Man-in-the-Middle Attacks without Rogue AP: When WPAs Meet ICMP Redirects

Xuewei Feng*, Qi Li†§, Kun Sun‡, Yuxiang Yang*, and Ke Xu*§✉
*Department of Computer Science and Technology & BNRist, Tsinghua University
†Institute for Network Sciences and Cyberspace & BNRist, Tsinghua University, §Zhongguancun Lab
‡Department of Information Sciences and Technology & CSIS, George Mason University
brafum@yeah.net, {qli01@, xuke@, y-yx18@mails}tsinghua.edu.cn, ksun3@gmu.edu

Abstract*—Modern Wi-Fi networks are commonly protected by the security mechanisms, e.g., WPA, WPA2 or WPA3, and thus it is difficult for an attacker (a malicious supplicant) to hijack the traffic of other supplicants as a man-in-the-middle (MITM). In traditional Evil Twins attacks, attackers may deploy a bogus wireless access point (AP) to hijack the victim supplicants' traffic (e.g., stealing credentials). In this paper, we uncover a new MITM attack that can evade the security mechanisms in Wi-Fi networks by spoofing the legitimate AP to send a forged ICMP redirect message to a victim supplicant and thus allow attackers to stealthily hijack the traffic from the victim supplicant without deploying any bogus AP. The core idea is to misuse the vulnerability of cross-layer interactions between WPAs and ICMP protocols, totally evading the link layer security mechanisms enforced by WPAs. We resolve two requirements to successfully launch our attack. First, when the attacker spoofs the legitimate AP to craft an ICMP redirect message, the legitimate AP cannot recognize and filter out those forged ICMP redirect messages. We uncover a new vulnerability (CVE-2022-25667) of the Network Processing Units (NPUs) in AP routers that restrict the AP routers from blocking fake ICMP error messages passing through the router. We test 55 popular wireless routers from 10 well-known AP vendors, and none of these routers can block the forged ICMP redirect messages due to this vulnerability. Second, we develop a new method to ensure the forged ICMP redirect message can evade the legitimacy check of the victim supplicant and then poison its routing table. We conduct an extensive measurement study on 122 real-world Wi-Fi networks, covering all prevalent Wi-Fi security modes. The experimental results show that 109 out of the 122 (89%) evaluated Wi-Fi networks are vulnerable to our attack. Besides notifying the vulnerability to the NPU manufacturers and the AP vendors, we develop two countermeasures to throttle the identified attack.

I. Introduction

Public Wi-Fi networks are available almost everywhere these days, whether you are in an airport, a coffee shop, a hotel, or a library. Different from wired LAN (e.g., Ethernet) where the end hosts usually belong to the same organization, supplicants in the same Wi-Fi network may be owned by people from all over the world. Since attackers may hijack the traffic from other users in the same wireless network, security mechanisms are evolving from the old Wired Equivalent Privacy (WEP) to the latest Wi-Fi Protected Access 3 (WPA3) on protecting Wi-Fi networks, along with the war against the emerging vulnerabilities [1]–[9].

Due to the open access characteristic, public Wi-Fi networks become the targets for Man-in-the-Middle (MITM) attacks. Attackers may launch Rogue Access Point attacks (also known as Evil Twins attacks) by installing a bogus AP to entice victim supplicants' connections [10]–[13]. To masquerade as a legitimate AP, the rogue AP keeps broadcasting the same or similar SSID (Service Set Identifier) as that of the legitimate AP to trick the victims. When a Wi-Fi network requires a credit card for access (e.g., an airplane "pay per hour" network), the attackers can easily steal the user's credit card information. Moreover, the attacker can hijack the victims' DNS requests and redirect them to bogus websites for stealing their login credentials. To hijack an existing Wi-Fi connection between a wireless user and the legitimate AP, the attacker needs to first break the connection via a denial of service attack and then reconnect the user to the rogue AP. As the countermeasures, the rogue AP may be identified by the wireless users via carefully comparing the fake SSID to the legitimate SSID or by the operators of the legitimate AP via detecting the SSID broadcast from the bogus AP. In addition, the pre-requisite denial of service attacks to break the existing connections may lead to the detection of the rogue AP attack.

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, so attackers can launch a MITM attack that stealthily hijacks the traffic from the victim supplicant without deploying an extra bogus AP [10]–[13]. After receiving a fake ICMP redirect message from the attacker, the victim supplicant with ICMP redirects enabled by default (i.e., Linux 2.6.39 and beyond, FreeBSD 6.0 and beyond, Mac OS 10.0.4∼10.10.5, iOS 1∼8, and Android kernel version before 10.0[1]) will be tricked to set the attacker as the next hop and ask the legitimate AP to forward all its traffic 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

[1]Table II in Section V-B shows the details of the affected Android devices from different manufacturers we tested.

Rogue AP attacks.

