WPA3_ARP Spoofing Exploit: Detection and Protection Technique

Hilal Breiss & Sohaib El Jundi

Course: Advanced Networks (American University of Beirut)

Abstract: The existence of wireless communication propagates patently more prevailing each year. Since the introduction of the IEEE 802.11 standard WLAN in 1997, technologies have proceeded to deliver wireless availability to businesses and customers with rising easiness and suitability. As connectivity through Wi-Fi growths, wireless exploits on users happened to be more serious. The main involvement of this paper is to examine the technology offered in the new Wi-Fi Protected Access III (WPA3) security scheme and provides detection techniques toward one of the attacks that WPA3 fall under them. ARP spoofing attacks will be our choice.

WPA is the next generation of Wi-Fi security and offers front-line security practices to the market. Relying on the extensive success and acceptance ofWPA2, WPA3 enhances new features to simplify Wi-Fi security, allow more vigorous authentication, bring improved cryptographic enhancement for extremely complex markets, and preserve resiliency of mission grave systems.

WPA3 networks enhancement features can be summarize in:

- Using the latest security methods
- Disallowing outdated legacy protocols
- Using of Protected Management Frames (PMF)

Advantages of WPA3:

- **Password Protection:** in WPA3 the attackers need to interact with the Wi-Fi for every password assumption they try, though cracking it is much tougher and time-consuming.
- **Safer for older data:** Using "forward secrecy," in its protocol, which means that if an attacker captures any encrypted data, he won't be able to decrypt that old data they captured. He'll only be able to decrypt newly captured data.
- **Simplify connecting to Wi-Fi:** WPA3's supports "Wi-Fi Easy Connect," though, the user will be able to connect a device (IOT devices) by just scanning a QR code on the phone
- **Protect Public Wi-Fi:** With WPA3, open networks will encrypt the individual traffic, which allows the safety of use.

WPA3 Vulnerabilities:

There are numerous exposures in existing security measures for WLAN that attackers can influence to raise all kinds of harm or earn undesired control. Investigators at the Wi-Fi Alliance tried to appraise the modern WPA2 system that took place for 14 years. The release of WPA3 aimed to address these problems and improves the present state of security. Although the high security schemes provided by the WPA3, attackers were able to exploit the protocol. Below table

represents all Wi-Fi networks attacks that are proved to be vulnerable in WPA2 and shows if WPA3 addressed them or not.

Attack	Solved by WPA3
Deauthentication	Yes
Handshake Capture Dictionary Attack	Yes
PMKID Hash Dictionary Attack	Yes
Rouge Access Point	Partially
Evil Twin Attack	No
Handshake Capture En/Decryption	Yes
KRACK Exploit	Yes
ARP Spoofing	Partially
SSL Stripping	No
DNS Spoofing	No

The table above shows that WPA3 is vulnerable to few attacks.
In our study, we will be addressing **ARP spoofing** attack on the WPA3. Note that, with client isolation in WPA3, connected hosts cannot reach each other, or send packets to each other. Knowing that, ARP spoofing attack will be between the router and an attacker spoofing a host. So our research will take this case.

What is ARP spoofing?

ARP spoofing is a sort of attack in which an attacker conducts forged ARP messages over a LAN. This results in the connecting of the attacker's MAC address with the IP address of a genuine user on the network. Once the attacker's MAC address is connected to an authentic IP address, the attacker will begin getting any data that is proposed for that IP address. ARP spoofing can allow malicious parties to interrupt, adjust or even break data in fly. ARP spoofing attacks only happen on LAN that uses the Address Resolution Protocol.

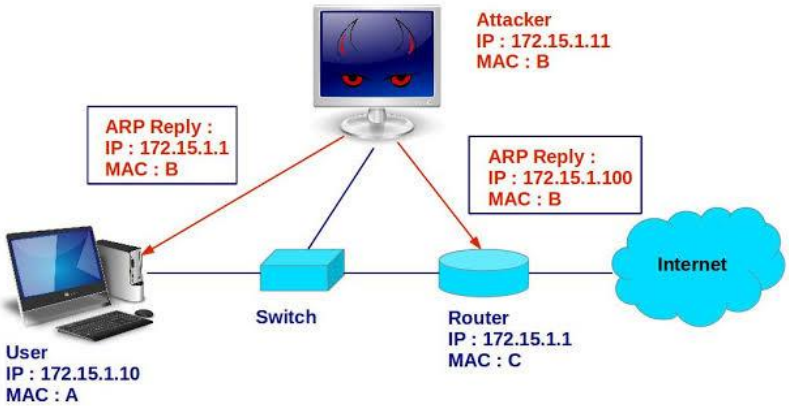

Figure 1: An ARP Spoofing Attack Illustration

Security Requirements for an Ideal Solution:

