Root Services Blog, Vol. I, No. 2, 2015
Copyright Root Services, 2014

# Man In the Middle (MITM) ARP Cache Poisoning Explained

Alexander Chopra[1]*, Michael Kaufman[2]

**Abstract**
This paper will detail ARP cache poisoning at a high level. The methods in which an attacker can poison the ARP cache such that they can eavesdrop on network traffic is explored. Details of of the process of ARP cache poisoning are explored as well as the OSI model in reference to the ARP cache.

**Keywords**
Man in the Middle — MITM — ARP Cache Poisoning

[1] *Research and Development, Root Services, Rockville, Maryland, United States*
[2] *Research and Development, Root Services, Rockville, Maryland, United States*

## Contents

**Introduction** 1
**1 Man in the Middle** 1
1.1 Utilization . . . . . 1
1.2 ARP . . . . . 1
1.3 ARP Cache Poisoning . . . . . 2
1.4 Open Systems Interconnection Model . . . . . 2
**2 Conclusion** 2
**Acknowledgments** 2
**References** 2

## Introduction

The motivations behind an attacker going after a business or individual generally involve financial gain or activism by information gained. This paper will focus on man in the middle type attacks and ARP (Address Resolution Protocol) poisoning. There are various types of man in the middle attacks that can be launched, including: ARP cache poisoning/spoofing, DNS (Domain Name System) spoofing, session hijacking and others. Man in the middle attacks are based off the concept of interception: before the recipient receives their data it is intercepted, but the two communicating parties believe they are still communicating directly with each other. In the event of a man in the middle attack, the communication is flowing from the sender to the attacker to the receiver as opposed to directly from the sender to receiver. This added hop to the attacker allowing the attacker to intercept data and manipulate it. Man in the middle attacks are able to fully monitor and modify traffic that is occurring between various LANs (Local Area Network).

## 1. Man in the Middle

### 1.1 Utilization

The utilization of man in the middle attacks is widely seen due to the unexpected nature of the attack. Typically, clients are not expecting an attacker to be between their network communications and are not aware how the attack itself is carried out. As a result of the high level of trust generally seen, clients usually approve or disregard any error or alert messages and continue with their activities, not realizing what was prompted to them.

### 1.2 ARP

The ARP is the protocol that is responsible for converting an IP address into a physical address or MAC (Media Access Control) address. The ARP protocol works on just a few message types ranging from a request for identification of an IP address and associated reply as well as a reverse ARP request which petitions the devices on the network to identify the IP address associated with a particular MAC address. The major flaw with the ARP protocol is that there is no authentication associated with the ARP requests. A host has no way of knowing if it actually generated an ARP request for which it is receiving ARP replies for. Whatever information that is received by a host is directly updated in the ARP cache without verification. An attacker in this case sending an ARP

reply to a host would be able to have routing altered through them and have that information saved in the ARP tables of the host.

All devices that are able to connect to the network have their own ARP table. The ARP table holds information about the various IP addresses and associated MAC addresses that the device has linked together. When an ARP request is sent out from a host, only the host which the ARP request matches are supposed to respond to the request with its appropriate information. For example, if there are five devices on an example network and the first device is looking for a particular IP address, let's say 192.168.0.4, only the device which is sitting on that IP address (if any) responds to the ARP request with their associated MAC address. All of the other hosts on the network remain silent while this request is being sorted. ARP has the added benefit of acting as a broadcast or an announcement tool for the rest of the devices on a particular network. A gratuitous ARP request or reply can be useful in the case of updating other machines ARP tables, but is also effective in assisting to poison them. Typically these types of gratuitous messages are sent by legitimate purposes when a computer reboots or when an IP conflict is being resolved. The process of tricking the protocol into adding altered information in the ARP cache table is coined ARP cache poisoning.

### 1.3 ARP Cache Poisoning

The process of ARP cache poisoning is effective as the ARP tables automatically refresh as new information is received. An attacker could as a result of this automatic refreshing, bombard a device with ARP replies. The bombarding of the device with fake replies would override, through brute force, any legitimate replies from the network, allowing an attacker to assume control.

To assist in the protection of networks against ARP cache poisoning attacks, which can leverage network devices to assist in a man in the middle attack, static ARP tables can be used for smaller networks. In the case of smaller networks, there are generally only a few devices that are connected to the network at a time and as a result are easy to monitor. In larger networks, there are many more devices that are coming and going offline on a regular basis and as a result is much more time consuming and difficult to keep up to date with. For smaller networks, the IP (Internet Protocol) address and MAC address of all of the devices on the network can be entered into a static ARP table. The static ARP tables give benefit to the network as it can prevent attackers from changing ARP tables. Automation can be generated such that the static ARP entries can be applied at boot. The various hosts on the network can be directed to ignore all ARP replies that are sent out in attempts to update those tables that are defined[1].

Even with the change of using static ARP tables, it is still possible that an attacker could manipulate the system in such a way to gain access to communications on the network. There are tools such as arpwatch that monitor the ARP traffic on a network assisting to detect ARP spoofing attacks. These types of tools create logs of pairings between an IP address and a MAC address and stores them all into a log for analysis. The tool, because of its log of previous correlations between MAC addresses and IP addresses, is able to see when there is something fishy happening on the network where a third party is trying to make changes to the association that is happening on the network[2].

### 1.4 Open Systems Interconnection Model

The OSI (Open Systems Interconnection) model separates networking protocols into seven distinct layers. The various layers include: the physical layer, the data link layer, the network layer, the transport layer, the session layer, the presentation layer and the application layer[3]. A drawback to the arpwatch tool is the inability for it to detect all traffic on the subnet. The tool cannot be used for monitoring of an entire network because it cannot send over Layer 3 (network link layer). A second subnet would not receive the information that the first subnet would have upon an ARP reply or request. It is possible depending on the configuration of the network that the various subnets might not see all of the ARP activity that is occurring on them, resulting in them not knowing the locations of the hosts on the alternate subnets. In order to overcome the limitations that are seen by arpwatch "implementation of networks utilizing mirrored ports on uplinks, tagged VLANs have been developed to increase the amount of ARP request and ARP reply traffic" that is observable by arpwatch[4]. ARP packets do not contain IP headers nor are they able to be routed. ARP is considered a layer 2 service that provides assistance for layer 3 services. ARP can be thought of in this sense as the bond that connects the second and third layers of the OSI model together.

## 2. Conclusion

ARP poisoning is something that is relatively easy to accomplish and is a great example of a passive man in the middle attack that can be carried out on most networks. Although the attack is very simple, the nature of the protocol itself, not having any verification procedures makes it an attack that is still a very real threat to modern networks. Detection of the attack taking place, often only happens after the attacker has left and the purpose of the attack has already been carried out. It is important to be proactive with network monitoring and to flag irregularities before they become an issue.

## Acknowledgments

This section needs to be redone.

## References

[1] A. Lockhart. Network security hacks. O'Reilly Media, Inc., jan 2006.

[2] F. Beck, T. Cholez, and I. Chrisment. Monitoring the neighbor discovery protocol. *HAL archives-ouveres*, 1, mar 2007. https://hal.inria.fr/inria-00153558/document.

[3] T. G. Handel and M. T. Sanford II. Hiding data in the osi network model. *Information Hiding*, 1:23–38, jan 1996. Springer Berlin Heidelberg.

[4] P . Kwan. U.s. patent no. 7,562,390. U.S. Patent and Trademark Office, jan 2009. Washington, DC.