Essentially, our new MITM attack misuses the vulnerability of cross-layer interactions between WPAs and ICMP protocols, totally evading the link layer security mechanisms enforced by WPAs. The security mechanisms of WPAs provide per-hop encryption at the link layer using a session key shared between the AP and each attached supplicant. However, due to the crafted ICMP redirect message, the victim supplicant will set the attacker as the next hop in the IP layer. Therefore, when the AP receives the encrypted link-layer frames from the victim supplicant, it needs multi hop at the link layer to complete forwarding the frames. The AP will first decrypt the encrypted frames using the shared secret key with the victim supplicant. Next, according to the `Destination Address` (which has been poisoned as the attacker) in the frame header, the AP encrypts the frames using the secret key shared with the attacker and sends them to the attacker. Consequently, after decrypting the frames, the attacker can hijack the victim supplicant's traffic. The link-layer per-hop encryption in Wi-Fi networks is successfully evaded by the attacker.

We resolve two challenges to successfully launch our attacks. 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 vulnerability in the AP router's Network Processing Unit (NPU) restricts a legitimate AP router from blocking those forged ICMP messages. Since the NPUs (e.g., Qualcomm IPQ5018 and Hisilicon Gigahome Quad-core) directly forward the forged messages to the victim supplicant at the lower layer, the Access Control List (ACL) rules at the higher layers of the AP cannot be enforced to block the messages. 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. We disclose the identified vulnerability to Qualcomm and Hisilicon, as well as the affected AP vendors. Qualcomm and Hisilicon have confirmed this vulnerability and they are currently fixing it in their NPUs according to our suggestions[2]. 6 out of the 10 AP vendors also confirmed the vulnerability in their products.

Second, the forged ICMP redirect message should be able to pass the legitimacy check of the victim supplicant and then poison its routing table. Following ICMP specifications [14], [15], 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. In the hub-connected Ethernet, attackers can easily eavesdrop on the victim's packet and then embed the packet into a crafted ICMP redirect message, thus evading the victim's legitimacy check to perform a MITM attack [16]–[21]. However, these ICMP redirect attacks cannot be simply ported from Ethernet to Wi-Fi networks. Since Wi-Fi packets are always encrypted at the link-layer, attackers cannot directly eavesdrop on the victim's packet to craft an evasive ICMP redirect message. Moreover, modern supplicants check the existence of the corresponding UDP socket when an ICMP redirect message embedded with a UDP header is received. If the UDP socket does not exist, the supplicant will discard the message silently to prevent some prior attacks [22]–[25], including the "DoubleDirect" attack that crafts a random UDP header to mislead the victim traffic [26].

We develop a new solution to solve this problem. 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 on the existence of the corresponding UDP socket. Our solution can evade the checks of a wide range of OSes with ICMP redirects enabled (e.g., Linux 2.6.39 and beyond, FreeBSD 6.0 and beyond, Mac OS 10.0.4∼10.10.5, iOS 1∼8, and Android kernel version before 10.0). Moreover, our evasion is unique to Wi-Fi scenarios. The malicious probing to active UDP ports in Wi-Fi networks can hardly be blocked by firewalls or middleboxes that are always deployed at network borders, since our probing traffic in Wi-Fi networks does not traverse the border.

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 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%. Our attack can also be successfully performed in IPv6 Wi-Fi networks. We disclose the vulnerability to the affected Wi-Fi network operators. Most of them have confirmed the vulnerability and planned to fix their Wi-Fi networks according to our suggestions. Besides, we report our attack to the Wi-Fi Alliance, which acknowledges our revelation and states that "you have identified an interesting area for Wi-Fi Alliance to explore and we look forward to discussing with our members after your research is published".

We develop two countermeasures to throttle the identified MITM attack. First, we propose to enhance security checks on cross-layer interactions in Wi-Fi networks to fix the root cause, especially that associated with ICMP. In Wi-Fi networks, attackers and victims always reside in the same network, which opens the attack surface to construct ICMP error messages. Thus, we propose fine-grained checks on the received ICMP error messages by the supplicants, i.e., identifying inconsistencies of the received messages between the link layer and the network layer. We prototype the proposed mechanism in Linux 4.18 and confirm its effectiveness in practice. Second, we propose to enhance wireless routers to filter and block spoofed ICMP redirect messages, which does not require kernel modifications and recompilation to supplicants.

Contributions. Our main contributions are as follows:

- We uncover a vulnerability of the NPUs in AP routers

[2]Qualcomm has assigned CVE-2022-25667 for the identified vulnerability.

that can be exploited by a malicious supplicant to spoof the legitimate AP to forge ICMP error messages in Wi-Fi networks.
- We develop a new technique in Wi-Fi networks to evade the legitimacy checks of supplicants on the received ICMP redirect messages.
- we demonstrate that ICMP redirects can be exploited to evade security features (even WPA3) of Wi-Fi networks to perform a MITM attack without a rogue AP or complicated cracking. Our extensive evaluations against 55 popular AP routers and 122 real Wi-Fi networks show that our attacks can cause serious damage in the real world.
- We propose two countermeasures and prototype our supplicant-side countermeasure in Linux 4.18. The evaluation confirms its effectiveness to foil the identified attack while preserving the functionality of ICMP redirects.

