# Intrusion Tolerant ARP Spoofing Detection and Prevention System

[1]Avinash Dhanshetti, [2]Meghan Kulkarni, [3]Dipali Bhosale, [4]Amit Das, [5]Vijay D. Katkar.
[1,2,3,4,5]Department of Information Technology,
Pimpri Chinchwad College of Engineering,
Pune, Maharashtra, India.

**Abstract** - The Address Resolution Protocol (ARP) is used by computers to map network addresses (IP) to physical addresses (MAC). The protocol has proved to work well under regular circumstances, but it was not designed to cope with malicious hosts. By performing ARP cache poisoning or ARP spoofing attacks, an intruder can impersonate another host (man-in-the middle attack) and gain access to sensitive information. This paper presents Intrusion Tolerant ARP Spoofing Detection and Prevention mechanisms. Experimental results are also provided to support the proposal.

**Index Terms** - ARP Spoofing, ARP Cache Poisoning, Spoofing Detection and Prevention.

## I. INTRODUCTION

The Address Resolution Protocol (ARP) is used to derive Media Access Control address i.e., MAC address of a machine given machine's IP address. MAC address is used to send packets over a network to destination host. Initially, this MAC address is not known to sender of packet. It is derived using ARP protocol. The working of ARP protocol is as follows:

i. Sender of Packet generates ARP Request, This request is locally broadcasted to all nodes in a LAN
ii. Ideally, intended receiver replies with its MAC address encapsulated in ARP reply
iii. Now sender receives this ARP reply and stores MAC address of destination host into its local cache.
iv. Using this MAC address sending host can deliver Data packets to destination host.

ARP protocol does not have Verification Process. That means it does not check whether ARP reply received is valid or not. It simply updates its local cache. Attacker can simply create a fake reply packet. Attacker sends this fake packet to victim where fake MAC address gets updated. It is explained subsequently:

i. Attacker observes ARP request in a network
ii. When ARP request is observed, attacker allows ARP reply from actual destination
iii. When ARP reply is received from actual receiver, attacker creates a fake reply packet and sends it to Victim with its MAC address.
iv. In this way, communication is intercepted and attacker is able to divert network traffic between two hosts through itself
v. This phenomenon is called ARP Cache Poisoning

ARP Cache Poisoning Scenario is explained with the help of figure 1.1. Here, host B generates fake ARP Reply packet and poisons host A & B's cache as shown in above Fig. 1. So, all communication intended between hosts A & C will flow under control of host B. In this way, because of stateless behavior of ARP, attacker can easily launch attacks such as those explained below.

The rest of this paper is organized as follows. Section 2 gives brief introduction of ARP spoofing based attacks. Section 3 gives overview of research work done for detection and prevention of ARP spoofing based attacks. Proposed mechanism for Intrusion Tolerant ARP Spoofing Detection and Prevention is discussed in Section 4 and Section 5 presents the experimental results. Section 6 concludes the paper while Section 7 presents Future Enhancement.

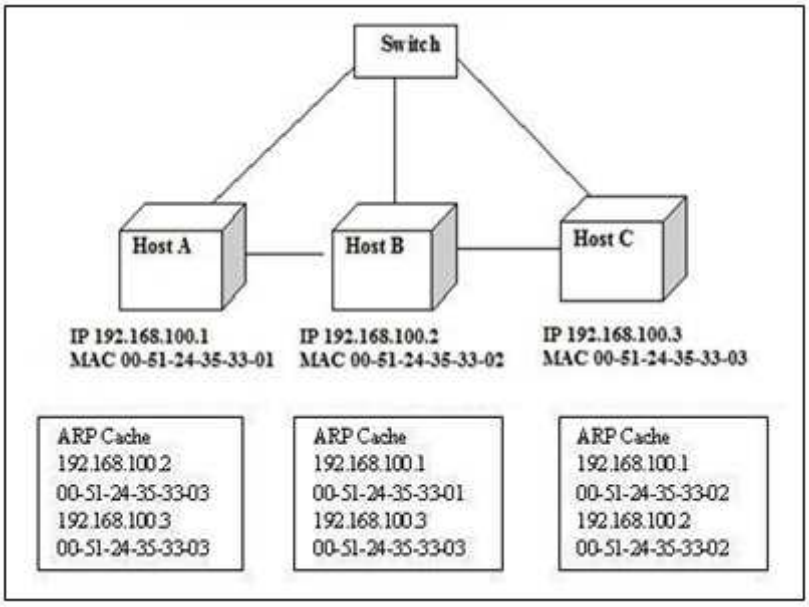


Figure 1.1: ARP Cache Poisoning

## II. ARP SPOOFING-BASED ATTACKS

ARP Spoofing means generation of fake ARP request and reply messages to launch attacks such as Denial-of-Service (DOS) explained subsequently. It is used by the attackers to gain access to unauthorized information from a network.

