Prevention of Phishing and ARP Cache Poisoning in Man-In-The-Middle Attacks by using ARP Cache Management

Nithin R[1], Prashanth C[2], Shreyas M S[3], Sadhvi G E[4]

[1,2,4] *Department of Computer Science and Engineering Global Academy of Technology, Bangalore, Karnataka, India.*
[3]*Department of Computer Science and Engineering MVJ College of Engineering, Bangalore, Karnataka, India.*

---***---

Abstract:– *Even after the inception of many protocols to transfer information in the form of packets over the internet, the current world still uses ARP as the base for any kind of transfer of packets. ARP (Address Resolution Protocol) is termed as the most vulnerable protocols present because this specific protocol is mainly considered prone to Man-In-The-Middle Attacks. Since to improvise the current ARP network we need to change the firmware of all existing customers and it involves a lot of cost to change a protocol itself it is not feasible.*
In this paper we present a novel approach to prevent ARP cache poisoning by using a detection system which monitors the ARP Table regularly for any malicious entries.

Key Words: Man-In-The-Middle Attacks, ARP (Address Resolution Protocol), HTTP, ARP Cache Poisoning TCP/IP.

1. INTRODUCTION

A Denial of Services attacker has the potential to cause catastrophic damage to his target server and can even cause a complete failure of the whole system by targeting all the system resources in the target machine such as bandwidth and CPU memory [1]. This is causing serious issues in our daily life which is mainly based on the use of internet and cellular networks. Almost every individual currently possesses at least 7 wireless devices which are vulnerable. Among them the most commonly used applications such as banking, e-commerce and social networking sites involve the highest usage of these wireless devices [5]. This paves way for opening a gateway to attackers to access all the sensitive information of a user.

1.1 Phishing

Phishing is mainly done through electronic communication. It is often done by duping the victim into opening a link in an email or an instant message where the attacker often steals user's data such as login credentials and also even credit card numbers. Phishing is mainly categorized into three types: Phishing, Spear-Phishing and Whaling;

Phishing is usually an attack which is sent by a known contact or organization. The emails include malicious links and installs malicious content on the target system.

Spear-Phishing is done after gathering intelligence. After getting to know about the user and his personal data or even it may be targeted to a restricted organization, the attacker attacks the target by resembling someone of their own and makes the target believe it is from a trusted source.

Whaling is directed at high-profile targets. Here a lot of research is done on a person and then the attacks are launched to target only that specific person.

1.2 Man-In-The-Middle

The normal MITM [5] attacks include targets (the two endpoints) and the aggressors (an outsider). The attacker gets to the communication channel maybe by intercepting the local LAN and controls the messages between the two endpoints. Subsequently, in MITM assaults, the malicious attacker can catch, change, supplant or adjust the information being transmitted in the communication channel between the endpoints. Target persons trust the communication channel to be ensured as they are ignorant of these vulnerabilities in their system.
With the help of Man-In The-Middle attacks the attacker will have complete access to sensitive information [12] such as the passwords and emails contents or he/she have also the ability to modify all the data that is being sent, and thus compromising the data's integrity.

2. EXISTING SYSTEM

Address Resolution Protocol is mostly used in LAN. It works on the basis of a sender initiating a communication where it looks for the destination IP, here the receiver gets the request and indicates that the address it is looking for is present with it. Now the MAC address of the corresponding computer is matched and allocates it to the receiving message. Since there is no cross-checking mechanism in the receiver end any attacker can start accessing the local network and falsely claim that his/her computer is the rightful receiver even though he is the middle man here. There have been certain methods used to improvise this ARP but all of them have failed. It is mainly because if we need to improvise we need to change the firmware of all the existing modems and it involves lot of cost to change an already existing firmware.

The ARP works with the help of BGP (Border Gateway Protocol). The BGP is another one of the protocols which has absolutely no authentication. It transfers packets between two autonomous systems. A single ISP Provider cannot transfer the whole data all over the world, hence there is transfer of data between different providers. This enables for attackers to explore vulnerabilities in between the transfer. The attacker can impersonate that his/her computer is the main server and can start getting requests directed to the main server.