Ethical Considerations. When we evaluate the impacts of our attack in the real world, we design and conduct the experiments carefully to avoid causing damages or negative impacts on the evaluated Wi-Fi networks. Before we conduct the experiments, we first obtain the consent from the network operators. With their help, we conduct our experiments when no other users were using the target Wi-Fi networks. Therefore, we ensure that during the experiments, the target supplicants whose traffic may be hijacked are all our controlled machines. After the experiments, we report the results and the vulnerability to the corresponding operators, who also restart the APs to clear route caches.

During our measurement studies, we identify 55 vulnerable wireless routers on the market that cannot block a crafted ICMP redirect message (with a spoofed source IP address of the wireless router itself) due to a vulnerability of the adopted NPU. These routers are from 10 AP vendors, which use two NPUs from Qualcomm and Hisilicon. We have responsibly disclosed the vulnerability to the 10 AP vendors and the chip manufacturers. Qualcomm and Hisilicon have confirmed this vulnerability, and 6 out of the 10 vendors have also confirmed the incapability of blocking the crafted ICMP redirect messages. The rest 4 AP vendors are still in the process of investigating the vulnerability. We also report the vulnerability of incorrectly processing crafted ICMP redirect messages to the communities of Linux, FreeBSD, and Android (as well as the affected Android device manufacturers of Samsung, HUAWEI, HTC, Meizu, Lenovo, Xiaomi, Nubia, OnePlus, and vivo). Google has confirmed the vulnerability.

II. Background

A. Security Modes in Wi-Fi Networks

Since WEP and WPA have been abandoned for many years, we focus on the security mechanisms of WPA2 and WPA3, which support two security modes, namely, personal mode and enterprise mode. In the personal mode, a pre-shared key (PSK) or a passphrase is used by the AP to authenticate all supplicants. Once a supplicant is authenticated, a unique session key called the Pairwise Transient Key (PTK) is generated to encrypt all the traffic between the supplicant and the AP. This session key is 512 bits in the Temporal Key Integrity Protocol (TKIP) or 384 bits in the Counter Mode CBC-MAC Protocol (CCMP). The personal mode is typically adopted by small organizations (e.g., coffee shops, bookstores, and restaurants) to secure their network traffic without using a dedicated authentication server.

In the enterprise mode, a RADIUS server is deployed to authenticate supplicants using user name, mobile phone number, password, etc. When a supplicant passes the authentication, the RADIUS server will return a random 256-bit Pairwise Master Key (PMK) that CCMP uses to encrypt traffic for the current supplicant only. The enterprise mode is a more secure option to protect the Wi-Fi networks of big organizations and corporations, since it provides individual authentication for each supplicant. Without using a bogus AP or a fake RADIUS server, our new MITM attack can successfully hijack the victim supplicants' traffic in both the personal mode and the enterprise mode.

B. ICMP/ICMPv6 Redirect Mechanism

In IPv4 networks, the ICMP redirect mechanism is designed to improve the network performance via optimizing the forwarding paths [14], [15]. When an end host tries to send packets to a remote host through its default gateway, if the default gateway discovers that it uses another gateway on the same network to forward the packets, the default gateway will issue an ICMP redirect message to inform the end host that the best next hop to the remote host will be the new gateway. Once the received ICMP redirect message passes the legitimacy checks, the end host updates its routing and redirects its subsequent traffic to the new gateway.

The ICMP redirect message is defined as one type of ICMP error messages [14]. The `Type` field in ICMP header is specified as 5, and the `Code` field can be specified arbitrarily as 0, 1, 2, or 3[3]. The `Gateway Internet Address` field defines the new next hop to the destination. According to RFC 792 [14], ICMP redirects should carry at least 28 octets (20 octets of the IP header plus at least 64 bits) of the original datagram that triggered the redirect message, which is used by the supplicant to locate the corresponding process and check the legitimacy of the message. In addition, RFC 1122 [27] states that ICMP redirects should only be sent by the current default gateway (i.e., the AP in Wi-Fi networks) and should not be sent by any hosts.

In IPv6 networks, ICMPv6 redirect is defined in the Neighbor Discovery (ND) protocol that is used to find neighboring routers for forwarding packets on their behalf [15]. ICMPv6 redirects work similarly to those in IPv4 networks. When issuing ICMPv6 redirects to supplicants for a better next hop, the AP in IPv6 Wi-Fi networks first specifies the `Next Header` field in IPv6 header as 58 to indicate that the packet is an ICMPv6 packet. Then, a value of 137 in the `Type` field

[3]As defined in RFC 792 [14], the `Code` field equal to 0, 1, 2, 3 indicates that redirecting packets for the network, for the host, for the type of service and network, and for the type of service and host, respectively.

of the ICMPv6 header identifies the ICMPv6 redirect message. The `Code` field of ICMPv6 header is always specified as 0. The `Target Address` field and the `Destination Address` field of the ICMPv6 header define the better next hop and the destination that is redirected, respectively.