- Management costs of hosts should be controlled.
- The cryptographic processing, which can lower the performance of ARP, should be minimized.
- Prevention and block should be detected with timely warnings, which will alert the administrator about the attack situation.
- The solution has to be universal and easily applicable.
- Hardware costs should be minimized.
- The solution has to be compatible with ARP.
- It should not slow down the ARP request/reply communications.
- If possible, it should consider all the ARP attacks.
- The network traffic should be contained

Techniques to detect ARP Spoofing Attack:

1- S-ARP: Secure Address Resolution Protocol:

Secure ARP extends ARP with an integrity/authentication scheme for ARP replies, to prevent ARP poisoning attacks. Since S-ARP is built on top of ARP, its requirement follows the one in ARP. In order to preserve compatibility with ARP, an added header to carry the authentication information is introduced. Hosts that run the S-ARP protocol will not allow non-authenticated messages to be processed unless specified.

2- D-ARP: Dynamic ARP

Dynamic ARP resolves security issues by stopping malicious or invalid ARP packets that are carried from the network. It classifies whether the ARP packet is genuine by associating the packet at the router, before it is reached. If a security problem is identified, the packet is canceled.

3- T-ARP: Ticket-based ARP

The ticket-based address resolution protocol defends ARP spoofing by broadcasting the centrally secured IP address and MAC address mapping proof. This proof, called ticket, is conveyed to the client when he gets into the network. This protocol can reduce costs, unlike any other protocol.

4- DS-ARP

DS-ARP is a detection scheme based on routing trace. It works by keeping the updated ARP cache table under surveillance. When the ARP table is updated, DS-ARP performs a routing trace to identify (IP, MAC) pairs. If ARP spoofing is suspected, the entry type is changed to static.

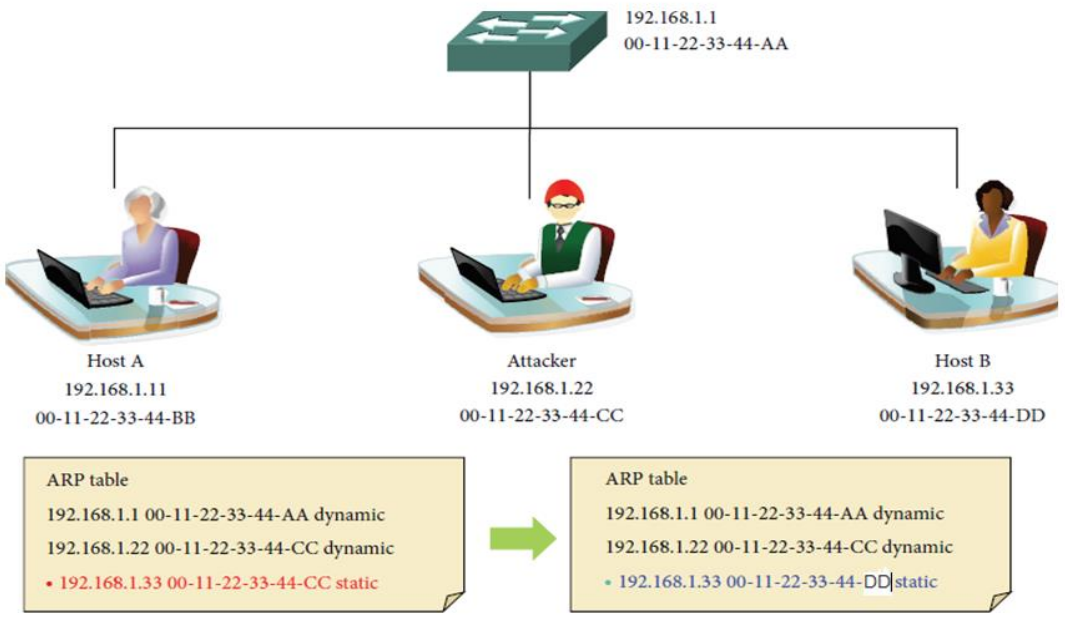

Figure AA: A description of how the ARP table is updated according to DS-ARP

5- Active Technique based on TCP Response packet

This technique takes advantage of the way networks work. The network interface card will accepts frames sent to its MAC address, Broadcast address and subscribed multicast addresses, then they are passed to the IP layer where the only accepted packets are the ones addressed to the IP address. If the accepted packet was TCP packet, it is passed to the TCP layer and if it was a SYN packet, and TCP SYN/ACK is issued. When a TCP SYN packet is sent to the source of the ARP reply packet, the host's response will be based on the previously mentioned process. So, if the ARP response had been from a malicious host then its network stack would silently discard the TCP SYN packet which allows detect based on receiving or not receiving a TCP SYN/ACK.

