Far East Journal of Electronics and Communications
Proceedings of SHANNON 100 - 3*rd Int. Conf. Comp. Sci.*, 2016

http://dx.doi.org/10.17654/ECSV3PII16273
Special Volume 3, Part II, 2016, Pages 273-282 **ISSN: 0973-7006**

AN EFFECTUAL APPROACH TO MITIGATE ARP POISONING BASED MAN-IN-THE-MIDDLE ATTACKS

Goldendeep Kaur and Jaideep Singh

Department of Computer Science Engineering
Guru Nanak Engineering College
Ludhiana, India

Department of Computer Science Engineering
CKD Institute of Management and Technology
Amritsar, India

Abstract

With the expeditious evolution in the field of computer networks, the cases of network intrusions and exploitations have increased to a great extent. ARP spoofing attack, an appalling technique that makes use of ARP protocol's defaults to assault the network and thereby destroying the communication between hosts by sending wrong IP/MAC addresses is one of the most being researched areas for preventive measures today. Even though large numbers of security measures have cropped up across the globe for prevention of ARP spoofing attacks but each approach lacks from different aspects. This paper proposes an idea to detect ARP poisoning in large organizations by verifying the authenticity of the user keeping in view the information maintained in the tables and using detection systems working independently at different departmental levels, in an effective way. In comparison to existing approaches worldwide, the proposed approach is more promising in terms of speed, perception and adaptability in

Conference held during April 8-9, 2016 at Lovely Professional University, Punjab, India.
Guest Editor: G. Geetha; Division of Research and Development, Lovely Professional University, Punjab, India.

different network scenarios. Thus, this paper is an endeavor to provide a holistic approach to solve the problem of man-in-the-middle attacks in wireless networks.

1. Introduction

In today's era, Internet has undergone an astounding growth. According to the most recent reports, the number of Internet users worldwide was 3.17 billion up from 2.94 billion in the previous year. Wireless technology is becoming popular day by day because of its low cost and convenience. No doubt, wireless networking allows users to gather, store, process and transfer vast amounts of data, including proprietary and delicate business, transactional and confidential data, but at the same time, businesses and consumers suffer heavily due to wireless attacks that continue to plague the Internet economy. Various types of attack tools have been developed to compromise 802.11 networks. The widespread use and popularity of wireless technology gives the attacker a dais through which they can cause most disruption. Cyber security threats are evolving as rapidly as the Internet is growing, and the associated risks are increasing worldwide. One of the most common attacks among these is the man-in-the-middle attack. When two users require communication with each other in a local area network, they require IP and MAC addresses of each other. Applications, which are above the layer four, use logical address to identify the destination host, i.e., IP address [1]. IP addresses are assigned to the hosts and are logically independent of the physical address. Mac address is the unique hardware address of a device that is assigned by the manufacturer. Now, source device that needs to communicate with other devices firstly checks its Address Resolution Protocol (ARP) cache to find if it knows the IP and MAC address of the destination device. If it is already in the ARP cache, then it uses that address for communication. On the contrary, only the IP address of the destination device is known and not the MAC address, an Address Resolution Protocol (ARP) request message is broadcasted into the network asking "who has so and so IP"? The message is received by each device on

the network, since it is a broadcast request. Each machine compares the target IP address with its own IP address. Those devices whose IP address does not match will drop the packet without any action. When the targeted device checks the target protocol address, it will obtain a match and construct an ARP reply message. The destination device sends the ARP reply message containing its IP and MAC address and it is a unicast. The source machine will process the ARP reply and update its ARP cache with the sender hardware address and sender protocol address, it receives from the reply [2].

Figure 1. Address resolution protocol.