Similar to ICMP redirects in IPv4 networks, ICMPv6 redirects have to pass certain legitimacy checks before being accepted by the supplicants. The ICMPv6 redirect packets should only be sent by the current default AP, and the `Hop Limit` field in IPv6 header should have a value of 255, i.e., the ICMPv6 redirect message cannot be forwarded by a router. Besides, ICMPv6 redirect messages should embed as much of the original IPv6 datagram that triggered the message as possible, without exceeding 1280 octets (i.e., the minimum IPv6 MTU) [15].

III. Threat Model

Figure 1 illustrates the threat model of our man-in-the-middle (MITM) attack. The AP encrypts the network traffic of its supplicants via the security mechanisms developed by the Wi-Fi Alliance. The security mechanisms enforced by the AP can be WPA2 or WPA3. Accordingly, the security mode used by the AP can be WPA2-Personal, WPA2-Enterprise, WPA3-Personal, or WPA3-Enterprise. A victim supplicant (e.g., a mobile phone or a laptop) is attached to a public wireless AP to access remote servers on the Internet. The attacker is a malicious supplicant with no particular demands for the hardware or software. We assume the attacker can access the same AP in both personal mode and enterprise mode before launching our MITM attacks to hijack the traffic sent from the victim supplicant to the remote server.

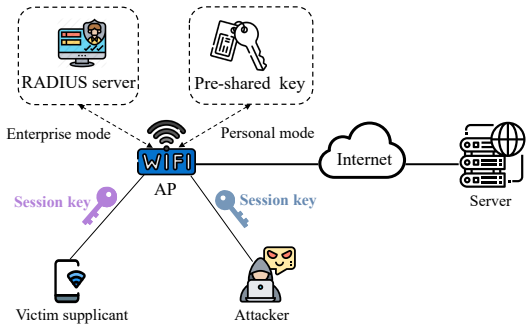


Fig. 1. Threat model of traffic hijacking in Wi-Fi networks.

Accessing Personal Mode Wi-Fi Networks. When the Wi-Fi network uses the personal mode, the attacker needs to obtain the pre-shared key of the network to connect to the AP. This requirement can be easily fulfilled in most cases, since the pre-shared key (PSK) is publicly known for everyone to access the Wi-Fi networks. Note even if the attacker obtains the pre-shared key, it still cannot hijack the traffic of other supplicants, since their connections are protected by a unique random session key (see Section II-A).

Accessing Enterprise Mode Wi-Fi Networks. The Wi-Fi networks using enterprise mode authenticate supplicants based on their unique credentials rather than the pre-shared key. Our survey shows that the credential used the most is the authorization code sent to the user's mobile phone. When the users (including attackers) are connected to the Wi-Fi network, a dialog box pops up and requests the user's mobile phone number. Then, an authorization code will be sent to the user's mobile phone. After the user inputs the authorization code into the dialog box, the RADIUS server completes the authentication and generates a session key for the supplicant. Note it is difficult for an outsider attacker to access non-public Wi-Fi networks protected by the enterprise mode, e.g., corporate networks employing the enterprise mode with user-specific Wi-Fi credentials. Similar to the personal mode, even if the attacker successfully access the Wi-Fi network, it cannot hijack the traffic of other supplicants before performing our attacks.

In order to hijack the victim supplicant's traffic sent to the server, the following requirements should be satisfied:

- ICMP redirects are enabled in the target Wi-Fi network. Once the AP router issues an ICMP redirect message to the attached supplicants according to ICMP specifications, the supplicant will respond to the message by optimizing its routing. Our extensive investigations show that the ICMP redirect mechanism is well supported by a wide range of supplicants and the real-world Wi-Fi networks.
- The supplicants (e.g., the victim supplicants and the attacker) residing in the Wi-Fi network can communicate with each other, so the attacker can receive the victim supplicant's traffic after performing our attack. In the real world, we discover that most of the Wi-Fi networks (more than 89% in our tests) allow communications between the supplicants.
- The attacker is able to know the IP addresses of the victim supplicant and the server that the supplicant is communicating with or will communicate to. In IPv4 networks, the attacker can easily probe the network to identify the IP address of a potential victim supplicant. In IPv6 networks, it is achievable too. It only needs to probe the resided Wi-Fi network (instead of the huge IPv6 address space), and existing studies on IPv6 address probing [28]–[30] can be used to improve the efficiency. The attacker can set the destination server as some popular services, e.g., famous DNS servers, famous web search engines, or social sites.
- The attacker is able to identify open UDP ports on the victim supplicant. According to our investigations, several public known UDP ports are often opened on supplicants by default for lightweight communications (e.g., more than 6 in Linux 5.4.0, including 5353 for mDNS and 68 for DHCP), and any one of them can be exploited to perform our attack. Besides, we observe that it is difficult to block the probing to open UDP ports, since the probing is originated from a normal request to the target UDP ports and the internal probing traffic does not traverse the border of the Wi-Fi network where firewalls are usually deployed in practice.
- The attacker can send spoofed packets using the AP as the source IP address. IP address spoofing is well known in the TCP/IP network [20]. Besides, according to our studies on 55 popular AP routers, we find that none of them can prevent

the attacker to send spoofed packets to the victim supplicant, even when the spoofed messages use the AP router as the source IP address.

