Traffic Hijacking in Wi-Fi Networks via ICMP Redirects

Xuewei Feng
Tsinghua University
fengxw06@126.com

Qi Li
Tsinghua University
Zhongguancun Laboratory
qli01@tsinghua.edu.cn

Kun Sun
George Mason University
ksun3@gmu.edu

Yuxiang Yang
Tsinghua University
yangyx22@mails.tsinghua.edu.cn

Ke Xu✉
Tsinghua University
Zhongguancun Laboratory
xuke@tsinghua.edu.cn

ABSTRACT

This paper uncovers a vulnerability involving identity spoofing through cross-layer interactions among Wi-Fi, IP, and ICMP protocols. The discovered vulnerability enables an off-path attacker to impersonate the Access Point (AP) of a Wi-Fi network, allowing the attacker to hijack plaintext traffic transmitted by wireless stations. We identify a design flaw in the Network Processing Units (NPUs) of widely-used chip manufacturers, which can be exploited by the attacker to spoof the AP and send ICMP redirect messages. By deceitfully mimicking a new AP within the network, the attacker successfully tricks other supplicants into believing that the attacker is a legitimate AP within the network. Consequently, the victim supplicants unknowingly forward their plaintext traffic to the attacker, leading to a successful Man-In-The-Middle (MITM) attack. Through extensive experimentation, we demonstrate that 55 popular AP routers and over 89% of real-world Wi-Fi networks are susceptible to the identified MITM attack.

KEYWORDS

Wi-Fi hijacking; ICMP redirects; Identity spoofing

ACM Reference Format:
Xuewei Feng, Qi Li, Kun Sun, Yuxiang Yang, and Ke Xu✉. 2023. Traffic Hijacking in Wi-Fi Networks via ICMP Redirects. In *ACM Turing Award Celebration Conference 2023 (ACM TURC '23), July 28–30, 2023, Wuhan, China.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3603165.3607441

1 INTRODUCTION

In this paper, we uncover that the security mechanisms in Wi-Fi networks can be evaded by spoofing the legitimate AP to send a forged ICMP redirect message to a victim supplicant. Consequently, an off-path attacker (i.e., a malicious supplicant) can launch a MITM attack that stealthily hijacks the traffic from other supplicants without deploying an extra bogus AP. After receiving a fake ICMP redirect message from the attacker, the victim supplicant with ICMP redirects enabled by default will be tricked into setting the attacker as its next hop to the remote server and ask the legitimate AP to forward all its traffic for the server to the attacker. Compared with traditional rogue AP attacks in Wi-Fi networks, our attack has three advantages. First, it does not require deploying a bogus AP or a fake authentication server. It only requires the attacker to be in the same Wi-Fi network as the victim supplicant. Second, it does not need to broadcast the same or similar SSID. The victim is still connected to the legitimate AP. Third, it can hijack existing Wi-Fi connections without performing any denial of service attacks. Our attack is more stealthy than Rogue AP attacks.

Our attack can evade the security mechanisms employed by WPAs (such as WPA2 and WPA3) in Wi-Fi networks, enabling the successful interception of the victim's plaintext traffic. WPAs implement per-hop encryption at the link layer using a shared session key between the AP and each connected supplicant. However, our attack utilizes a carefully crafted ICMP redirect message to manipulate the victim supplicant into setting the attacker as the next hop at the IP layer. As a consequence, when the AP receives encrypted link-layer frames from the victim supplicant, it must undergo multi-hop processing at the link layer to complete the frame forwarding. Initially, the AP decrypts the encrypted frames using the shared secret key established with the victim supplicant. Subsequently, based on the poisoned "Destination Address" field in the frame header, which has been manipulated to point to the attacker, the AP encrypts the frames using the secret key shared with the attacker and forwards them accordingly. Consequently, once the frames are decrypted by the attacker, the attacker is able to hijack the victim supplicant's traffic [2].

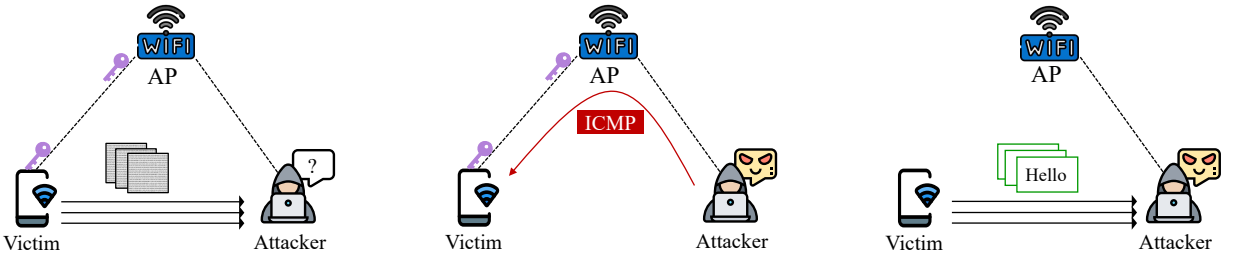
2 BACKGROUND

In order to protect wireless users in Wi-Fi networks, several types of security mechanisms have been proposed in recent years, i.e., WEP, WPA, WPA2, and WPA3 [1]. However, existing studies [3, 6, 7] show that implementation vulnerabilities or design flaws have been discovered in these security mechanisms to compromise Wi-Fi networks. Different from previous attacks that mainly focus on discovering vulnerabilities in Wi-Fi protocols at the link layer or relying on rogue APs, our study is to find the vulnerabilities of Wi-Fi networks incurred by the cross-layer interactions. The vulnerability can be exploited to perform a MITM attack without using a rogue AP.

