A Survey of Different Strategies to Pacify ARP Poisoning Attacks in Wireless Networks

Jaideep Singh
ECE Department
GNDU RC Jalandhar

Vinit Grewal
ECE Department
GNDU RC Jalandhar

ABSTRACT

This paper discusses poisoning of Address resolution protocol and the most advanced schemes which help to mitigate such exploits. The attack has been illustrated under different environments. The various detection and mitigative methods have been tested and compared on the basis of important network parameters.

Keywords

Wireless Networks, Cyber Security, Address Resolution Protocol, ARP poisoning, Promiscuous mode, MAC spoofing, Man in the Middle, Mitigation.

1. INTRODUCTION

Evolution of computer networks and the diversity of services they provide to the users have enhanced the need for LANs in today's world. Subsequently, security of LANs has also grown into a major concern. Address Resolution Protocol plays a fundamental role in successful communication between clients within a LAN. Despite the fact that the importance of ARP protocol for communication in Wireless Networks cannot be deserted, it can be shaped up to carry out the most dangerous attacks such as Man in the Middle and Denial of Service Attacks. Since the ARP protocol is a stateless protocol that receives and processes ARP replies without issuing ARP requests [1], the manipulation of the IP-MAC bindings by the attackers become uncomplicated and straightforward.

The authentication mechanisms have been made stronger due to the increase in the number of online crimes. Earlier, authentication involved sending the user login information in clear text. This led to variety of credential harvesting attacks by the hackers, which was tackled by providing additional security in the form of Secure Sockets Layer (TLS/SSL). This protocol (SSL) is still in use and authenticates the server to the client and vice a versa. In SSL, each party uses a digital certificate which is signed by a trusted third party. However with the new intrusion tools developed, the SSL can be stripped apart. Moxie Marlinspike [2], during a BlackHat conference in 2009 released a tool known as SSLStrip which rendered the use of SSL digital certificates unfruitful. Here, the attacker created a fake digital certificate with spoofed identity and echoed the data both ways between client and the server. So, the vulnerability did not remain limited to HTTP connections after this, rather HTTPS connections became susceptible to attacks as well.

Most existing wireless Intrusion Detection Systems take measures to detect the false AP. Snort-wireless is a much popular choice because of its open source characteristics. However it simply matches the legitimate control list. When the attacker changes legitimate AP's MAC address using Mac Spoofing technique, nothing can be done to identify a MITM attack in a particular network.

When a device needs to communicate with any other device on the same wireless network, it checks its ARP cache to find the MAC Address of the destination device. As a result of this check, if the MAC address is found in the cache, it is used for communication. If not found in local cache, the source machine generates an ARP request. The source broadcasts this request message to the local network. The message is received by each device on the LAN as a broadcast. ARP is a stateless protocol, therefore all client operating systems update their cache if a reply is received, inconsiderate of whether they have sent an actual or faked request. Since ARP does not offer any method for authenticating replies in the network, these replies are vulnerable to be manipulated by other hosts on a network.

Section I of this paper gives a brief introduction about Address Resolution Protocol and its vulnerabilities. Various defense strategies are explained in Section II. Section III provides the testbed for implementation and Section IV presents research analysis in a tabulated manner.

2. DEFENSE STRATEGIES

Cisco switches had proposed a security feature known as Dynamic ARP Inspection [3] that uses local pairing table built using a feature called DHCP snooping to detect and block the invalid <IP, MAC> bindings. The only disadvantage of this method is the high cost of switches which makes this feature ineffective.

An enhanced version of ARP, called MR-ARP is proposed by Nam et al. [10] that prevent ARP poisoning-based MITM attacks based on the concept of voting. If there is any ARP request or reply message that contains a MAC address for an IP address different from the one registered in the ARP cache, MR-ARP requests the neighboring nodes to vote for the new IP address to make the correct decision for the corresponding MAC address. The voting is advantageous only when the voting traffic rates of the responding nodes are almost the same. This condition may not be valid in the wireless network due to the traffic rate adaptation based on the signal-to-noise ratio (SNR), i.e., auto rate fallback (ARF).

Static ARP entries [12]are used for preventing ARP cache poisoning attacks. MAC addresses can be made static; therefore the hacker won't be able to apply ARP spoofing in the network. This static entry is done using windows command prompt. However this method does not work well in large networks as it becomes very cumbersome for the network administrator to manage and update these tables throughout the network.