IV. MITM Attacks Without Rogue AP

A. Attack Overview

Our attack exploits the vulnerability incurred by the cross-layer interactions between WPAs and ICMP in Wi-Fi networks. Since the TCP/IP protocol suite is based on the hierarchical model [31], the communication content destined to a remote receiver will be processed and encapsulated across multiple protocols at different layers before being sent from the sender. Specific network functionalities (e.g., frame relay, packet routing, flow control) are isolated at different layers. It involves cross-layer protocol interactions via various procedure calls when assembling these functionalities to deliver the communication content, and it will inevitably raise a lot of exceptions. The designed or expected functionality of a certain layer may be disturbed by the exceptions even when other layers during the cross-layer interactions are executed correctly. For example, a known cross-layer issue in Wi-Fi networks is that a frame loss on a wireless link (happening frequently in practice) may be mistaken as an indicator of network congestion by the TCP layer [32].

ICMP is designed for diagnostic and control purposes during packets forwarding on the Internet. The ICMP messages usually carry certain layer's information (e.g., a TCP segment, UDP datagram, or an ICMP message) to report the errors to that layer, which will respond to the messages and handle the errors. In this paper, we show that the designed functionality of wireless frames encryption at the link layer, which aims to prevent traffic hijacking in wireless channels, can be disturbed by the normal executions of ICMP errors handling at the IP layer, thus allowing an attacker to hijack the traffic of victim supplicants.

Figure 2 presents the three steps of our attack. At the beginning, the traffic originating from the victim supplicant to the remote server is sent to the AP and encrypted by a session key between the AP and the victim. The attacker may sniff the encrypted frames, but it cannot decrypt the packets without knowing the session key. In the first step of the attack, by leveraging the ICMP *Destination Unreachable Message* [14] that is unimpeded in Wi-Fi networks, the attacker focuses on probing the target Wi-Fi network to identify an exploitable UDP port on the victim supplicant. In the second step, the attacker crafts an ICMP redirect message embedded with a fake UDP header (carrying the probed open UDP port) to poison the victim supplicant's routing. In the third step, the attacker evades WPAs and hijacks the victim supplicant's traffic in plaintext at the link layer. In the following, we elaborate the three steps.

B. Network Probing

In this step, the attacker prepares the MITM attack in two aspects, namely, creating a routing entry on the victim supplicant for the target remote server and identifying an

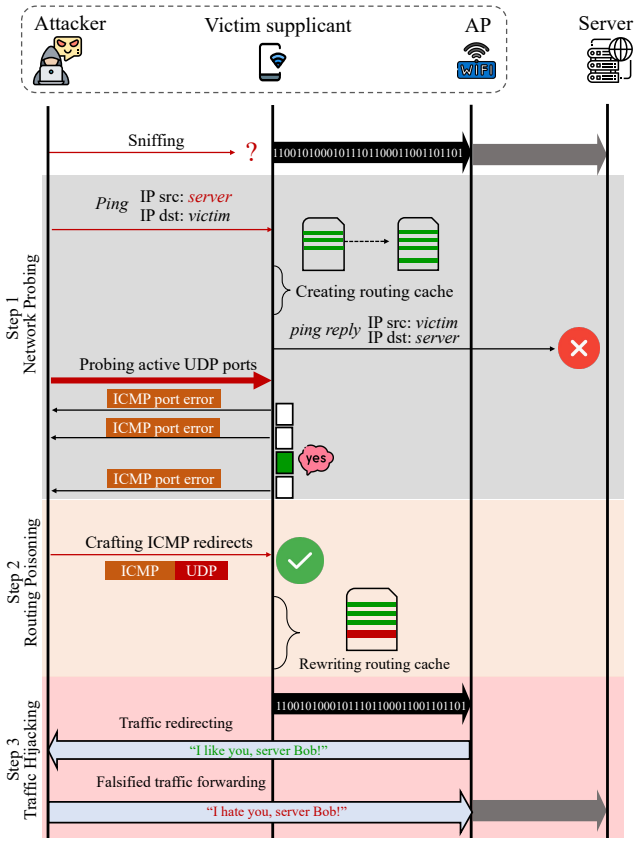


Fig. 2. Three attack steps in our MITM attack.

active UDP port on the victim supplicant. First, the attacker actively tricks the victim supplicant into creating a routing entry for the remote server. As shown in Figure 2, the attacker spoofs the remote server (i.e., source IP address spoofing) and issues forged ping requests (ICMP packets with `Type`=8 and `Code`=0) to the victim supplicant. When the AP enables NAT [33] and assigns private IP addresses to its supplicants, the destination IP address of the forged ping request packets will be a private IP address, and the source IP address will be a public IP address (i.e., the remote server's IP address). Note that if the attacker is located out of the Wi-Fi network, these forged packets will be discarded on the Internet and cannot be forwarded to the victim supplicant, since IP packets with a private IP address as the destination are only allowed in the local networks. In our attack, since the attacker can access the same Wi-Fi network with the victim supplicant, the forged ping request packets can be successfully delivered to the victim supplicant, which is similar to external ICMP echo requests and replies with NATed hosts [34].