ARP cache poisoning [10] is one of the most commonly used techniques in ARP Cache Poisoning. It targets the ARP cache with an altered ARP request. So now the requests directly go through the attacker and then to the final destination.

To fix this integral problem in ARP network there were many protocols developed to replace ARP. There were also systems developed to provide anonymous actions for the user such as TOR. It works by having multiple random connection before reaching the final destination. There maybe three or five volunteers who will be present to traverse these hops. Thus, an attacker cannot carry out the Man in The Middle attack because he/she will not have knowledge on where the packets are traversing. But this also faced failure because it was very slow in making a simple data transfer to happen.

The basic TCP/IP connection was present in any of these protocols where whenever a connection is needed to be started, the browser sends out a SYN (I want to connect) which is a size of 43 bytes across the globe to reach its destination which will be port 80 in the server usually. It responds with an ACK (acknowledged) message. This SYN/ACK is the basis of how a TCP/IP communication works in the network layer.

Table -1: ARP Reply Table

MAC src	MAC dst	IP Src	IP Dst	TCP sport	TCP dport	Action
BA:BA:BA:BA:BA:BA	*	*	*	*	*	Drop
AA:AA:AA:AA:AA:AA	FF:FF:FF:FF:FF:FF	*	*	*	*	Drop
*	*	192.168.1.5	192.168.1.100	*	22	Accept
*	*	192.168.1.0/24	*	*	22,3389	Drop
*	*	*	192.168.1.100	*	389	Accept
*	*	*	192.168.1.100	*	135-139,445	Accept
*	*	*	*	*	135-139,445	Drop
*	*	192.168.1.0/24	*	*	*	Accept

ARP is considered a trustworthy protocol and was not developed to handle with malicious host. There are different ways for the malicious host to make an unsuspecting host modify its ARP cache and thus add or update entries with an (IP, MAC) mapping to thus have the attackers to impersonate different random hosts and perform man-in-the-middle attacks to gain access to all the sensitive information and also perform DOS attack on all of the systems.

So, the moment the hosts add an incorrect (IP, MAC) mapping to the given ARP cache, it is known as ARP cache poisoning. It can also be termed as ARP Poisoning or ARP Spoofing. This indicates that hackers would have tried to use spoofed or fake ARP packets to poison the Address Resolution Protocol cache in the system.

The attackers will start sending ARP replies with the new fake (IP, MAC) mapping, to try to poison the ARP cache of all the other hosts on the network.

For example, if the attacker wants to impersonate host P so that host Q has to send the data which is destined to P to the attacker instead.

Thus, the attackers can start sending ARP replies indicating that the host with the IP xy:xy:xy:xy has the MAC aa:aa:aa:aa:aa:aa which is the MAC address of the attacker.

Since the Address Resolution Protocol is considered to be stateless protocols, there is a chance that the receiver will immediately update its ARP cache with the (IP, MAC) pairing it received without any checking.

Furthermore, some operating systems might even start updating the static cache entries with all the information which are received from these unsolicited ARP replies.

Even if the Address Resolution Protocol is configured as to be stateful, the attacker can still have the option to perform an ARP spoofing attack by sending fake Internet Control Message Protocol echo requests to person Q which indicates that it is coming from the person P, but instead it is using the MAC address of the attackers.

Relying on this given implementation, the operating systems can now either use the (IP, MAC) pairing which is inferred from the newly received Ethernet frame and also the ICMP packet, or even it can issue an Address Resolution Protocol request to learn the mapping (before sending the ICMP echo reply). In the given latter case, the attackers are able to instantly reply to the ARP request thus poisoning the cache.