As ARP does not offer any method for authenticating ARP replies in the network, these replies are vulnerable to be spoofed by other hosts on the network. Various existing intrusion detection systems take measures to detect the false binding. Snort-wireless™ is a much popular choice because of its open source characteristics. Other systems such as anticap and antidote are used to find the real and MITM hosts by rejecting the ARP reply different from that already in the cache, but these are used only for specific kernel. In a situation, when the attacker changes legitimate AP's MAC address using MAC spoofing technique, then nothing can be done to identify an MITM attack in a particular network. Staying protected against attacks requires all users, even the most experienced ones, to be aware of the threats and improve their security practices on a regular basis. Having strong network, security does not mean that one can prevent the network from being attacked it simply means that the security mechanisms implemented are just that secure and have not been broken yet. Computer and network security is constantly evolving and strong security mechanisms must also evolve to save the users across the world. So, this paper focuses on a new proposed solution to detect ARP spoofing by using a detection system based on the information maintained in the tables at various network levels.

The remainder section of this paper is organized as follows: Section 2 describes defence strategies, Section 3 describes the proposed idea, Section 4 describes the comparison of the proposed solution with the existing techniques, and finally, Section 5 concludes the paper.

2. Defence Strategies

Thus, in order to have reliable communication, one should be able to detect and actively mitigate such attacks. ARP cache poisoning on the network can completely go undetected if appropriate measures are not implemented. One of the simplest methods to mitigate this exploit is to use static ARP entries [2]. As static entries cannot be updated, spoofed ARP replies can be ignored. This method is not suitable for large networks as it requires manually adding each entry into the cache. Free detection systems like ARPWatch [5], XArp are working on detection mechanism but have not able to provide complete defence. On the other hand, port security detects MAC cloning significantly but does not prevent ARP spoofing. Dynamic ARP inspection [4], a technique proposed by Cisco switches allows the switch to block invalid <IP, MAC> pairings. It uses local pairing table that is built using a feature known as DHCP snooping to detect what pairings are invalid. A limitation to the use of these switches is high cost of switches that make this feature ineffective. From an exhaustive literature survey [6], every solution exhibits some cons and no universal defence mechanism was reported. Thus, taking into account the current scenario, a new algorithm has been developed and proposed through this research paper. The algorithm presented here detects ARP poisoning and raises alarm to the network administrators.

3. Proposed Idea

In the proposed work, a detection system to curb spoofing attacks has been put forward. In this context, a large organisation may be thought of as being divided into small virtual blocks. Each virtual block posses its own wireless local area network, such that all clients working in the distinct

blocks are connected to the network by a localised Wi-Fi (802.11b/g/n) modem. An information agent working on each client machine sets up the required platform for detection of ARP spoofing in an effective manner. In addition to the information agent, each virtual block has a centralised detection system. For proper working of the system, it becomes evident to determine that the information agents and the detection systems of subsequent virtual blocks communicate in a proper manner. The information agent undertakes the following responsibilities to ensure the proper functioning:

(1) When a machine needs to join the wireless network by issuing an ARP request, information agent on that machine should inform this event to the detection system of the particular block.

(2) When the machine has connected with the subsequent access point in a virtual block, it must send the IP-MAC binding pair to the detection system, to be stored in the memory of detection system.

(3) In a similar manner, when a machine sends the ARP reply, IA must inform this event to the detection system.

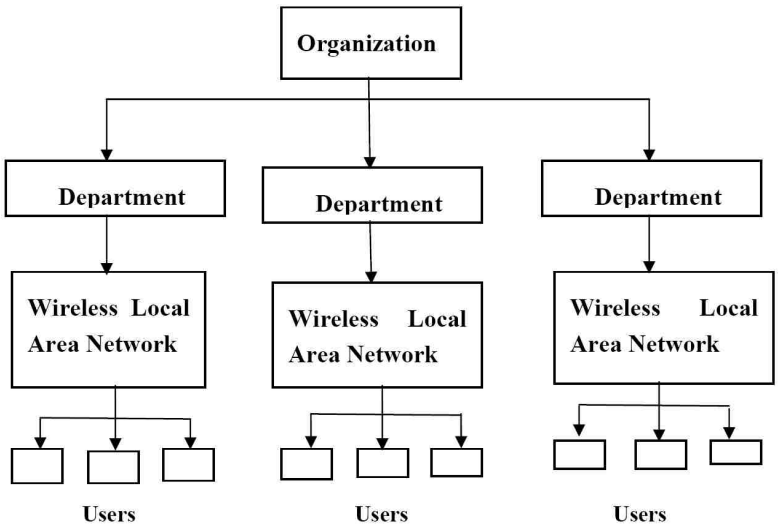

Figure 2. Model of the proposed system.