After receiving the forged ping requests, the victim supplicant will create an entry in its routing cache table (e.g., "*remote server* via *next-hop* dev *Interface* src *victim supplicant*"), which instructs how to forward the packets for the remote server. Moreover, due to the forged ping requests, the victim supplicant is tricked into replying to the requests. The reply packets will be destined to the remote server, which simply discards those unexpected packets.

Second, the attacker probes the victim supplicant to find

active UDP ports. In Wi-Fi networks, an attacker can easily determine if a UDP port on the target supplicant is opened by sending probing packets to the target supplicant via tools like Scapy [35]. After receiving a UDP request packet, if the destination UDP port (i.e., the target UDP port that the attacker is probing) in the packet is not active (i.e., unopened) on the victim supplicant, the supplicant will reflect an ICMP *Destination Unreachable Message* with `Type`=3 and `Code`=3 directly to the attacker according to ICMP specifications, indicating that the currently probed UDP port is unreachable. By contrast, when the target UDP port is active, the attacker will not receive such an ICMP error message[4]. Our probing in Wi-Fi networks is more accurate and efficient than the UDP port probing on the Internet, since the middleboxes or firewalls on the Internet may block both the crafted UDP request packets from the attacker and the reflected ICMP *Destination Unreachable Message* from the victim supplicant. However, our probing in Wi-Fi networks does not traverse the network border where middleboxes and firewalls are usually deployed in practice.

Note that brute force probing on active UDP ports may incur intrusions to the victim supplicant. To avoid this, we can choose to probe public UDP service ports to minimize the impact of probing. Modern OSes usually open certain public known UDP ports by default for lightweight communications (e.g., DHCP, NTP, etc.). Therefore, in practice, the attacker may be able to directly exploit those active UDP ports to carry out subsequent attacks without conducting complicated probing [36], [37]. For example, there are more than six known UDP ports (e.g., 53, 68, 681, 5353, 38837, 43800, etc.) opened by default in Linux kernel version 5.4.0. On Android systems, more UDP ports are opened by default [38].

C. Routing Poisoning

After probing an active UDP port on the victim supplicant, the attacker crafts a fake ICMP redirect message and spoofs the AP to poison the victim supplicant's routing. According to ICMP specifications, modern OSes will check the legitimacy of the received ICMP redirects based on the embedded 28 octets data (see Section II-B). We discover that the legitimacy check can be evaded by exploiting UDP to craft an evasive ICMP redirect message. Figure 3 shows the structure of our crafted ICMP redirect message, where the embedded 28 octets data consists of an IP header (20 octets) and a UDP header (8 octets). The `Protocol` field in the IP header is specified as UDP, which tricks the victim into believing that an original UDP datagram from the victim to the server triggers the ICMP redirect mechanism. One active UDP port on the victim is specified as the source port in the UDP header. The destination port and the `Length` field in the UDP header can be set arbitrarily. Figure 4 in Section IV-D shows the delivery of the crafted ICMP redirect message from the attacker to the victim

[4]The probing on UDP ports is quite different from probing TCP ports. If the probed TCP port is not open, the target will not reflect an ICMP *Destination Unreachable Message*, but a TCP *RST* packet.

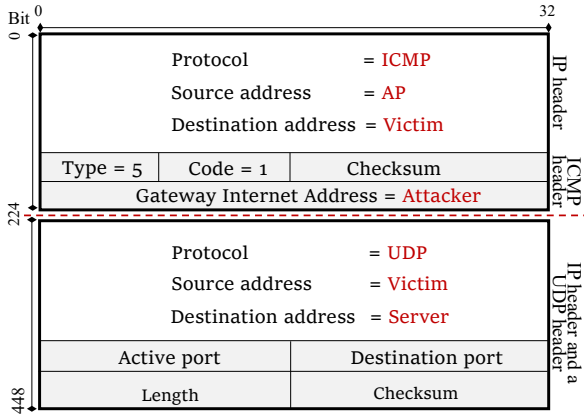


Fig. 3. Crafted ICMP redirects carrying a UDP header.

at the link layer, particularly, the different MAC addresses of the message.

This crafted ICMP redirect message can successfully evade the checks of a wide range of supplicants, e.g., Linux 2.6.39 and beyond, FreeBSD 6.0 and beyond, Mac OS 10.0.4∼10.10.5, iOS 1∼8, and Android kernel version before 10.0 (see Table II in Section V-B for more details about the affected Android devices we tested from different manufacturers) with ICMP redirects enabled by default. Then, the victim supplicants will be tricked into updating their routing cache, and the next hop to the server will be replaced by the attacker's address, i.e., the `Gateway Internet Address` field in the message.

Note that prior ICMP redirect attacks [22]–[26] may embed an empty or a random UDP header to craft an ICMP redirect message; however, those attacks can only succeed on the early OSes that do not enforce any legitimacy checks on the received ICMP redirect messages embedding a UDP header. In contrast, modern OSes will check the existence of the corresponding UDP socket, and if the UDP socket does not exist, the supplicant will discard the message silently. Hence, the prior attacks will fail on modern Wi-Fi networks. Instead, we uncover that the check enforced in modern OSes can be evaded by attackers in Wi-Fi networks via probing an open UDP port on the victim supplicant.

