Computer Engineering
Software Systems

Ain Shams University
Faculty of Engineering

Project
Phase One
ARP Poisoning Attack

Under Supervision of

Dr. Wael Elsersy

&

Eng. Ahmed Askar

Submitted By:

Ahmed Khaled Saad Ali Mekheimer
ID: 1809799
(Team Leader)

Ahmed Adel Mounir
ID: 19P9647

Amr Salah El-Deen Ahmed
ID: 18P6049

1. Analysis Of Various ARP Poisoning Mitigation Techniques

Journal:

Proceedings of the 2014 International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT)

Authors:

N. Tripathi and B. M. Mehtre

Problem:

The paper addresses the problem of ARP poisoning attacks, which involve an attacker sending fake ARP messages to a network in order to associate their MAC address with the IP address of another device on the network. This can allow the attacker to intercept and manipulate network traffic, leading to a range of security issues.

Related Work:

The paper discusses previous research on ARP poisoning attacks and mitigation techniques, including static ARP tables, dynamic ARP inspection, ARP watch, and machine learning approaches.

Methods:

The paper provides a comparative analysis of various ARP poisoning mitigation techniques. It evaluates the performance of each technique using various metrics such as detection accuracy, false positive rate, and processing overhead. The paper also discusses the advantages and disadvantages of each technique and suggests possible improvements and future research directions.

Evaluation Matrix:

The paper evaluates the performance of different ARP poisoning mitigation techniques based on various metrics such as detection accuracy, false positive rate, and processing overhead.

Results:

The evaluation results show that dynamic ARP inspection and ARP watch are more effective at detecting ARP poisoning attacks compared to static ARP tables. The authors also note that machine learning techniques show promise for detecting ARP poisoning attacks.

Limitations:

The paper acknowledges that each ARP poisoning mitigation technique has its own limitations, such as the need for specialized hardware or the potential for false positives.

Future Work:

The authors suggest several directions for future work, including improving the performance of existing detection techniques, developing new techniques that are more resistant to evasion techniques, and exploring the use of machine learning and artificial intelligence techniques for detecting ARP poisoning attacks.

2. Agent-Based ARP Cache Poisoning Detection In Switched LAN Environments

Journal:

Journal of Computer Virology and Hacking Techniques

Authors:

Daniyal Sakhawat, Abdul Nasir Khan, Mudassar Aslam, and A. T. Chronopoulos.

Problem:

The paper addresses the problem of ARP cache poisoning attacks in switched local area network (LAN) environments, which involve an attacker sending fake ARP messages to a network in order to associate their MAC address with the IP address of another device on the network. This can allow the attacker to intercept and manipulate network traffic, leading to a range of security issues.

Related Work:

Static ARP tables: This technique involves manually configuring the ARP table on each device on the network to ensure that the MAC-IP mappings are correct. While this technique is simple to implement, it can be difficult to manage on large networks, and is vulnerable to attacks that modify the ARP table.

Dynamic ARP inspection: This technique involves inspecting all ARP messages on the network to ensure that they originate from trusted sources. This can be done using hardware-based solutions, such as switches that support dynamic ARP inspection, or software-based solutions, such as intrusion detection systems.

ARP watch: This technique involves monitoring the ARP cache of a device to detect any changes in the MAC-IP mappings. If a change is detected, an alert is generated, and appropriate action can be taken to prevent further attacks.

Machine learning approaches: This technique involves training machine learning models to detect ARP poisoning attacks based on network traffic patterns. This approach has shown promise in detecting previously unknown or sophisticated attacks but requires significant amounts of training data and computational resources."

Methods:

The paper proposes a novel method for detecting ARP cache poisoning attacks in switched LAN environments using an agent-based approach. The proposed technique involves deploying software agents on each host on the network to monitor the ARP cache and detect any changes in the MAC-IP mappings. The agents communicate with a central server to report any suspicious activity, which can then be analyzed to identify and mitigate the attack. The paper includes a detailed description of the proposed technique, including the architecture of the system, the communication protocol used by the agents and the server, and the algorithms used to detect and respond to ARP cache poisoning attacks.

