ARP Enhancement to Stateful Protocol by Registering ARP Request

Mohammed Abdulridha HUSSAIN[1,2], Hai JIN[1], Zaid Alaa HUSSIEN[1,3], Zaid Ameen ABDULJABBAR[1,2], Salah H. ABBDAL[1], Ayad IBRAHIM[2]
[1]Cluster and Grid Computing Lab
Services Computing Technology and System Lab
School of Computer Science and Technology
Huazhong University of Science and Technology, Wuhan, 430074, China
[2]University of Basrah, Basrah, Iraq
[3]Southern Technical University, Basrah, Iraq
mohsubber@gmail.com, hjin@hust.edu.cn

Abstract— **Networking has become an essential factor in daily life and activities where the major problem in network security is the safety of the transfer information. The infrastructure for the networking is the TCP/IP suite, and the address resolution protocol is the core part of the standard which maps the logical address into a physical address. Address resolution protocol is defined as a stateless protocol in the network standard. Cache poisoning attacks target the address resolution protocol mapping to redirect the network traffic to the attacker machine, while the spoofing attack is an initialization phase for other attacks such as man-in-the-middle and denial of service attacks. The proposal in this paper is to defeat cache poisoning attacks by discarding the unregister reply, in other words, to enhance the address resolution protocol to become a stateful protocol and send a request based on the number of fake attacker replies received. The suggested address resolution protocol enhancement is examined and implemented in Linux kernel.**

Keywords- ARP; ARP poisoning; ARP spoofing, Linux kernel; stateful ARP

I. INTRODUCTION

In the TCP/IP suite there are three address modes and every packet contains source–destination pairs for each mode. The first addressing is the Port Number used to identify the application in the host. The second addressing is the *Internet Protocol* (IP), also known as the logical address, which can be changed. However, the IP is used to identify the host globally [1]. The third addressing mode is *Media Access Control* (MAC), which comes with the *Network Interface Card* (NIC) and is known as a physical and unchangeable address, namely, a unique address for each NIC device [2]. The MAC is used to identify the host within the *Local Area Network* (LAN) [3]. The packet should be sent to the intended destination IP. If the destination IP belongs to the Internet then the host needs the MAC of the gateway (router), and if the destination IP belongs to the same LAN then it still needs the MAC but for the local host. In both cases the mechanism for resolving the IP into the MAC is known as the *Address Resolution Protocol* (ARP) [4].

The ARP is used for binding the IP address into the MAC address [5]. When the host wants the MAC address of an IP then the host broadcasts an ARP request containing the IP, and the node that has the given IP replies with the MAC as a unicast ARP reply message [6]. When the host receives an ARP reply, the result mapping will be stored in the ARP table for future use [7]. Each entry in the ARP table has an expiry time, and the host will send an ARP request for each entry when it is finished [8].

The ARP is a stateless protocol because any reply received will affect the ARP table even if there has been no request sent before [9]. The attackers use this loophole for sniffing the network packets by sending fake replies to the victim host for redirection of the link to the attacker machine, which is also known as ARP spoofing or an ARP cache poisoning attack [10].

Several schemes have been proposed to detect and prevent ARP attacks; however, each technique is hindered by several limitations. In [3, 5, 11], the authors proposed the addition of a longer lifetime secondary table, such that if an attack occurs, the system will send messages to confirm and authenticate the change; the limitation of such an approach is the increased traffic congestion in the network and the latency incurred by the host in deciding what to do. In [4, 12] the proposed schemes add a centralized server to authenticate the messages; the drawback of these approaches are the single point of failure problem, and the other drawback of the scheme is increasing the network traffic when the hosts communicate with the server. In [13, 14] the proposed approaches use asymmetric cryptography to sign the reply message and to add an extra node to distribute the public keys. The disadvantage of these approaches is that the use of cryptography consumes system time and reduces system performance. In addition, the single point of failure problem is present in the key distribution node. In [15, 16] software for detecting ARP poisoning is proposed; its main limitation is that the system administrator must identify the malicious node and false position problem.

The objective of this paper is to prevent the ARP poisoning attack from updating the ARP table. To meet this objective, an enhancement to the ARP protocol is proposed. The proposed enhancement is implemented and tested on Linux environments. The main contributions of this paper in network security are as follows:

- Our proposed scheme can withstand ARP poisoning attacks by discarding all the attacker's fake replies.

978-1-4673-8838-2/16 $31.00 © 2016 IEEE
DOI 10.1109/ICNISC.2016.53