D. Traffic Hijacking

After the victim supplicant's routing to the server is poisoned by the crafted ICMP redirect message, the attacker will act as the new next hop at the IP layer and be responsible for forwarding the supplicant's traffic to the server. However, the attacker cannot directly receive the victim's frames at the link layer to hijack the traffic, since in the infrastructure mode of Wi-Fi networks [39], all frames will go through the AP. The attacker overcome this issue by exploiting the vulnerability arising during the cross-layer interactions between the IP layer and the link layer in Wi-Fi networks.

Different from wired LAN (e.g., Ethernet), Wi-Fi frames can have up to 4 address fields in the MAC header, i.e., transmitter address, receiver address, source address, and destination address. The transmitter address and receiver address

are the MAC addresses of the wireless devices (i.e., the AP or supplicants) that are directly transmitting and receiving frames over the wireless LAN. The source address and destination address are the MAC addresses of the wireless devices that are the ultimate source and destination of this frame. When a supplicant communicates with a remote server, the source address is identical to the transmitter address (i.e., the supplicant's MAC address) and the destination address is identical to the receiver address (i.e., the AP's MAC address).

Instead, if supplicants in the same Wi-Fi network communicate with each other internally, the wireless frame's source address and the transmitter address will be different, as well as the destination address and the receiver address. In our attacks, the communication between the victim supplicant and the attacker can be completed in one hop at the IP layer; however, multi hop forwards are required at the link layer. The AP becomes the receiver and the transmitter alternately for relaying the frames between the source (i.e., the victim supplicant) and the destination (i.e., the attacker).

The security mechanisms of WPAs encrypt each hop at the link layer independently using a session key (between the AP and the attached supplicant). However, a crafted ICMP redirect message will result in the multi hop forwarding of the wireless frames at the link layer. The mis-redirected frames from the victim supplicant to the attacker will be firstly decrypted by the AP and then encrypted using the session key shared with the attacker, thus allowing an attacker who is reachable in one hop at the IP layer to hijack the victim supplicant's traffic.

Figure 4 elaborates how the security mechanisms in Wi-Fi networks can be evaded during the cross-layer interactions between the link layer and the IP layer. At first, the normal encrypted frames originated from the victim supplicant to the remote server are sent to the AP with the AP's MAC address as the receiver and destination address. As a result, when the AP receives such a frame, the AP realizes that it is the final destination of the frame. Then, the AP decrypts the frame using the session key and forward it to the next-hop router on the way to the remote server.

During our attack, a frame carrying the crafted ICMP redirect message is sent from the attacker to the AP. The AP will forward the received message to the victim supplicant based on the destination address of the frame. Tricked by the forged ICMP redirect message, the victim treats the attacker as a better next hop to the remote server. Consequently, subsequent IP packets destined to the remote server will be routed to the attacker at the IP layer. However, at the link layer, the encrypted frames will still be forwarded to the AP at first, since all wireless traffic must be forwarded through the AP in the infrastructure mode.

Compared with the normal encrypted frames (see "1. Normal encrypted frames" in Figure 4), the destination address of the mis-redirected frame is the attacker (instead of the AP), since the victim supplicant considers that the destination (i.e., the next-hop router on the way to the remote server) of the frame is no longer the AP, but the attacker who is also reachable at the link layer.

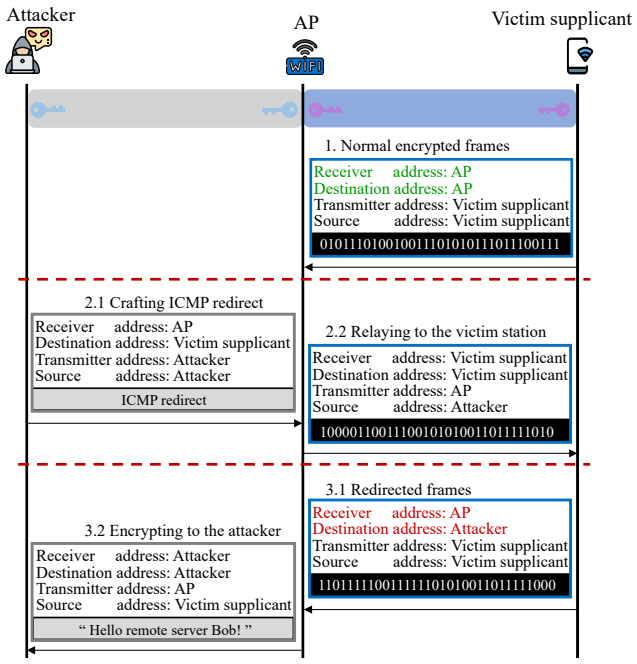


Fig. 4. Attacking interactions at the link layer.