Evaluation Matrix:

The authors present evaluation results showing the effectiveness of the proposed technique in detecting ARP cache poisoning attacks in a simulated LAN environment.

Results:

The evaluation results show that the proposed approach is able to detect ARP cache poisoning attacks with a high degree of accuracy and a low false positive rate. The authors also show that the proposed approach is able to detect attacks in real-time, which is an important requirement for effective detection of ARP cache poisoning attacks.

The authors also compare the performance of the proposed approach with other existing detection techniques such as static ARP tables, dynamic ARP inspection, and ARP watch. The results show that the proposed agent-based approach outperforms these traditional techniques in terms of detection accuracy and false positive rate.

Limitations:

The paper acknowledges that the proposed technique requires the deployment of software agents on each host on the network, which may be impractical or infeasible in some scenarios.

Future Work:

The authors suggest several directions for future work, including improving the performance of the proposed technique, developing more efficient communication protocols between the agents and the server, and exploring the use of machine learning and artificial intelligence techniques for detecting ARP cache poisoning attacks.

3. Detection and Prevention of ARP Poisoning Attack using Modified ICMP and Voting

Journal:

International Journal of Computer Science and Network Security (IJCSNS) in 2015.

Authors:

K. V. Arya, Prerna Arote

Problem:

The paper addresses the problem of ARP poisoning attacks, which involve an attacker sending fake ARP messages to a network in order to associate their MAC address with the IP address of another device on the network. This can allow the attacker to intercept and manipulate network traffic, leading to a range of security issues.

Related Work:

Static ARP tables: This technique involves manually configuring the ARP table on each device on the network to ensure that the MAC-IP mappings are correct. While this technique is simple to implement, it can be difficult to manage on large networks, and is vulnerable to attacks that modify the ARP table.

Dynamic ARP inspection: This technique involves inspecting all ARP messages on the network to ensure that they originate from trusted sources. This can be done using hardware-based solutions, such as switches that support dynamic ARP inspection, or software-based solutions, such as intrusion detection systems.

ARP watch: This technique involves monitoring the ARP cache of a device to detect any changes in the MAC-IP mappings. If a change is detected, an alert is generated, and appropriate action can be taken to prevent further attacks.

Machine learning approaches: This technique involves training machine learning models to detect ARP poisoning attacks based on network traffic patterns. This approach has shown promise in detecting previously unknown or sophisticated attacks, but requires significant amounts of training data and computational resources.

Methods:

The paper proposes a novel approach for detecting and preventing ARP poisoning attacks using a combination of modified ICMP packets and a voting-based mechanism. The proposed technique involves modifying ICMP packets to include additional information about the sender's MAC and IP addresses and using a voting mechanism to verify the authenticity of ARP messages.

Evaluation Matrix:

To evaluate the detection accuracy and false positive rate, the authors simulate ARP poisoning attacks on the network and measure the success rate of detecting these attacks using their proposed approach and other traditional techniques. The results show that the proposed approach has a higher detection accuracy and a lower false positive rate than other traditional techniques, such as static ARP tables, dynamic ARP inspection, and ARP watch.

To evaluate the execution time of the proposed approach, the authors measure the time taken to process a single ARP packet and compare it with other traditional techniques. The results show that the proposed approach has a lower execution time than other traditional techniques, making it more efficient for real-time detection of ARP poisoning attacks.

Results:

The evaluation results show that the proposed technique is effective in detecting and preventing ARP poisoning attacks in a simulated network environment. The authors also compare the performance of the proposed technique with other existing detection techniques, and show that the proposed technique outperforms these traditional techniques in terms of detection accuracy and false positive rate.

Limitations:

The paper acknowledges that the proposed technique may require modifications to existing network protocols, which may not be feasible in all scenarios.

Future Work:

The authors suggest several directions for future work, including improving the performance of the proposed technique, evaluating the technique in real-world network environments, and exploring the use of machine learning and artificial intelligence techniques for detecting ARP poisoning attacks.

4. A Distributed Security Approach against ARP Cache Poisoning Attack

Journal:

Conference paper presented at the 2021 International Conference on Advanced Computer Science and Information Systems (ICACSIS)

Authors:

Hadi Mahmoudi, Omid Rahimzadeh, Mehdi Nobakht

Problem:

The paper addresses the issue of ARP cache poisoning attack, which is a common and serious threat to network security. The authors propose a distributed security approach to prevent ARP cache poisoning attacks.