ARP Spoofing Based Attacks:

1) Denial-of-Service (DoS) Attack:
   Using ARP spoofing to launch Dos attack, attacker changes ARP cache of hosts such that all communication is blocked temporarily. So some hosts are unable to access authorized services for e.g., Internet Bandwidth.

2) Distributed Denial-of-Service (DDoS) Attack:
   Large no. of Spoofed IP packets are sent towards the server from a large number of distributed machines. This will abrupt the normal working of the system and the server cannot provide services to the clients.

3) Man-in-The-Middle (MiTM) Attack:
   The attacker launches Man-In-The-Middle Attack by creating fake ARP entries in cache of two hosts. In this way, the attacker can observe as well as traffic between two hosts. This traffic may contain sensitive information such as passwords, etc.

## III. RELATED WORK

To prevent ARP Spoofing, easiest way is to add static ARP entries of victim. But this is not ideal in case of a large organization. Neminath Hubballi et al. [2] have developed a Discrete Event System (DES) based network IDS is used for detecting ARP related attacks. A DES is characterized by a discrete state space and some event driven dynamics. All such systems either make IP-MAC pairing static or modify existing ARP. However, to change core ARP structure in not recommended at all. Somnuk Puangpronpitag et al. [3] have proposed a light weight mechanism where the System Administrator has the responsibility of maintaining static IP-MAC entries of connected clients. Craig A. Shue et al. [4] have used the concept of Secure DHCP and issuing of Certificate for authenticity of ARP reply message. But the discrepancy of the proposed mechanism is that it requires modification in the implementation of ARP protocol.

Vijay Katkar et al [1] have proposed Light Weight Approach for IP-ARP Spoofing Detection and Prevention but the drawback of the proposed

mechanism is that it is not Intrusion Tolerant and it cannot detect IP spoofing attacks launched from the LAN against the LAN itself. The remaining proposed mechanisms [6, 8] to detect and prevent IP spoofing based attacks. But none of these can detect and prevent IP spoofing at the organizational level.

The middleware approach proposed by Tripunitara et al. [5] is not practical, as it requires changes on all the hosts in the network, and no implementation is widely available. Carnut et al. [7] have proposed an ideal mechanism for reducing wrong alerts, but it has the disadvantage of building complex setup, and software is not available yet. ARP-Guard tool [8] may be a good choice, but it is not free, although other tools like arpwatch [9] and Snort [6] are free, they tend to generate a high-number of false positives, increasing the work of the network administrator.

## IV. PROPOSED MECHANISM

This paper proposes following mechanism to prevent ARP Spoofing:-

i. Initially, client registers by sending its own (IP, MAC) pair to Main Server.
ii. Server notifies the received (IP, MAC) pairs of all clients connected in LAN till that point of instance.
iii. Server publishes information of newly connected clients to all other clients connected in LAN.
iv. Packet Captor starts capturing ARP packets from network and it sends to packet analyzer module for analysis.
v. If any fake packet is detected by packet analyzer then IA takes proper action for preventing spoofing activity.
vi. Simultaneously, main server continuously communicates with IA and if IA is found terminated then main server remotely restarts IA.

Intrusion Tolerant ARP Spoofing Detection and Prevention contains following 4 modules:

i. ARP Packet Capturing
ii. ARP Spoofing Detection
iii. ARP Spoofing Prevention
iv. Intrusion Tolerance

Figure 4.2 shows proposed system architecture. **Main Server** is a component to which hosts in LAN register themselves by sending their IP-MAC. This information is sent to all other IA's. Also Main Server is responsible for remotely restarting IA.

**Information Agent (IA)** is a component which includes Packet Captor, Packet Analyzer and Intrusion Tolerance sub-components. IA resides on each Client machine in LAN.

**Packet Captor** is a sub-component which captures ARP Packets from a network and sends to Packet Analyzer.

**Packet Analyzer** is a sub-component which checks ARP Spoofing. Packet Analyzer has a Hash table which contains IP-MAC pairs of all clients registered initially. Based on the packet received from Packet Captor, Packet Analyzer decides ARP Spoofing is present or not.

**Intrusion Detection** is a sub-component which continuously monitors IA running at client side. When Intrusion Detection detects IA is terminated then Main Server remotely restarts IA without any human intervention.

## V. EXPERIMENTAL RESULTS

Experimental Results were held on machine having Intel® Dual Core Processor (2.0 GHz) having Microsoft® Windows XP platform. Information Agent (IA) is deployed on every host machine in LAN. It includes components explained above. Main Server is deployed on administrator machine in LAN.