Secure Protocol Domain Controller [13] is client side detection method that will validate the websites with its white list domain. If the user enters the website (normally require secure protocol) without a secure protocol head, then it will inform the user to include the HTTPS as part of its website's URL. However, the user must maintain the whitelist in order to keep it updated.

SSL Certificate Validator [15] is another client side SSL stripping detection method that will redirect a user to an error page when it detects any fake certificate or website. The protocol can detect this whenever a client receives a response from a website without any protocol header or just only the HTTP header.

XArp [16] is a defense mechanism that provides foremost and immensely customizable ARP spoofing detection. Active and passive mechanisms in XArp detect hackers inside the network. But the disadvantage of this method is that the detection requires continuous traffic monitoring.

Due to ARP protocol's inherent vulnerabilities, no perfect solution has been devised so far. The paper presents a testbed to investigate the vulnerabilities of ARP described in the next section.

3. TESTBED FOR IMPLEMENTATION

ARP poisoning renders the wireless networks very unstable and can often be used as a part of other serious attacks such as DOS attacks, Session Hijacking and Cloning attacks.

The **mechanism** of the **ARP Assault** has been illustrated by means of flowchart in figure 1.

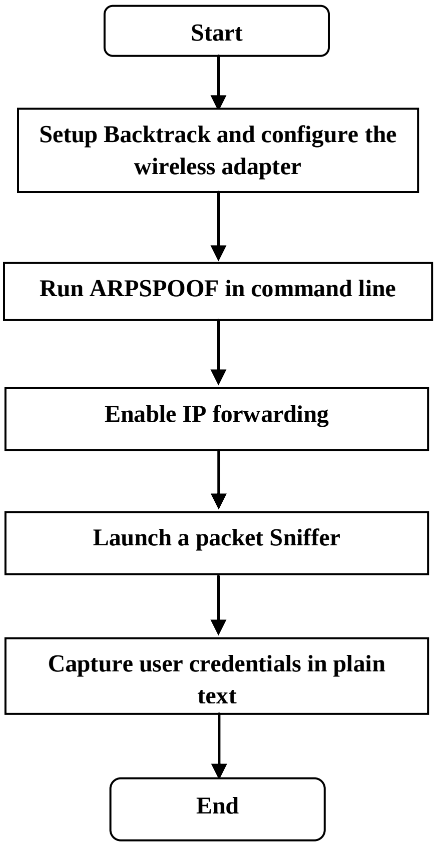
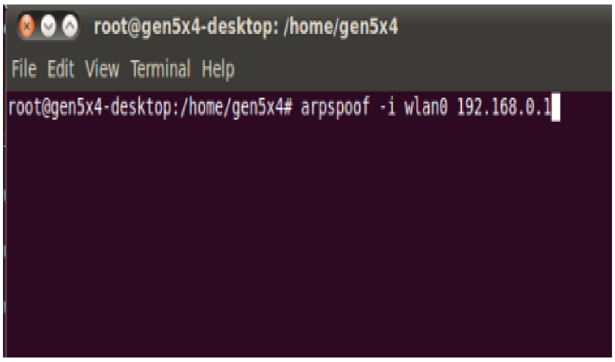

Start
Setup Backtrack and configure the wireless adapter
Run ARPSPOOF in command line
Enable IP forwarding
Launch a packet Sniffer
Capture user credentials in plain text
End

Fig 1: ARP Poisoning Mechanism

The attack has been **implemented** in Backtrack-5 R3 operating system in the command line mode

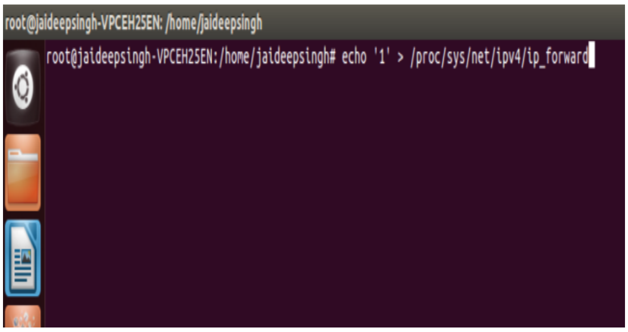
1. By the command shown in figure 2, a client is made to believe that it is communicating with the valid access point (router) when it is actually made to communicate with the malicious user.