Related Work:

The authors review previous work on ARP cache poisoning attacks and existing security approaches to prevent such attacks, including static ARP tables, dynamic ARP inspection, and ARP spoofing detection.

Methods:

The proposed approach is based on a distributed security mechanism that involves multiple devices in the network. The approach utilizes a distributed hash table (DHT) to store and share ARP cache information among devices. The DHT enables the detection of ARP cache poisoning attacks and the distribution of secure ARP cache entries to prevent such attacks.

Evaluation Matrix:

The authors evaluated the proposed approach by simulating ARP cache poisoning attacks on a testbed network using the ARPspoof tool. They compared the proposed approach to existing security mechanisms in terms of detection rate, false positive rate, and latency.

Results:

The simulation results showed that the proposed approach achieved a higher detection rate and a lower false positive rate than existing security mechanisms. The latency of the proposed approach was also lower than that of other mechanisms.

Limitations:

The paper does not provide a comprehensive evaluation of the proposed approach in a real-world setting. Additionally, the approach requires the deployment of additional hardware and software, which may not be feasible for some organizations.

Future Work:

The authors suggest that future work could focus on improving the efficiency and scalability of the proposed approach, as well as on conducting further evaluations in a real-world setting.

5. Analysis on Various Methods to Detect ARP Cache Poisoning Attack

Journal:

International Journal of Advanced Research in Computer Science and Software Engineering

Authors:

Md. Ataullah, Naveen Chauhan

Problem:

The paper addresses the problem of ARP cache poisoning attacks, which involve an attacker sending fake ARP messages to the victim's system, causing the system to update its ARP cache with incorrect information. This can lead to a variety of security issues, including man-in-the-middle attacks and data theft.

Related Work:

The paper discusses several existing methods for detecting ARP cache poisoning attacks, including static ARP cache inspection, dynamic ARP cache inspection, and ARP traffic monitoring.

Methods:

The authors conducted experiments to compare the effectiveness of the different detection methods. The experiments involved setting up a test network and launching ARP cache poisoning attacks on the network. They then used each of the detection methods to identify the attacks and compared the results.

Evaluation Matrix:

The evaluation metrics used in the experiments were accuracy, false positive rate, false negative rate, and detection time.

Results:

The experiments showed that dynamic ARP cache inspection and ARP traffic monitoring were the most effective methods for detecting ARP cache poisoning attacks. Both methods had a high accuracy rate and low false positive and false negative rates. However, dynamic ARP cache inspection had a faster detection time than ARP traffic monitoring.

Limitations:

The paper did not address the issue of preventing ARP cache poisoning attacks, only detecting them.

Future Work:

The authors suggest that future research could focus on developing a comprehensive solution for preventing and detecting ARP cache poisoning attacks.

6. An Efficient and Secure Solution for the Problems of ARP Cache Poisoning Attacks

Journal:

International Journal of Computer, Electrical, Automation, Control and Information Engineering

Authors:

Md. Ataullah, Naveen Chauhan

Problem:

The paper addresses the problem of ARP cache poisoning attacks, which are a type of man-in-the-middle attack that occur when an attacker sends falsified ARP messages to associate their own MAC address with the IP address of another device on a local area network (LAN). This allows the attacker to intercept and manipulate network traffic.

Related Work:

The paper discusses related work on ARP cache poisoning attacks and prevention techniques.

Methods:

The paper proposes a solution for preventing ARP cache poisoning attacks that involves a combination of techniques. The solution includes a new ARP protocol that uses a hash function to verify the authenticity of ARP messages, as well as a monitoring system that detects and responds to ARP cache poisoning attacks in real-time.

Evaluation Matrix:

The proposed solution is evaluated using simulation experiments. The experiments measure the effectiveness of the solution in detecting and preventing ARP cache poisoning attacks.

Results:

The simulation experiments demonstrate that the proposed solution is effective in preventing ARP cache poisoning attacks. The solution is shown to have a low false positive rate and a high detection rate for ARP cache poisoning attacks.