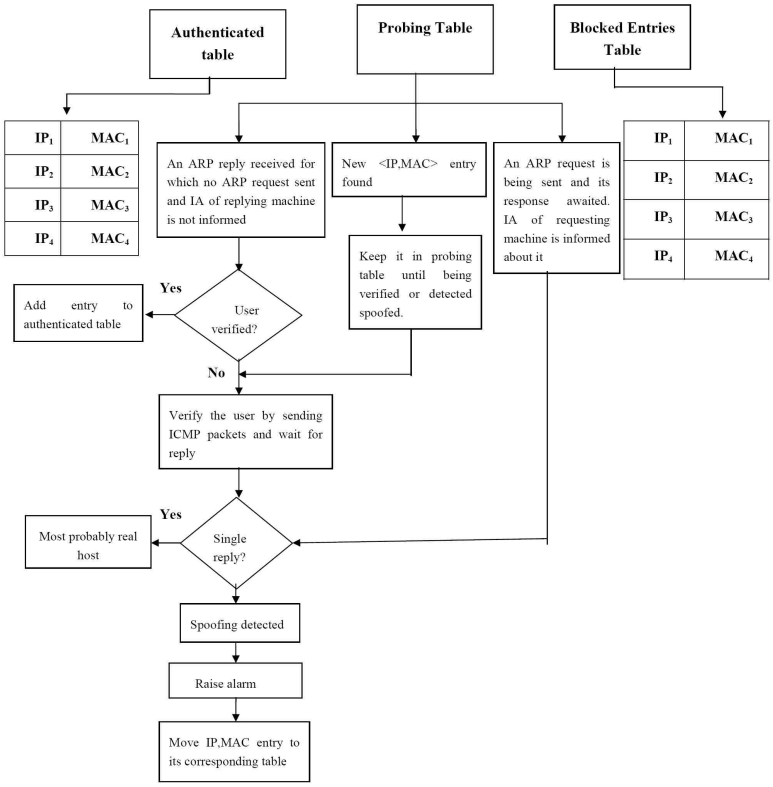

Figure 3. Flowchart of the proposed system.

Keeping in view the information collected by the detection system of various virtual blocks from the respective information agents, the tables namely verified entries table, probing table and blocking table must be maintained. The verified entries table keeps a record of all the ARP bindings between the clients and the servers in a virtual block. The probing table must keep a track of all the ARP replies that are received at the server end, that were not sent an ARP request for. This table confirms the possibility of ARP spoofing in a particular virtual block and further probe can be carried out on the basis of this information. Furthermore, to strengthen this claim, in case an attacker is carrying out an ARP poisoning attack in a particular block, ICMP packets are sent to the MAC address of spoofing client machine. Based on number of replies received, it can be made sure whether the host is

genuine or fake. The new entries (IP, MAC) must be kept in the probing table until they are verified clear, or been detected fake. Those entries in the probing table that are identified fake are moved to yet another table maintained by the detection system, the blocking table. All the blocked entries that have been detected as fake by issuing out ICMP packets and monitoring the replies are permanently stored in this table.

4. Comparison with Existing Techniques

It has been observed that the technique proposed in Section 3 of the paper is expeditious and reliable due to the following reasons:

- **Scalability.** It can be used in large networks to detect ARP poisoning attacks because the time lag between ARP attack and its detection is very less. So it is better than the existing passive techniques.