3. ANALYSIS

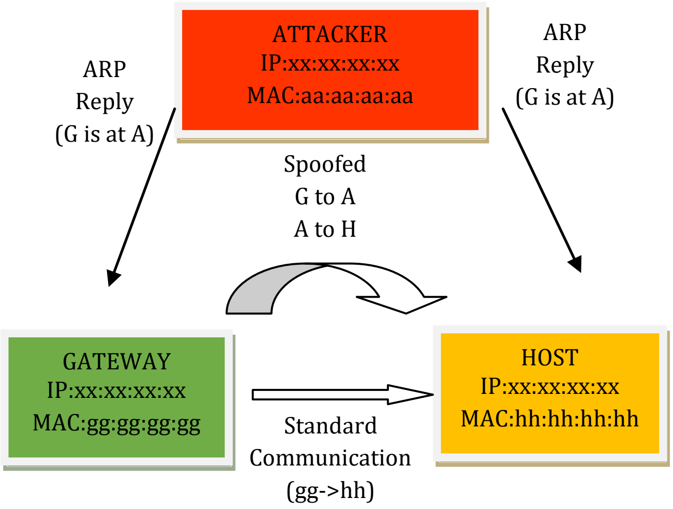


Fig -1: Analysis of ARP Attack

Here the attacker is the man-in-the-middle wherein he takes the MAC address of the root server and impersonates it to the host by changing his MAC address. So now the host believes that the attacker itself is the destination and starts sending data to the attacker and then attacker is now privy to all the information from the sender. Thus, the data is compromised and now the attacker makes sure his/her trace is not seen and the communication goes on.

The types of all the possible ARP replies that host A may receive will depend on the types of the attack (MiM, DoS, or Cloning) that the attacker is intending to perform on host A. Suppose within a timeout, host A receives only one ARP reply, then it is assured that the host B is generating the ARP reply, which will not include the fake IP and MAC addresses.

In such a case, the host A will update the ARP caches, and also change the status of the entries corresponding to the host B's IP addresses to" Resolved".

Suppose if within the timespan of the timeout, there is a situation that occurs wherein the host A will receive more than a single ARP reply, then we can confirm that one packet came from host B and the remaining packets came from attacker. We can now concur that host C is an attacker.

4. PROPOSED SYSTEM

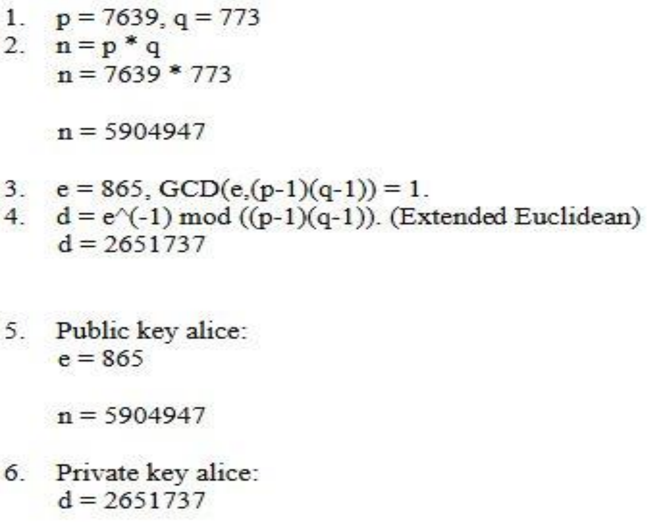
This man-in-the-middle-attack problem can be overcome by using an interlock protocol. The interlock protocol was coined by Rivest and Adi Shamir [15] The main algorithm of this protocol is that this protocol sends 2 parts of the main encrypted message.

The first part may be result of the one-way hash function of the message and the second part is always the encrypted message itself [1] [16].

This will cause the wiretapped person to be unable to decrypt the first message by using its own private key. It can now only create a new message and send it to the person who will receive the message [16].

In short, the workings of the interlock protocol are as follows:

1. A sends its public key to B.
2. B sends its public key to A.
3. Now A starts encrypting the message by using B's public key. Then, it sends part of this new encrypted message to B.
4. B encrypts its message using A's public key. Then, it sends a partially encrypted message to A.
5. Now again A will send another part to B.
6. B will now combine both the A messages and will decrypt using its private key.
7. B will now send the other piece to A.
8. A will now combine both of the B's messages and will decrypt using its private key.