Limitations:

The paper does not explicitly discuss limitations, but it is important to note that the proposed solution may have limitations in real-world implementations and may require further testing and refinement.

Future Work:

The paper suggests that future work could include further research and development of the proposed solution to address any limitations and to explore other potential approaches to preventing ARP cache poisoning attacks.

7. ARP Poisoning Detection and Prevention using Scapy

Journal:

Journal of Physics Conference Series

Authors:

Aayush Majumdar, Shruti Raj and T.Subbulakshmi

Problem:

The research paper discusses the problem of ARP Spoofing or ARP Poisoning, which is a type of attack that exploits the vulnerabilities of the Address Resolution Protocol (ARP) in a Local Area Network (LAN). ARP is a protocol used to map IP addresses to MAC addresses. However, the stateless and unauthenticated nature of ARP makes it easier for attackers to send malicious ARP packets to change the IP address - MAC address pairings in the ARP cache table, redirecting traffic through their own computer. This can be used to carry out Man-in-the-Middle attacks, where the attacker can inspect or modify the messages before forwarding them to the intended recipient, or to cause denial-of-service conditions over a LAN by intercepting or dropping the target's packets.

Related Work:

-N Tripathi and Mehtre B M have proposed ICMP based secondary cache approach for the ARP detection.
-D Bruschi et al introduced a Secure Address Resolution Protocol which enables the user to avoid ARP based attacks.
-J Xia et al proposed an Active Defense Solution for ARP Spoofing in OpenFlow Network, he first implemented ARP spoofing in SDN technology and then proposes a defense mechanism for ARP Spoofing in OpenFlow Platform.
-G Jinhua and Keijian have published work on ARP Spoofing detection algorithm using ICMP Protocol.
-Pandey introduces prevention of ARP spoofing by a probe packet based technique with an Enhanced Spoof Detection Engine.
-Puangpronpitag proposes Dynamic ARP-spoof protection & surveillance (DAPS) system.
-Kumar et al introduced a Centralized System and ARP Central Server (ACS) is used to validate all ARP entries.

Methods:

The method discussed can be subdivided into three main modules: Attack Generation Module, Detection Module and Prevention Module.

Attack Generation Module is to simulate ARP Spoofing attack, Detection module is to detect if the response MAC Address does not match with the Real MAC Address, then the script sends a warning stating that the system is under attack.

Prevention Module uses static ARP entries, they are added for each system on the network into every individual system. This module when applied makes the IP and Mac address static and prevents any spoofing. Any attempt at spoofing will cause the system to automatically disable the attacking device and remove it from the network.

Evaluation Matrix:

Evaluation is done by the experiments provided in the paper executing the Attack Generation Module, Detection Module and Prevention Module and checking their expected outputs and results.

Results:

Attack Generation Module:
MAC address of gateway has been spoofed to the MAC Address of the attacker. Hence any responses to be sent to the gateway would actually be sent to the attacker. Thus any packets sent between gateway and the victim are first intercepted by the attacker.

Detection Module:
It was deduced that the detection script detects the ARP spoof attack and identifies the fake MAC Address associated with the IP Address and sends a warning message. It also finds what the real MAC Address is.

Prevention Module:
By observing experiment of this module in the paper, the mac address has become “PERM” or permanent and now the target does not listen to ARP responses from Gateway’s IP Address (since it has been declared static) thus preventing ARP Poisoning attack.

Limitations:

Since Prevention Module uses static ARP entries, it is recommended for smaller networks only as it necessitates a huge administrative overhead.

Future Work:

This Prevention Module can be used for other attacks by involving machine learning models. Use of Dynamic ARP Inspection integrated with DHCP server and Packet Filtering using tools such as Wireshark can also be done for prevention of ARP Spoofing attacks.

8. An Efficient Mechanism to Detect and Mitigate an ARP Spoofing Attack In Software-Defined Networks.

Journal:

Scientific and Technical Journal of Information Technologies Mechanics and Optics.

Authors:

Ghadeer Darwesh, Alisa A. Vorobeva and Viktoriia M. Korzhuk.

Problem:

In this paper, authors proposed a new approach to secure SDN from an ARP poisoning attack.