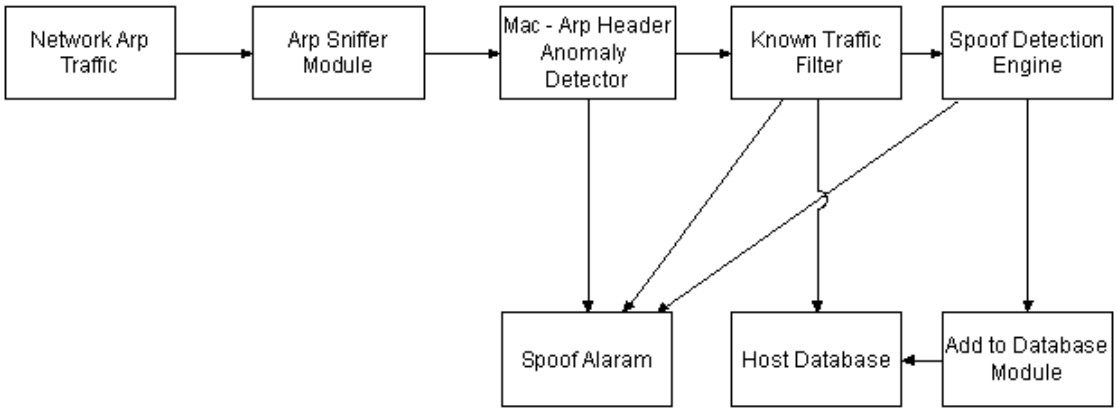

Figure BB: The process an ARP packet it takes to be accepted/rejected based on the above technique

A New Proposed Technique

When a host connects to a router a key pair is generated that is shared between them. When the gateway detects an ARP packet from a Source (S), it would generate a message encrypted the key pair associated with S, which only S can decrypt, then S would have to acknowledge the message. It the message was acknowledged, the ARP cache table is allowed to be updated.

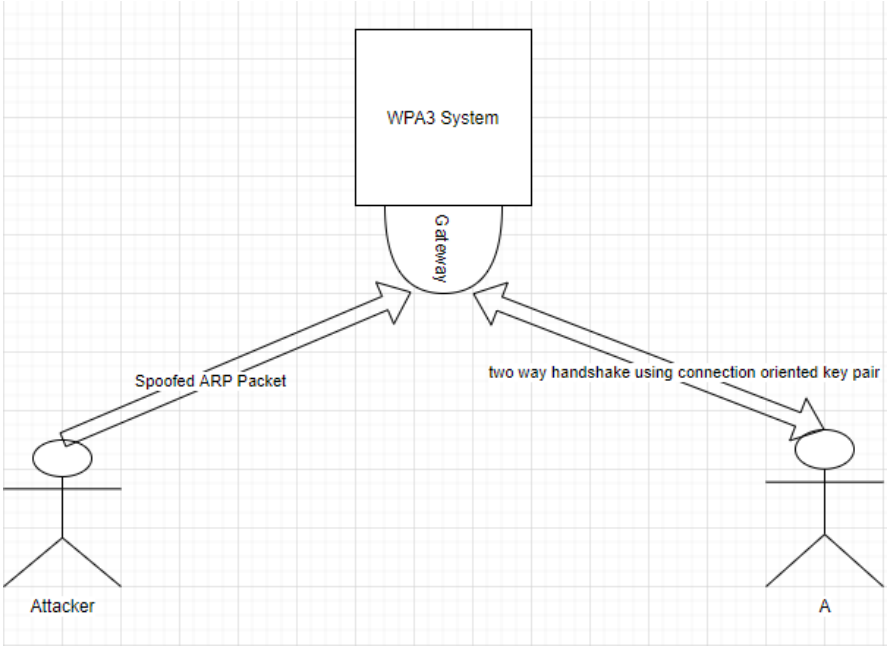

Figure CC: A description of how the proposed technique works

References:

- Ramachandran V., Nandi S. (2005) Detecting ARP Spoofing: An Active Technique. In: Jajodia S., Mazumdar C. (eds) Information Systems Security. ICISS 2005. Lecture Notes in Computer Science, vol 3803. Springer, Berlin, Heidelberg
- Su Song M., Dong Lee J., Jeong Y., Jeong H., Park J. (2014) DS-ARP: A New Detection Scheme for ARP Spoofing Attacks Based on Routing Trace for Ubiquitous Environments. In: Department of Computer Science and Engineering, SeoulTech, Seoul 139-743, Republic of Korea.
- Zawar Shah and Steve Cosgrove, Mitigating ARP Cache Poisoning Attack in Software-Defined Networking (SDN): A Survey, *Electronics*, 10.3390/electronics8101095, 8, 10, (1095), (2019).Crossref
- Kohlios C., Hayajneh T. (2018) A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3. In: Fordham Center for Cybersecurity, Fordham University, New York
- J. Castillo-Velazquez, M. A. Garcia and D. J. S. Martinez, "Hardening as a best practice for WLAN Security Meanwhile WPA3 is released," *2019 IEEE 39th Central America and Panama Convention (CONCAPAN XXXIX)*, Guatemala City, Guatemala, 2019, pp. 1-5, doi: 10.1109/CONCAPANXXXIX47272.2019.8977073