

**School of Computer Science and Engineering (SCOPE)**

**B.tech- Computer Science and Engineering**

**CSE3501 – Information Security Analysis and Audit**

**J Component**

**Review-1**

Title: Mitigating ARP spoofing-based attacks on IOT systems

Submitted By

Jaivant Vassan – 19BCE2322

Divakar.A.S – 19BCE2337

Kabhilan S – 19BCE2339

B.S.Sandheep – 19BCE2341

Prithvi Saran S – 19BCE2344

Faculty: Dr. Vimala Devi K

Slot: L9 + L10

**ABSTRACT:**

ARP poisoning (also known as ARP spoofing) is a form of LAN-based cyber-attack that includes delivering malicious ARP packets to a LAN's default gateway in order to alter the IP to mac address table's pairings. IP addresses are translated into mac addresses via the ARP mechanism. Because the ARP protocol was created for efficiency rather than security, ARP poisoning attacks are relatively simple to carry out as long as the attacker has control of or is directly connected to a computer on the target LAN.

**PROBLEM STATEMENT**

ARP has a few fundamental security issues since it changes the host's ARP cache table in the absence of trustworthy mutual agreement processes while delivering request/reply messages. The attacker takes advantage of this lack of verification to manipulate the cache table by broadcasting fake ARP packets association his/her own MAC address to the IP address of the target or vice versa. The latter creates the perfect conditions for attacks like DOS and the former could lead to massive data leaks.

The most efficient method to prevent ARP spoofing is making the network as secluded as possible i.e., making it difficult for external devices to access the network.

That is why IFTTT based networks are in risk, as they have relaxed rules on addition of new devices on the network.

IOT based systems like smart homes often comprise of IFTTT(if this, then that) based applets to give users more freedom on modifying the interoperability of the devices.A very good example would be home security systems whose interface apps often allow users to add more devices to the IOT network. While this freedom often helps in ease of access and efficiency, it severely compromises the security of the network by creating potential entry points for attackers.

**OBJECTIVE:**

We plan to implement a model that makes it very hard for the attackers to have their fake ARP packets validated while compromising as little as possible.

A successful ARP spoofing-attempt allows the attacker to open up the network for various risks like Man in the Middle attack, Denial of Service etc., We plan to analyse a home automation system for suitable circumstances for attacks and the potential risks they pose and also estimate the damage to the network and its devices should an attack prove successful.

Then we plan to compare and analyse the impact our solution would have in mitigating the possibility of these risks while also taking into account the loss in efficiency because of the methods employed by our model.