Related Work:

- FICUR extends the POX controller with an application that monitors and analyzes the ARP traffic to detect and mitigate the ARP spoofing attack according to pre-defined traffic patterns.
- Using cryptography in communication is still a reliable solution, but the encryption and decryption process causes overload on the network and consumes more resources.
- “Anticap1 and Antidote” uses the OS patches to mitigate the ARP spoofing attack but this solution has its limitations because it requires different patches for different operation systems, which effects the whole communication process.
- Static ARP mapping stops the attack by using the manual configuration of ARP entries. Thus, the attacker has no chance to spoof an already registered host. But it is effective only in small-scale networks.

Methods:

To detect the ARP cache poisoning attack, the paper has extended the POX controller with a new module that analyses all ARP types and effectively detects the attack with no effects on the ARP normal work.

Before presenting the solution, the paper classified the hosts in SDN network into three classes:
Verified hosts table (VHS) hosts that are verified and trusted, their packets are forwarded normally.
Candidate host table (CHT) hosts that are in the middle way to be in VHT.
Banned host table (BHT) hosts that aren't trusted like attacker so their packets will be dropped.

Solution:
The paper's mechanism to detect the attack is to start processing the ARP packets by checking the source MAC address of the Ethernet packet and the source MAC address included in the ARP packet. If the two MAC addresses are not the same, the controller will give a warning, that a new ARP spoofing attack was detected and direct the switches to drop the packet and block the attacker for some time.
Another mechanism proposed is to count the similar ARP packets on the switches and the controller, which have the same metadata.

The DHCP server follows an algorithm to give an IP address to host, get a "DHCP ACK", then server will add this IP to VHT. If the host tries to set IP address manually, the IP address will be treated according to its class (VHT or CHT or BHT).

Using the arpspoof tool in the dsniff package, various spoofed ARP packets were forwarded to the victim to simulate a real ARP spoofing attack.

Evaluation Matrix:

- Attack Detection Time is a metric defined as the total time elapsed to detect the ARP Cache Poisoning attack.
- Attack Mitigation Time is a metric defined as the total time elapsed from detecting the attack to completely blocking the attacker.
- CPU Utilization of the Controller is a very important metric, The NMON tool is used to measure CPU usage before, during and after the attack.
- Throughput metric: Using the Iperf tool we performed the throughput test.

Results:

Attack Detection Time:

Experiment shows that the time elapsed for the detection is very short and it took only 2 ms to detect faked ARP requests and 1.7 ms for ARP replies.

Attack Mitigation Time:

Experiment shows that the time elapsed for the mitigation process is very short too, and it took only 11 ms for attacks with ARP requests and 11.5 ms with ARP replies.

CPU Utilization of the Controller:

The CPU usage with the modified component, was increased from 3.4 % to 4.5 % during the attack. Then the module successfully stopped the attack and the CPU usage returned to 3.3 %.

Throughput:

We noticed that the controller with the pure L2 component is hardly affected by the attack, and the throughput reached 0 in some moments. With the modified component, we can notice that the throughput has decreased only 10 % of the bandwidth and back to its normal situation in a very short time after blocking the attacker.

Limitations:

The use of a single controller network and testing in a virtual environment.

Future Work:

The solution can be further developed to handle ARP attacks in multiple controller SDN networks with high availability, and it is highly recommended to test the described method on a physical testbed to observe the performance parameters in real network environments.

9. ARP Cache Poisoning Mitigation and Forensics Investigation

Journal:

The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-15)

Authors:

Heman Awang Mangut, Ameer Al-Nemrat, Chafika Benza¨ıd and Abdel-Rahman H. Tawil.

Problem:

In this paper, a quantitative research approach is used to propose forensic tools for capturing evidence and mitigating ARP cache poisoning.

Related Work:

-Gouda and Huang proposed a mitigation technique for ARP cache poisoning **using invite-accept protocol and request-reply protocol.**
-A. Bremler-Barr and H. Levy proposed a **Spoofing Prevention Method** (SPM), where a distinctive key is associated with the source and destination domains.

Methods:

To verify whether the network is under attack or not using several forensic tools, namely: TCPdump, Wireshark, and Linux commands TCPstat and Ntop.