- **Network overhead.** It does not blindly add the unknown traffic in the ARP cache but firstly verifies the authenticity of the unknown ARP packets by sending one ICMP echo request per newly seen packet.

- **Compatibility.** Our solution is backward compatible with address resolution protocol and can be easily matched to run on dynamic environments.

5. Conclusion

In this paper, an adequate mechanism to overcome the limitations faced by the existing schemes has been proposed. The technique is scalable and perceptive in detecting ARP poisoning attacks. Furthermore, there is an injection of a single ICMP echo request for each newly seen packet to probe the authenticity of unknown traffic. An added advantage of this feature is that this decreases the traffic overhead by a great deal. Apart from being an active approach, as the time lag between the attack and its detection is very less, the system promises to detect the real mapping during an ongoing assault. In the end, as a future scope, the work may be extended by

accomplishing experimental observations keeping in view the proposed method under varied 802.11 network conditions, including real time scenarios under which ARP spoofing attacks usually occur.

References

[1] S. Whalen, An introduction to ARP spoofing, 2600: The hacker quarterly 18(3) (2001), Available: http://servv89pn0aj.sn.sourcedns.com/_gbpprorg/2600/arp spoofing intro.pdf

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

[3] M. Carnut and J. Gondim, ARP spoofing detection on switched ethernet networks: a feasibility study, Proceedings of the 5th Simpósio Segurança em Informática, 2010.

[4] Cisco Systems, Configuring Dynamic ARP Inspection, Chapter 39 (2012), 1-22. Catalyst 6500 Series Switch Cisco IOS Sofware Configuration Guide, Release 12.2SX.

[5] L. N. R. Group, Arpwatch, the ethernet monitor program; for keeping track of ethernet/ip address pairings (last accessed April 17, 2012).

[6] Snort Project, The Snort: The Open Source Network Intrusion Detection System, http://www.snort.org.

[7] Jaideep Singh, Goldendeep Kaur and Jyoteesh Malhotra, A comprehensive survey of current trends and challenges to mitigate ARP attacks, Proceedings of 1st Inter. Conf. on Electrical, Electronics, Signals and Optimization, IEEE, 2015.

[8] ARP-Guard (accessed 28-July-2013): http://www.arp-guard.com.

[9] Zouheir Trabelsi and Khaled Shuaib, Spoofed ARP packets detection in switched LAN networks, J. Filipe and M. S. Obaidat, eds., ICETE 2013, CCIS 9, pp. 81-91.

[10] M. Barnaba, Aanticap (accessed 17 April 2013): http://www.antifork.org/anticap.

[11] V. Goyal and V. Abraham, An efficient solution to the ARP cache poisoning problem, Proc. of 10th Australasian Conf. on Information Security and Privacy, July 2013, pp. 40-51.

[12] I. Teterin, Antidote, Security Focus: http://online.securityfocus.com/archive/1/299929 (last accessed, Apr. 2012).

[13] M. Gouda and C.-T. Huang, A secure address resolution protocol, Computer Networks 41(1) (2012), 57-71.

[14] H. Neminath, S. Biswas, S. Roopa, R. Ratti, R. Nandi, F. A. Barbhuiya, A. Sur and V. Ramachandran, A DES approach to intrusion detection system for arp spoofing attacks, 18th Mediterranean Conference on Control and Automation (MED), IEEE, 2010.

[15] Wenjian Xing, Yunlan Zhao and 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: 10.l109IETCS.2010.75, 2010 IEEE.

[16] Somnuk Puangpronpitag and Narongrit Masusai, An efficient and feasible solution to ARP spoof problem, 6th International Conference on Electrical Engineering Electronics, Computer, Telecommunications and Information Technology, ECTI-CON 2009.

[17] D. Bruschi, A. Omaghi and E. Rosti, S-ARP: a secure address resolution protocol, Annual Computer Security Applications Conference (ACSAC), 2003.

[18] Craig A. Shue, Andrew J. Kalafut and Minaxi Gupta, A unified approach to intra-domain security, Inter. Conf. on Computational Sci. and Engineer., IEEE, 2009.