root@gen5x4-desktop: /home/gen5x4
File Edit View Terminal Help

```
root@gen5x4-desktop:/home/gen5x4# arpspoof -i wlan0 192.168.0.1
```

Fig 2: ARP Spoofing

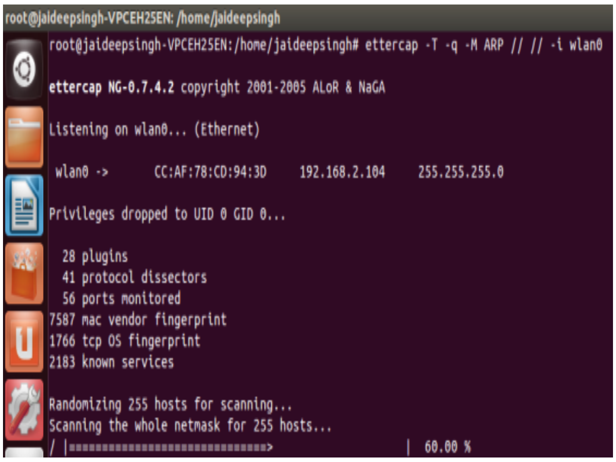
2. The packets are passed or forwarded to the other machine by using IPFORWARD as shown in figure 3.



```
root@jaideepsingh-VPCEH25EN:/home/jaideepsingh# echo '1' > /proc/sys/net/ipv4/ip_forward
```

Fig 3: IP Forwarding

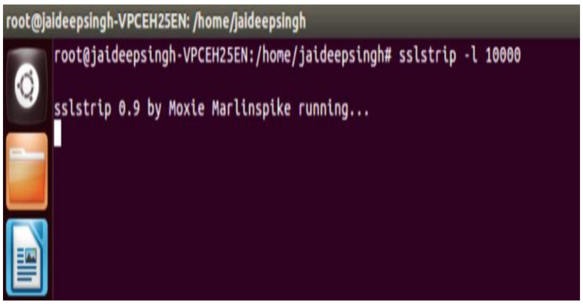
3. Sniffing, as depicted in figure 4 is an act of grabbing all the traffic that passes over a specific wireless communication channel. There are a number of tools that enable attackers to do this.



```
root@jaideepsingh-VPCEH25EN:/home/jaideepsingh# ettercap -T -q -M ARP // // -i wlan0

ettercap NG-0.7.4.2 copyright 2001-2005 ALoR & NaGA

Listening on wlan0... (Ethernet)

 wlan0 ->       CC:AF:78:CD:94:3D     192.168.2.104     255.255.255.0

Privileges dropped to UID 0 GID 0...

  28 plugins
  41 protocol dissectors
  56 ports monitored
7587 mac vendor fingerprint
1766 tcp OS fingerprint
2183 known services

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
/ |==============================>                     |  60.00 %
```

Fig 4: Sniffing

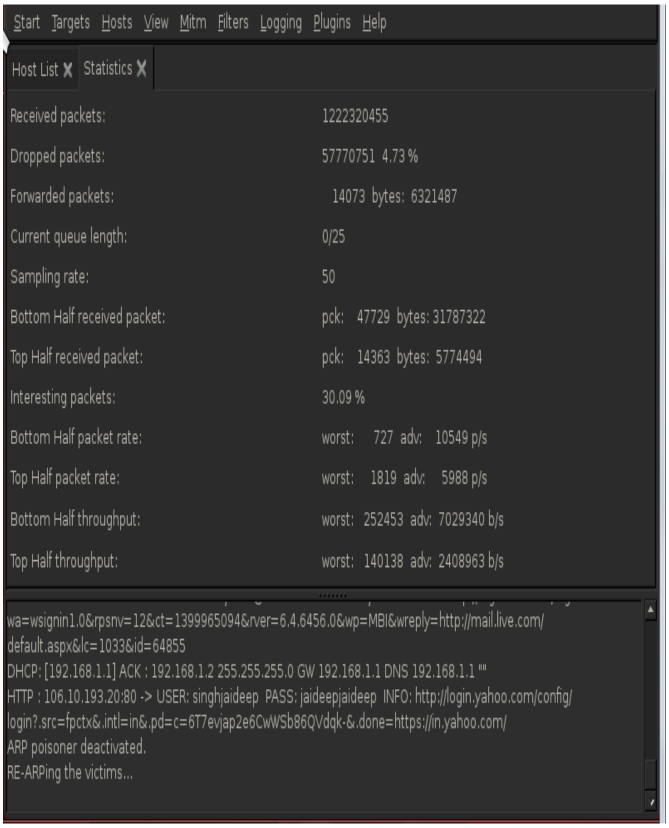
4. sslstrip[2] is a tool that was released in 2009 and this renders the use of SSL digital certificates useless. The tool can be seen running in figure 5.



```
root@jaideepsingh-VPCEH25EN: /home/jaideepsingh
root@jaideepsingh-VPCEH25EN:/home/jaideepsingh# sslstrip -l 10000

sslstrip 0.9 by Moxie Marlinspike running...
```