To mitigate the ARP cache poisoning attack, DHCP snooping and dynamic ARP inspection (DAI), two port security features, are enabled and configured on the switch.

To validate the proposed forensics investigation of ARP cache spoofing, comparison will be made between the forensics evidences collected when there is no attack on the network against those collected when the network is under attack.

To validate the proposed mitigation technique, the evidences collected when the network is under attack with DHCP snooping and DAI enabled will be compared to those when the two security features are disabled.

Evaluation Matrix:

Evaluation is done by observing the tools TCPdump, Wireshark, and Linux commands TCPstat and Ntop what they offered of evidences and comparing them at Normal state (No attack) and at Attack state, also compare evidences between when the network is under attack with DHCP snooping and DAI enabled to those when the two security features are disabled.

Results:

As of Forensic Investigation of ARP Cache Poisoning:
After comparing the timestamps of the captured evidences with TCPdump when no attack was launched (timestamp was 23h3min7s) and when the network was under attack (timestamp was 23h17min1s), it could be seen that the evidence of a normal traffic flow was captured before launching the attack on the victim machine.

From the evidence collected with Wireshark when the victim machine was under attack, we observed that another MAC address was captured by Wireshark and a duplication of IP address was reported.
It could be observed that the IP address of the default gateway has two MAC address bindings one is the initial MAC address of default gateway and the other is a fake MAC address of a host that does not exist on the network.

From the TCPstat statistics it could be obviously seen that the estimated traffic rate has increased when the network was under attack.
From the Ntop statistics it is obvious to see that the number of unicast during attack increased abruptly.

As of Mitigation of ARP Cache Spoofing:
Obtained results showed that the ARP cache spoofing was prevented when DHCP snooping, and DAI were enabled an configured on the switch.

Limitations:

Comparisons were done on a small network, so in a huge network it will be difficult to identify which IP has two MAC address bindings, also in such a network high traffic is a normal thing, so this won't be an enough evidence to suspect an attack.

Future Work:

Since this paper focused on investigating evidences after the attacks happened, it will be extremely helpful to add Detection & Prevention techniques to these attacks. So that in one system you detect, prevent, investigate forensics of these attacks.

10. ARP Poisoning Prevention in Internet of Things

Journal:

Conference: 2018 9th International Conference on Information Technology in Medicine and Education (ITME)

Authors:

Weihua Gao, Yuhao Sun, Qingying Fu, Zhouzhe Wu, Xiao Ma, Kai Zheng and Xin Huang.

Problem:

ARP is responsible for parsing an IP address into a corresponding MAC address. ARP attacks still threaten the Internet of Things (IoT). To find a method to prevent ARP attack from attacking IoT, this paper describes an ARP attack defense method for the IoT.

Related Work:

Two researches discussed adding the entity of the server in network, to try to decrease computational load (more specifically, the load of authentication and authorization) from IoT devices, in order to prevent the attacks to IoT.

Multiple researches proposed Software-defined networking (SDN) as a novel kind of solution to IoT attacks.

Methods:

For ARP Poisoning Prevention method, first capture the ARP packets sent by the Kali Linux (Attacker) to the single-chip microcomputer and analyzes packets via Wireshark on an Ubuntu machine (VM) considered as Surveillance to obtain the attacker. Afterwards intercept malicious ARP packets with arp-tables tool to protect the Internet of Things from ARP attacks.

Evaluation Matrix:

The paper evaluates its method's success by experimenting and observing if the ARP packets sent by Kali Linux (Attacker) are prevented or not.

Results:

It could be seen from experiments in the paper that all malicious ARP packets have been intercepted, and use Wireshark in Kali Linux to capture packets again. It could be seen that Kali Linux cannot eavesdrop Arduino (IoT Node) now.
So, the prevention of an ARP attack on IoT nodes executes successfully.

Limitations:

The proposed method does not apply to numerous IoT devices, because users need to find out attacker via Wireshark and manually add rules using arp-tables tool.

Future Work:

If the method could be designed to use the script to complete the detection of the attacker's machine and the setting of the arp-tables' rules this approach will be more effective.
Also, using shell script to complete above whole process will be studied.