1. p = 7639, q = 773
2. n = p * q
   n = 7639 * 773

   n = 5904947

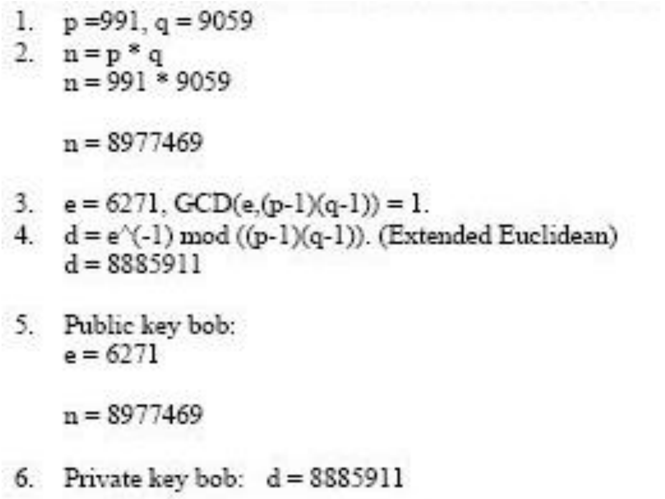
3. e = 865, GCD(e,(p-1)(q-1)) = 1.
4. d = e^(-1) mod ((p-1)(q-1)). (Extended Euclidean)
   d = 2651737

5. Public key alice:
   e = 865

   n = 5904947

6. Private key alice:
   d = 2651737

Fig -2: A person's Key Calculation (Alice)



1. p =991, q = 9059
2. n = p * q
   n = 991 * 9059

   n = 8977469

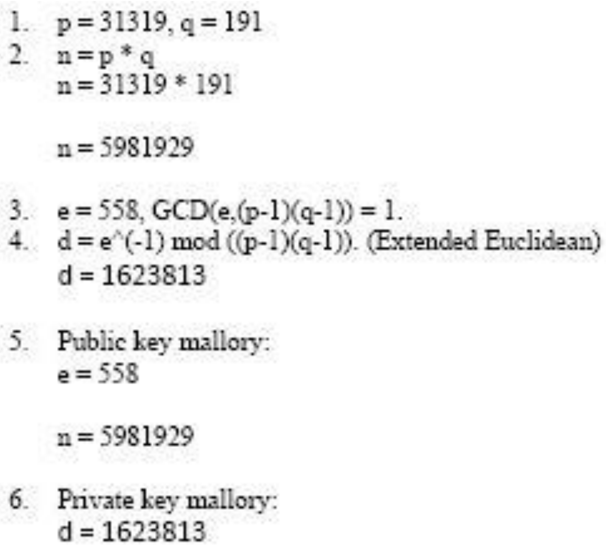
3. e = 6271, GCD(e,(p-1)(q-1)) = 1.
4. d = e^(-1) mod ((p-1)(q-1)). (Extended Euclidean)
   d = 8885911

5. Public key bob:
   e = 6271

   n = 8977469

6. Private key bob: d = 8885911

Fig -3: B person's Key Calculation (Bob)



1. p = 31319, q = 191
2. n = p * q
   n = 31319 * 191

   n = 5981929
3. e = 558, GCD(e,(p-1)(q-1)) = 1.
4. d = e^(-1) mod ((p-1)(q-1)). (Extended Euclidean)
   d = 1623813
5. Public key mallory:
   e = 558

   n = 5981929
6. Private key mallory:
   d = 1623813

Fig -4: Attacker's Key Calculation (Mallory)

5. CONCLUSION

The repeated sending of all the ARP requests to the router from the victim is very much effective and then depending on the refresh interval of the specific Address Resolution Protocol tables and the attackers code programming strategies, the result demonstrates the variety of solutions to the attack against varieties of ways to carry it out. For all the test conditions the refresh rate is less of the specified ARP table was effective to prevent man in the middle attack, this given values can incredibly vary which depends on all the characteristics of the attack. This defense was not so much effective when the attacker had launched an attack at an interval of a millisecond using threads. Another aspect which is to be noted in this solution is that the traffic which is being generated on the current network if all the hosts are permanently launching requests to the given router.