Fig 5: Sslstrip

5. The user credentials are thus harvested by the use of ARP Poisoning in conjunction with sslstrip as shown in figure 6. The secure login sites such as banking sites and all sorts of encrypted connections are easily split apart by this method.



```
Received packets:               1222320455
Dropped packets:                57770751  4.73 %
Forwarded packets:                14073  bytes:  6321487
Current queue length:           0/25
Sampling rate:                  50
Bottom Half received packet:    pck:   47729  bytes: 31787322
Top Half received packet:       pck:   14363  bytes:  5774494
Interesting packets:            30.09 %
Bottom Half packet rate:        worst:     727  adv:   10549 p/s
Top Half packet rate:           worst:    1819  adv:    5988 p/s
Bottom Half throughput:         worst:  252453  adv:  7029340 b/s
Top Half throughput:            worst:  140138  adv:  2408963 b/s
```

```
wa=wsignin1.0&rpsnv=12&ct=1399965094&rver=6.4.6456.0&wp=MBI&wreply=http://mail.live.com/
default.aspx&lc=1033&id=64855
DHCP: [192.168.1.1] ACK : 192.168.1.2 255.255.255.0 GW 192.168.1.1 DNS 192.168.1.1 ""
HTTP : 106.10.193.20:80 -> USER: singhjaideep  PASS: jaideepjaideep  INFO: http://login.yahoo.com/config/
login?.src=fpctx&.intl=in&.pd=c=6T7evjap2e6CwWSb86QVdqk-&.done=https://in.yahoo.com/
ARP poisoner deactivated.
RE-ARPing the victims...
```

Fig 6.Credentials Harvested

Table 1

Scheme	**Mechanism**	**Pros/Cons**
MR-ARP [10]	Enhanced version of ARP to prevent ARP poisoning using the concept of voting	May not be valid in the wireless LAN network due to auto rate fallback.
Dynamic ARP Inspection [4]	Blocks the invalid <IP,MAC> bindings using a feature DHCP Snooping.	High cost of switches makes this feature ineffective.
Static ARP Entries [12]	Use of static ARP cache entries.	Simple method but not suitable for large networks.
Secure Protocol Domain Controller [13]	Domain Controller that will validate the website with its white-list domain	User must maintain the white list to keep it updated.
SSL Certificate Validator [15]	Redirects the user to an error page in case of fake certificate.	Detects only SSL stripping attacks and does not provide any prevention.
XArp [16]	Detects false <IP, MAC> bindings.	Detection requires continuous traffic monitoring.

4. RESULTS AND ANALYSIS

To highlight the current state of art in this area, the most important and apt techniques based on the literature survey have been tabulated in table 1. The tabular analysis in figure 8 reveals that Static ARP entries is least suited method to combat ARP poisoning assaults followed by XArp, as both methods require continuous monitoring of network administrators. To support the view, a graphical analysis of various explored techniques has been given in figure 7.