**LITERATURE SURVEY:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Paper Details** | **Problem and Objectives** | **Proposed Methodology** | **Limitations** |
| A New Detection and Prevention System for ARP Attacks Using Static Entry  S. Hijazi and M. S. Obaidat  IEEE Systems Journal, Sept. 2019 | This paper proposes a new static IP-MAC approach for LAN  specific client-server architecture, which does not need any extra constraint to fix ARP security problem. This approach was  built for LANs under a static IP address settings. The experiments are conducted on different measurements of detection  and prevention ARP attacks to find out the best results. | The idea used in this paper to prevent the ARP poisoning attacks is through a simple static entries solution where the dynamic IPMAC is mapped to the static state. There are many tools which are there to detect the arp attack for example ARPwner,wind ow ARP spoofed etc, But none of these software protect from ARP attack. In this particular paper they have adopted passive and active approach | 1) The TCP is a stateful protocol. Thus, unlike ARP, replies will not be processed unless a request has been made.  2) The TCP uses sequence number and acknowledgement numbers for sequencing packets. These also provides authorization to packet. That is, a malicious node on the network cannot inject TCP packets in the communication. |
| Mitigation for Brute Force Attack against  IP/CCTV Camera Login  Devang Thakar, Hepi Suthar  IJRASET, Mar 2020 | The researchers aim to evaluate the  different vulnerabilities of the IP camera which can be used by attackers to exploit and misuse the IP camera. Their finding shows  the different vulnerabilities of the IP camera and not much strong mitigation system to prevent against those vulnerabilities. They aim to  suggest a method to counter Brute Force attack and reiterate the need of good login system. | First of all when user opens the portal of ip camera he/she will see the registration page where he/she has to  fill-up the details such as username, password, email id. Along with the basic details one more thing he/she has to input for  registration which is an image of his/her choice. The only allowed file types for the image are PNG, JPG and JPEG. As soon as user  enters the details and click on registration button. System will fetch the hash value of the image file using MD5 and SHA1 hashing  algorithms. After fetching the hash value system will encrypt that hash value and finally store that value into the database. During login the user must upload the same image and only if the hashes match can the user login. | 1. MD5 crypt's 128-bit output size would become the limiting factor in security. A brute force attacker could more easily find short strings hashing to the same value as a user's password than guess the actual password.  2. SHA-1 provides insufficient protection against collision attacks. An attacker could iterate over all possible combinations of secret key, creating a new hash until a matching hash was found. |
| Address Resolution Protocol Based Attacks: Prevention and Detection Schemes.  Francis Xavier Christopher D., Divya C.  ICCBI 2018 | This  paper discusses about the ARP poisoning attacks and focuses on reviewing  various mechanisms developed for attack detection and prevention with specified analysis to their advantages. Different attack detection and mitigation  methods are evaluated in addition to comparison in terms of key parameters.  This study helps in understanding the strategy employed for ARP attack  detection and mitigation and developing a framework for improvement. | Several solutions have been proposed for manipulate the ARP poisoning problem. The ARP watch, ARP Guard are manual solutions, so these depend on administrator to process the ARP cache, which is achieved by specialized network tools. This solution involves assigning a static IP address to all hosts in the LAN, also setting VLAN (Virtual LAN) and so on. This technique laborious for administrators and there is no mechanism to distinguish between a malicious and genuine host, as well as this solution is unsuitable for DHCP environments. | The Bombing Packets Attack, MAC, IP Cloning Attacks, the attacker can also pretend to be a receiver devise. This means impersonated an important entity like bank and obtain private information about user. In fact, ARP poisoning attacks violate all the security rules: confidentiality, integrity, and availability. Since the attacker |
| An analysis of security solutions for ARP poisoning attacks and its effects on medical computing.  Prabadevi, B., Jeyanthi, N. & Abraham, A.  Int J Syst Assur Eng Manag 11, 1–14 (2020). | This paper analyzes the  existing defence systems against ARP attacks and proposes  three different techniques for detecting and preventing the  ARP attacks. The three techniques ensure security of traditional ARP and its impact in Medical computing where a  single bit inversion could lead to wrong diagnosis. | Cross-layer Consistency Checking (CLCC), Timestamp and Counter based approach (TSCBA) and Extended TCBA in large data centre networks. (TCDCN) | TCDCN mitigation technique effectively performs the attack prevention by moving NULL MAC addresses, available MAC addresses, Multicast addresses detection before cross-layer inspection, thus reducing the computational time and cost involved in Data tables Scanning. However, it may still incur some considerable cost in maintenance. TCDCN can detect the ARPbased DoS, MiTM, Cloning and host migration issues. |
| Towards Secure Smart Home IoT: Manufacturer and User Network Access Control Framework  M. Al-Shaboti, I. Welch, A. Chen and M. A. Mahmood,  IEEE AINA 2018 | In this paper, the reasearchers propose an SDN-based framework for  enforcing network static and dynamic access control, where  manufacturers, security providers, and users can cooperate to  enhance the smart home IoT security. They also  proposed IPv4 ARP server as an NFV security service to mitigate  ARP spoofing attack by replying to ARP requests in the network.  They aim to implement a prototype to demonstrate the functionality of  the framework against common attack scenarios (i.e. network  scanning, ARP spoofing). | Proposed approach has  three features: a) it allows the manufacturers to enforce the least  privileged policy for IoT, and hence reduce the risk associated  with exposing IoT to the Internet; b) it enables to enforce access  policy as a feedback from security services; c) it enables users to  customize IoT access based on social and contextual needs (e.g.  only permits LAN access to the IoT through his/her mobile),  which reduce the attack surface within the network. | The list of SDN challenges consists of: Controller placement, Scalability, Performance, Security, Interoperability and Reliability. SDN controllers must be wisely configured and the SDN's network topology authenticated to prevent manual errors and increase network availability.  Applicable only for IPv4 ARP spoofing an nor IPv6.  DPDK ARP server was able to handle only  up to 50 parallel ARP requests |

**EXISTING METHODOLOGIES:**

There are two techniques introduced to detect ARP spoofing: the passive approach and the active approach. The passive approach involves monitoring the ARP traffic and looking for inconsistencies in the IP-MAC mapping. The main drawback of this approach is the time lapse between learning and detecting spoofing. The detection that uses an active approach is injecting ARP packets into the network to probe for inconsistencies. The active technique is scalable, faster, intelligent, and more reliable in detecting attacks than the passive techniques.

A technique is in existence using ICMP requests by collecting and analysing the ARP packets, and then it uses ICMP request packets to probe for a malicious host, according to its response packets. The ARP spoofing detection architecture is divided into four

modules.

1) The ARP packet sniffer module: This is meant to sniff all ARP packets from the Ethernet.

2) The IP-MAC mapping database: It compares two table entries in the database in order to check for a new MAC entry for the same IP entry. If found, it assumes it to be a spoof and then sends that IP to the ARP spoofing detection module.

3) The ARP spoofing detection module: It sends an ICM packet to the requesting IP address, and if a reply comes from that host, it decides if the host is legitimate or fake, with returns to the real MAC to update the database.

4) The Response module: It is used to alert the detecting ARP of a spoofing attack. Detection using routing trace is used to find a change in the network movement path to protect the internal network. This technique detects ARP attacks through real-time monitoring (TTL) of the ARP cache table.

**PROPOSED ALTERNATE METHODOLOGY:**

A gateway-based approach to filter out the malicious ARP packets would be efficient. We plan to add an intelligent device capable of handling the packets about to be received by the devices in the network. Through IP - forwarding, the packets sent to the devices from other devices or vice versa could be made to pass through the aforementioned gateway, to undergo screening.While this gateway device would be capable of controlling the flow of the packets,(i.e.,block them from reaching the destination) it would need a reference table to check the authenticity of the the packets, we intend to create a script capable of identifying the fake packets by comparing the no. of request/response packets. The purpose of the script is to eliminate the need for manual updating of the reference table, as manual entries could prove inefficient when there is a large number of devices in the network.