC, EAD2) INTO NODE2 USING REQUST R2

Step 6: NODE1 – ACCEPTS FP (IPHEADER1, MAC, EAD1) SINCE REQUEST R1 MAY BE A VALID REQUEST

Step 7: NODE2 – ACCEPTS FP(IPHEADER2, MAC, EAD2) SINCE REQUEST R1 MAY BE A VALID REQUEST

Step 8: NODE 1 AND NODE 2 IN THEIR CACHE STORES THE FALSE PACKETS.

In the ARP slaughtering approach, two nodes with an adversary say node 2 are considered initially with their original ip addresses and mac addresses. The adversary say node3 may inject false packet by the known ip addresses of either node 1 or node 2. For instance node 1 tries to share its data to node 2 where communication establishes between nodes in the network. During this tenure, the adversary can hack the ip address of node 1 and may inject false packet by using his own request or phishing. This event can occur for node2 also for which every ADDRESS RESOLUTION PROTOCOL (ARP) maintains the details of addresses. Now and then, both the nodes are slaughtered by their own ip addresses. This issue is detected based on the original pairing of ADDRESS RESOLUTION PROTOCOL (ARP) and MAC notifications. The details can also be obtained from the DYNAMIC HOST CONFIGURATION PROTOCOL(DHCP) server too.

5. FRAMING DATA MODEL

The data model suggests the novel framing of union catalogue packet assumption along with the timing constraints. Mapping of packets within the original packets are summed up in the checksum field that includes the timing constraint also. Within the timing constraint, the packet with novel data model suggests and identifies the false packet which is injected in the ARP Slaughtering model.

The framing of union catlog protocol data model sketch is below

IP1 198.168.0.101	MAC 00:00:00:00:00:00	UCLPT p1:t1:ct1

Figure – 3 Union Catalog Model for Node1

IP2 198.168.0.125	MAC 00:00:00:00:00:00	UCLPT p2:t2:ct2

Figure – 4 Union Catalog Model for Node2

Let us prove it through the following sample as

1. Initialize the Union Catalogue Packet say packet no, node no, time1 , say t1 of original ip, mac, and Catalogue timing say ct1.

2. Send to the DHCP Server where the Union Catalogue is stored onto the server.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 3, pp: (10-15), Month: July - September 2021, Available at: www.researchpublish.com

3. Server initializes the novel (Union Catalogue Packet) to 1.
4. Server monitors the nodes and its timings say time1 of node1 or time 2 of node 2.
5. If the time1 differs from catalogue timing say (T1 >= Ct1), then depicts the packet is from any adversary
6. If the time1 differs from catalogue timing say (T1 >= Ct1) then depicts the packet is from any adversary
7. Notify the status to any of the network administrator or chief say supdate1 = 1

Code:

```
Procedure unioncataloguepacket(pno, n1, t1, ip1, mac, ct1 )
{
Pno = 1, n1 = 1, ip1 = 198.168.0.101 ; mac = 00:00:00:00:00:00, ct1 = 1.1
  S1 = pno&&n1&&ip1&mac&&ct1 ¥     n1,n2, n3
do
   {    s1 = 1, n1 = 1;
        if (s1 == n1)
            Check (t1 (n1) >= ct1(s1))
|| (t2(n2) >=ct1(s1)
                Let p1 be original packet of node 1;
          n1 = p1;
 Update p1 to ucp(pno1,   n1, mac, ct1);
                    n1 = n1 + 1;
    } while (s1 == ct1); }
```

6. ANALYSIS

The method illustrates the various arrangements of internet protocol addresses with its packet influenced zones. The original addresses within the available catalogue combines the time with respect to the packet arrival timings and the respective internet protocol address originations. Further packets with their arrival timings and their transmission in the bandwidth can influence the protocol where there is a chance for address replacements. This can result to ip spoofing attacks. The below analysis narrates the various internet protocol addresses with their boundary packet timing with respect to catalogue provisions. If any overcrossing of the catalogue may be evaded by any malicious activities. The limits start from the value 1, 2, 3, 4, 5 with parallel timings from 0microseconds to 1 microseconds. The original ip addresses initially starts from 112 and ends up to 114 depicting that the machines within these addresses are in comfort zone when distinguished from the other.