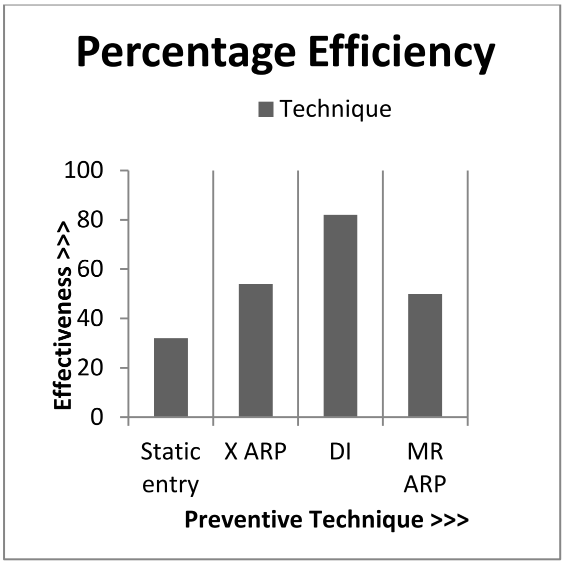


Fig 7: Bar Graph Analysis

5. CONCLUSION

Though a lot of measures have been implemented to defend the spoofing attacks, yet some vulnerability in ARP remains a topic of concern. This paper depicts the problem of ARP poisoning in detail. From the survey, it can be concluded that the ideal method used to prevent ARP attacks is D-ARP[4], used by CISCO. In future, an ideal mechanism can be developed and implemented by accomplishing several experiments with reference to the work done in wide scenarios of ARP spoofing attacks. The present work can also be taken to advantage to improve the efficiency of existing techniques.

6. REFERENCES

[1] Marco Antônio Carnut and João J. C. Gondim, "ARP spoofing detection on switched ethernet networks: a feasibility study," 5th Symposium on Security in Informatics held at Brazilian Air Force Technology Institute, November 2003

[2] Moxie Marlinspike, "SSLStrip, Black Hat DC 2009", Retrievedhttp://www.thoughtcrime.org/software/sslstrip/

[3] D. Plummer. An ethernet address resolution protocol, Nov.2010. RFC 826.

[4] Cisco Systems. *Configuring Dynamic ARP Inspection*,chapter 39, pages 39:1–39:22. 2012. Catalyst 6500 Series Switch Cisco IOS Sofware Configuration Guide, Release 12.2SX

[5] T. Demuth and A. Leitner. ARP spoofing and poisoning:Traffic tricks. *Linux Magazine*, 56:26–31, July 2011.

[6] Jaideep Singh, Goldendeep Kaur, Dr. Jyoteesh Malhotra, "A Comprehensive Survey of Current Trends and Challenges to mitigate ARP attacks", In Proceedings of 1st International Conference on Electrical, Electronics, Signals and Optimization , ISBN: 978-1-4799-7678 2/15/$31.00 ©2015 IEEE

[7] Neminath H, S Biswas, S Roopa, R Ratti, R Nandi, F A Barbhuiya, A Sur, V Ramachandran, "A DES Approach to Intrusion Detection System foe ARP Spoofing Attacks", 18th Mediterranean Conference on Control& Automation (MED), ISBN: 978-1-4244-8091-3, IEEE 2010

[8] Wenjian Xing, Yunlan Zhao, Tonglei Li, "Research on the defense against ARP Spoofing Attacks based on Winpcap", 2010 Second International Workshop on Education Technology and Computer Science, Digital Object Identifier: 1O.l109IETCS.201O.75, 2010 IEEE

[9] M. Carnut and J. Gondim. ARP spoofing detection onswitched Ethernet networks: A feasibility study. In *Proceedingsof the 5th Simp´osioSeguranc¸aemInform´atica*, Nov.2011.

[10] SY Nam, D Kim, J Kim, Enhanced ARP: preventing ARP poisoning-basedman-in-the-middle attacks. IEEE Commun Lett.14(2), 187–189 (2010).

[11] V. Goyal and V. Abraham " An efficient Solution to the ARP cache poisoning problem", in Proceedings of 10th Australasian Conference on Information Security and Privacy, Jul 2013, pp 40-51.

[12] Divya Sharma, Oves Khan, Kanika Aggarwal, Preeti Vaidya, "A New Approach to Prevent ARP Spoofing", In Proceedings of International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-3, Issue-1, June 2013.

[13] Hodges, C. Jackson, A. Barth, HTTP Strict Transport Security(HSTS), IETF, Internet draft, 2012.

[14] S. Whalen, "An introduction to ARP spoofing," 2600: The HackerQuarterly, vol. 18, no. 3, Fall 2001,.Available:http://servv89pn0aj.sn.sourcedns.com/_ gbpprorg/2600/arp spoofing intro.pdf

[15] A. Fung, K. Chueng, "SSLock: Sustaining the Trust on Entities brought by SSL, Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, Beijing, China, 2010.

[16] ChristophP. Mayer, "Advanced ARP Detection: XArp", Retrievedfrom: http://www.securityfocus.com/tools/6908.