Here in this paper the script that runs on the client and maintains the ARP table updated, and the script that keeps monitoring the system by comparing the current record against one fixed. Thus, the solutions are complimentary with each other,

The static configuration of the specified MAC address of the host systems can be a strenuous task for the network admin and this should be considered when defining the set of measures that are being planned in order to secure the network.

REFERENCES

Radhakishan, V., & Selvakumar, S. (2011, September). Prevention of man-in-the-middle attacks using ID based signatures. In Networking and Distributed Computing (ICNDC), 2011 Second International Conference on (pp. 165-169). IEEE.

1. Bernal, A. J. P., Parra, O. J. S., & Díaz, R. A. P. (2018). Man, in the Middle Attack: Prevention in Wireless LAN. International Journal of Applied Engineering Research, 13(7), 4672-4671.

2. Kim, E., Kim, K., Lee, S., Jeong, J. P., & Kim, H. (2018, January). A Framework for Managing User-defined Security Policies to Support Network Security Functions. In Proceedings of the 12th International Conference on Ubiquitous Information Management and Communication (p. 85). ACM.

3. Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man in the middle attacks. IEEE Communications Surveys & Tutorials, 18(3), 2027-2051.

4. Bhushan, B., Sahoo, G., & Rai, A. K. (2017, September). Man-in-the-middle attack in wireless and computer networking—A review. In Advances in Computing, Communication & Automation (ICACCA)(Fall), 2017 3rd International Conference on (pp. 1-6). IEEE.

5. Patni, P., Iyer, K., Sarode, R., Mali, A., & Nimkar, A. (2017, June). Man-in-the-middle attack in HTTP/2. In Intelligent Computing and Control (I2C2), 2017 International Conference on (pp. 1-6). IEEE.

6. Rahim, R. (2017). Man-in-the-middle-attack prevention using interlock protocol method. ARPN J. Eng. Appl. Sci, 12(22), 6483-6487.

7. Katz, J. (2002). Efficient cryptographic protocols preventing" man-in-the-middle" attacks. Columbia University.

8. Meyer, U., & Wetzel, S. (2004, October). A man-in-the-middle attack on UMTS. In Proceedings of the 3rd ACM workshop on Wireless security (pp. 90-97). ACM.

9. Abad, C. L., & Bonilla, R. I. (2007, June). An analysis on the schemes for detecting and preventing ARP cache poisoning attacks. In Distributed Computing Systems Workshops, 2007. ICDCSW'07. 27th International Conference on (pp. 60-60). IEEE.

10. Karapanos, N., & Capkun, S. (2014, August). On the Effective Prevention of TLS Man-In-The-Middle Attacks in Web Applications. In USENIX security symposium (Vol. 23, pp. 671-686).

11. Trabelsi, Z., & El-Hajj, W. (2007, June). Preventing ARP attacks using a fuzzy-based stateful ARP cache. In Communications, 2007. ICC'07. IEEE International Conference on (pp. 1355-1360). IEEE.

12. Trabelsi, Z., & Shuaib, K. (2008). A novel Man-in-the-Middle intrusion detection scheme for switched

LANs. International Journal of Computers and Applications, 30(3), 234-243.

13. Burgers, W., Verdult, R., & Van Eekelen, M. (2013, October). Prevent session hijacking by binding the session to the cryptographic network credentials. In Nordic Conference on Secure IT Systems (pp. 33-50). Springer, Berlin, Heidelberg.

14. S. Glass, V. Muthukkumurasamy and M. Portmann. 2009. Detecting Man-in-the-Middle and Wormhole Attacks in Wireless Mesh Networks. in International Conference on Advanced Information Networking and Applications, Bradford, UK (PDF) Man-in-the-middle-attack prevention using interlock protocol method.

15. D. S. R. Murthy, B. Madhuravani, and G. Sumalatha. 2012. A Study on Asymmetric Key Exchange Authentication Protocols. International Journal of Engineering and Innovative Technology (IJEIT). 2(2)