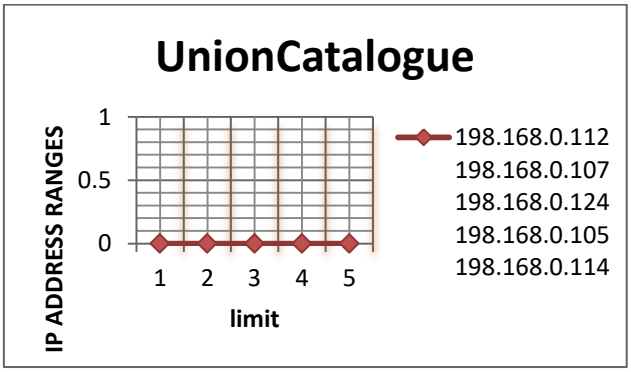

Figure-5 Distinguished Packets in Comfort Zone

Thereafter the other internet protocol addresses out of range from the original ip addresses are subject to be hacked by intruders which results in ipaddress spoofing. The union catalogue model since, the bond between their ipaddresss with their packet transmission timings are interlinked each other. Therefore this model proves to be the best utilizing model for any network organizations who wish to arrange their configurations subject to be union catalogue representation which can minimize the evasion of malicious activities in the network devices.

7. CONCLUSION

This model suggests a new approach of identifying timing attacks based on the union catalogue approach. Arrangements of various nodes according to the organizational needs often seem difficult in the initial stage. This issue can be solved if the nodes are arranged in a linear fashion and adapting the new model suggested. Various algorithms to safeguard the network and the data focus mainly on the data part but suggest the packet identifications later on. This model identifies the false packet injection in the network by known fashion of ADDRESS RESOLUTION PROTOCOL (ARP) and DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP) models. Using the same approach, the research depicts the intrusion by creating a novel method of timing constraints within the server and analyzes the timing by providing new union catalogue model of packets. Thus successful delivery of union catalogue model stored in the server not only identifies the false packet assumptions but also identifies the adversary based on their original pairwise mapping address timings. The nodes can be limited in the earlier stage but the model can be enlarged according to the organizational needs or cost.

REFERENCES

[1] Computer Networks, by Andrew S.Tanenbaum, Fourth Edition, PHI Publications, 2009

[2] Cryptography and Network Security, William Stallings, PHI Publications, Sixth Impression 2008

[3] A. K. M. N. Sakib and M. S. Kowsar, "Shared Key Vulnerability in IEEE 802 .16e :Analysis & Solution," presented at the 13th International Conference on computer and Information Technology Engineering and Technology, Bangladesh, 2010.

[4] R. K. Jha and U. D. Dalal, "A Journey on WiMAX and its Security Issues," Journal of Computer Science and Information Technologies, vol. 1, pp. 256-263, 2010.

[5] H. Altunbasak, S. Krasser, H. Owen, J.Sokol, and J. Grimminger, “Addressing the weak link between layer 2 and layer 3 in the Internet architecture,” Proceedings of29th Annual IEEE International Conference on Local Computer Networks (LCN), pp. 417- 418, Florida, USA, 2004.

[6] D. Bruschi, A. Ornaghi, and E. Rosti,“S-ARP: A se-cure address resolution protocol,” 19th Annual Computer Security Applications Conference, pp. 66-74, Nevada, USA, 2003.

[7] T. Komori, and T. Saito, “The secure DYNAMIC HOST CONFIGURATION PROTOCOL(DHCP) system with user authentication, “Proceedings of the 27thAnnual IEEE Conference on Local Computer Networks(LCN), pp. 123-131, Florida, USA, 2002.