✉ Corresponding author.

ACM TURC '23, July 28–30, 2023, Wuhan, China

ACM ISBN 979-8-4007-0233-4/23/07.
https://doi.org/10.1145/3603165.3607441



(a) The encrypted Wi-Fi traffic initially sniffed. (b) crafting an ICMP redirect message. (c) Plaintext traffic is forwarded to the attacker.

Figure 1: Plaintext traffic hijacking in Wi-Fi networks via ICMP redirects.

3 ATTACK DESIGNS

The overview of our attack is shown as Figure 1. We resolve two challenges to successfully launch our attack. First, when the attacker spoofs the legitimate AP to send a fake ICMP redirect message to the victim supplicant, the legitimate AP cannot recognize and filter out those forged ICMP error messages when they pass through the AP. We uncover that a fundamental vulnerability (CVE-2022-25667) in the AP router's Network Processing Unit (NPU) restricts a legitimate AP router from blocking those forged ICMP messages. Due to the performance consideration, the NPU (e.g., Qualcomm IPQ5018 and Hisilicon Gigahome Quad-core) in the AP router will directly forward the received fake message of ICMP redirects to the victim supplicant, and thus ACL rules at the higher layers of the AP cannot be enforced to block the messages. This vulnerability affects a wide range of AP routers and restricts the AP vendors from easily repairing their products, since the repair relies on the collaboration between the NPU chip manufacturers and the AP vendors.

Second, the forged ICMP redirects should be able to pass the legitimacy check of the victim supplicant and then poison its routing table. Following ICMP specifications [4, 5], the victim supplicant will check at least 28 octets of the payload in the ICMP redirect message and confirm if the message is really triggered by the packet originated from the supplicant itself. We develop a new solution to pass this check. The attacker can craft a fake UDP header with an active source UDP port on the victim supplicant. Then, it embeds the fake UDP header into the crafted ICMP redirect message, which will pass the supplicant's check. Eventually, the victim will be tricked into setting the attacker as its next hop to the remote server and ask the legitimate AP to forward all its plaintext traffic to the attacker.

4 MEASUREMENT FINDINGS

Our extensive measurement results show that the identified MITM attack can be successfully performed in various Wi-Fi networks to cause serious damages. We evaluate 55 popular wireless routers from 10 well-known AP vendors, and we find that none of the 55 routers can block the crafted ICMP redirect message issued from an attacker, as shown in Figure 2. We also evaluate 122 real-world Wi-Fi networks in six months, including all prevalent Wi-Fi security modes (i.e., WPA2-Personal, WPA2-Enterprise, WPA3-Personal, and WPA3-Enterprise) and most popular real-world Wi-Fi scenarios (e.g., Wi-Fi networks in coffee shops, hotels, shopping malls, and campuses). The experimental results show that 109 out of the 122 evaluated Wi-Fi networks are vulnerable to our MITM attack, resulting in a vulnerable rate of higher than 89%.

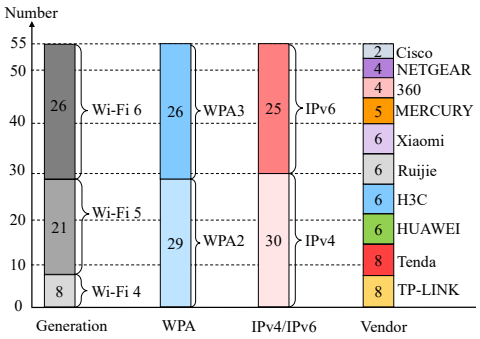


Figure 2: Statistics of the 55 vulnerable wireless routers.

5 COUNTERMEASURES

We develop two countermeasures to throttle the identified attack. First, we propose fine-grained checks on the received ICMP messages by the supplicants, i.e., identifying inconsistencies of the received messages between the link layer and the network layer. For example, we verify consistency between the addresses in the network layer and the corresponding one in the link layer to identify fake ICMP messages. Second, we propose to enhance wireless routers to block spoofed ICMP redirect messages, which does not require kernel modifications and recompilation to supplicants.

REFERENCES

[1] Wi-Fi Alliance. Accessed November 2021. Discover Wi-Fi Security. https://www.wi-fi.org/discover-wi-fi/security.
[2] Xuewei Feng, Qi Li, Kun Sun, Yuxiang Yang, and Ke Xu. 2022. Man-in-the-Middle Attacks without Rogue AP: When WPAs Meet ICMP Redirects. In *2023 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society, 694–709.
[3] Scott Fluhrer, Itsik Mantin, and Adi Shamir. 2001. Weaknesses in the key scheduling algorithm of RC4. In *International Workshop on Selected Areas in Cryptography*. Springer, 1–24.
[4] Thomas Narten, Erik Nordmark, William Allen Simpson, and Hesham Soliman. 2007. *Neighbor Discovery for IP version 6 (IPv6)*. RFC 4861. Internet Engineering Task Force. 1–97 pages.
[5] Jon Postel. 1981. *Internet Control Message Protocol*. RFC 792. Internet Engineering Task Force. 1–21 pages. http://www.rfc-editor.org/rfc/rfc792.txt
[6] Mathy Vanhoef. 2021. Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation. In *30th USENIX Security Symposium (USENIX Security 21)*.
[7] Mathy Vanhoef and Frank Piessens. 2017. Key reinstallation attacks: Forcing nonce reuse in WPA2. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 1313–1328.