[19] Yunji Ma, An effective method for defense against IP spoofing attack, 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM), IEEE, 2010.

[20] Haining Wang, Cheng Jin and Kang G. Shin, Defense against spoofed IP traffic using hop-count filtering, IEEE/ACM Transactions on Networking l5(1) (2007), 40-53.

[21] Lei Wang, Tianbing Xia and Jennifer Seberry, InterDomain routing validator based spoofing defence system, International Conference on Intelligence and Security Informatics (lSI), IEEE, 2010.

[22] Dalia Nashat, Xiaohong Jiangand and Susumu Horiguchi, Detecting SYN flooding agents under any type of IP spoofing, IEEE International Conference on eBusiness Engineering, IEEE 2008.

[23] Wei Chen and Dit-Yan Yeung, Defending against TCP SYN flooding attacks under different types of IP spoofing, International Conference on Networking, International Conference on Systems and Inter. Conf. on Mobile Communications and Learning Technologies, IEEE 2006, ICNIICONS/MCL 2006.

[24] Zhenhai Duan, Xin Yuan and Jaideep Chandrashekar, Controlling IP spoofmg through inter domain packet filters, IEEE Transactions on Dependable and Secure Computing, Issue: Jan.-March, 2008.

[25] N. Borisov, Computational puzzles as sybil defenses, Proc. IEEE International

Conference on Peer-to-peer Computing, 2006.

[26] B. Parno, D. Wendlandt, E. Shi, A. Perrig, B. Maggs and Y.-C. Hu, Portcullis: protecting connection setup from denial-of-capability attacks, Proc. SIGCOMM, Kyoto, Japan, 2007.

[27] Gratuitous ARP – The Wireshark. Wiki.<http://wiki.wireshark.org/Gratuitous_ARP>.

[28] T. Sakurai and H. L. Vu, MAC access delay of IEEE 802.11 DCF, IEEE Transactions on Wireless Communications 6(5) (2007), 1702-1710.

[29] P. Chatzimisios, A. C. Boucouvalas and V. Vitsas, IEEE 802.11 packet delay - a finite retry limit analysis, Prof. of IEEE Globecom, 2003.

[30] C. M. Koksal, H. Kassab and H. Balakrishnan, An analysis of short-term fairness in wireless media access protocols, Prof. ACM SIGMETRICS, 2000.

[31] Z. Fang, B. Bensaou and Y. Wang, Performance evaluation of a fair backoff algorithm for IEEE 802.11 DFWMAC, Prof. ACM MOBIHOC, 2002.

[32] Z. Li, S. Nandi and A. K. Gupta, Modeling the short-term unfairness of IEEE 802.11 in presence of hidden terminals, Performance Evaluation 63(4) (2006), 441-462.

[33] SSLSTRIP, Retrieved 2012, 2009, from thoughtcrime.org: http://www.thoughtcrime.org/software/sslstrip/.

[34] Symantec-Norton, Two attacks against VoIP, Retrieved, 2012, from Symantec connect: http://www.symantec.com/connect/articles/two-attacks-against-voip

[35] S. N Vivek Ramachandran, Detecting ARP spoofing: An active technique, Retrieved March 5, 2012, from vivekramachandran.com: http://www.vivekramachandran.com/docs/arpspoofing.pdf

[36] N. Donato, Poisoning attack and mitigation techniques, Retrieved from Windows ARP attack tools: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white, 2005.

[37] T. Frias, Cisco security-enabling the self defending network, 1995. Retrieved from spoofing an IP address: http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/

[38] B. Tony, Catalyst 6500 Configuration Guide, Cisco Dynamic ARP (DAI), 2007.

[39] B. Cox, How Does ARP Work, 2005.

[40] N. Desai, Cisco VLAN security white paper, 2007, Retrieved from Virtual LAN Security Best Practices: http://www.cisco.com/en/US/products/hw/switches/ps708/