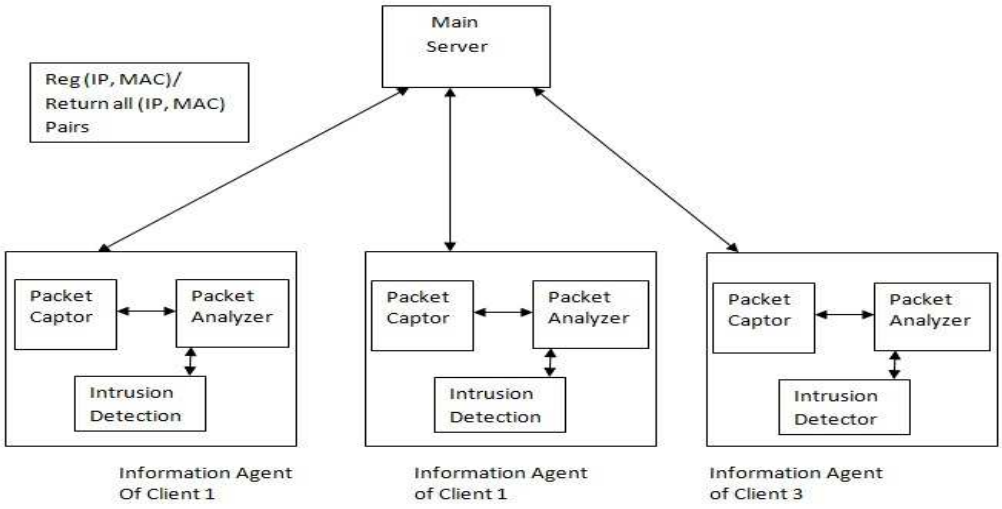


Figure 4.2: Proposed System Architecture

Following results were observed in experimental analysis:

A. Scenario 1:
We have generated fake ARP reply packets and sent these packets over a network. The attacker whose IA registers itself initially, sent its original IP-MAC to Main Server. When attacker created fake ARP reply packets, it was detected by IA residing locally. IA when detected Spoofing took action by adding Static IP-MAC entry in local ARP cache of victim.

B. Scenario 2:
When IA was killed by an Intruder, Main Server was informed about this event. So, in response to this, Main Server remotely restarted IA on intruder machine. In this way proposed mechanism is able to handle Intrusion.

C. Scenario 3:
In worst case scenario Main Server was crashed. This event was notified by sending an e-mail to administrator. In this way, without any human intervention, failure of Main Server was also handled.

## VI. CONCLUSION

Proposed mechanism for ARP Spoofing Detection and Prevention has following features:

i. Proposed mechanism for ARP Spoofing Detection and Prevention do not alter basic ARP protocol.
ii. It can detect as well as prevent attacks such as MiTM, DoS.
iii. Proposed System is Intrusion Tolerant.
iv. Detection, Prevention and Intrusion Tolerance do not involve any human intervention.

## VII. FUTURE ENHANCEMENT

Proposed Intrusion Tolerant ARP Spoofing Detection and Prevention mechanism works in wired LAN. We can easily install Information Agent on each client machine. But when we consider Wireless Environment, it is not feasible to install Information Agent on each client machine. Also, wireless environment is ad hoc in nature. So, future scope of our project is to implement proposed mechanism in wireless environment.

## REFERENCES

[1] Dr. S. G. Bhirud, Prof. Vijay Katkar Light weight approach for IP-ARP Spoofing detection and prevention, IEEE 2011.
[2] Neminath Hubballi, Santosh Biswas, S. Roopa, Ritesh Ratti, Sukumar Nandi,"LAN Attack Detection using Discrete Event System" ISA Transactions, August 2010
[3] Somnuk Puangpronpitag, Narongrit Masusai, An Efficient and Feasible Solution to ARP Spoof Problem, IEEE 2009
[4] Craig A. Shue, Andrew J. Kalafut, Minaxi Gupta, A Unified Approach to Intra-Domain Security, IEEE 2009.
[5] M. Tripunitara and P. Dutta. A middleware approach to asynchronous and backward compatible detection and prevention

of ARP cache poisoning. In Proceedings of the 15th Annual Computer Security Applications Conference (ACSAC 99), Dec. 1999.
[6] Snort Project, The. Snort: The open source network intrusion detection system, 006. <http://www.snort.org>.

gz>

[7] M. Carnut and J. Gondim. ARP spoofing detection on switched Ethernet networks: A feasibility study. In Proceedings of the 5th Nov.2003.
[8]ARP-Guard. <http://www.arp-guard.com>.
[9] L. N. R. Group. arpwatch, the ethernet monitor program; for keeping track of ethernet/ip address pairings.
<ftp://ftp.ee.lbl.gov/arpwatch.tar.