After receiving the frame, the AP considers the attacker as the final destination of the frame according to the link-layer headers. Hence, the AP first decrypts the frame using the session key between the AP and the victim supplicant, and then the AP encrypts the frame again using the attacker's session key and forwards it to the attacker. In the header of the new encrypted frame, the receiver address and the destination address are set as the attacker. After receiving the frame, the attacker is capable of decrypting the frame using its session key. Consequently, the security mechanisms enforced in Wi-Fi networks to protect the victim supplicant's traffic are evaded stealthily. The attacker successfully constructs a man-in-the-middle attack that can silently hijack and modify the victim supplicant's traffic without using any rogue APs.

V. Empirical Study

We conduct extensive real-world evaluations to measure the impacts of our attack. We first investigate if vulnerable APs can block crafted ICMP redirect messages issued from an attacker to a victim supplicant. We test 55 popular wireless routers in our lab and find that none of these routers can block forged ICMP redirect messages. Next, we evaluate our attack against the security mechanisms of WPA2 and WPA3 in both IPv4 and IPv6 Wi-Fi networks, respectively. We evaluate 122 real-world Wi-Fi networks and discover that 109 (89%) of them may suffer from our MITM attack.

A. Vulnerability Analysis of Vulnerable APs

According to ICMP specifications [14], [15], [27], [40], ICMP redirects should only be issued by the current default gateway (i.e., the AP in Wi-Fi networks) of the victim supplicants to inform a better next hop for the remote server. Modern OSes (e.g., Linux 2.6.39 and beyond, FreeBSD 6.0

and beyond, and Android 1.5 and beyond) faithfully implement this check via IP address matching. However, the attacker can craft ICMP redirect messages via source IP address spoofing, i.e., specifying the message's source IP address as the AP's IP address. Then, the attacker issues the crafted message to the victim supplicant, who will be misled into believing that the ICMP redirect message is issued from the AP.

In Wi-Fi networks, the crafted ICMP redirect message will be relayed by the AP to the victim supplicant. Theoretically, the AP should be able to identify the illegality of the crafted ICMP redirect message whose source IP address is specified with the AP itself, and then discard the message to prevent potential attacks. However, we discover that the crafted ICMP redirect message can always be successfully forwarded to the victim. It cannot be blocked by the AP and existing security mechanisms [41]–[43]. 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.

Our evaluations against 55 mainstream wireless routers (acting as an AP to provide the Internet access services) in the market confirm the vulnerability. We discover that none the 55 wireless routers can block the crafted ICMP redirect messages with the spoofed source IP address of the wireless router itself, thus allowing the crafted message to traverse through and arrive at the victim supplicants eventually.

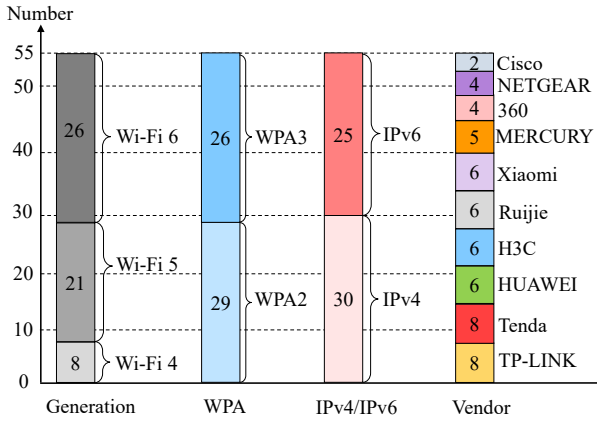


Fig. 5. Statistics of the 55 vulnerable wireless routers.

Figure 5 shows the statistics of the 55 vulnerable wireless routers. The distribution is plotted according to four attributes of the wireless routers, i.e., the Wi-Fi generation that the router supports, the WPA that the router is compatible with, whether the router enables IPv6, and the vendor of the router. Based on our measurement results, we can conclude that most of mainstream wireless routers in the market are vulnerable to our attack, regardless of which Wi-Fi generation the routers support, whether IPv6 is enabled, whether the routers are compatible with the latest security mechanism of WPA3, or by which vendor they are manufactured.

Table I shows the detailed information of 32 vulnerable wireless routers in our investigations. As shown in the first row, the vulnerable wireless router "TL-XVR1800L" produced by TP-LINK supports the latest generation of Wi-Fi, i.e., Wi-Fi 6, and is compatible with WPA3. The router also supports IPv6. According to the product specification, "TL-XVR1800L" enables MAC-ADDR Filtering, i.e., filtering fake MAC address announcements in the ARP protocol to prevent ARP poisoning attacks (see Section VI-B), Anti-Flooding, i.e., throttling malicious flooding traffic to prevent DoS attacks, and Suspicious Packets Blocking, i.e., blocking malformed or crafted packets. Therefore, the router should be able to block the crafted ICMP redirect messages issued from attackers and prevent potential attacks. However, our tests show that the crafted messages can traverse through the router and thus arrive at the victim supplicants, which means the router does not strictly follow its product specification and there is an inconsistency between the AP product and its product specification. In fact, all vulnerable wireless routers we investigated have enabled different security mechanisms to prevent various attacks. However, our study demonstrates that the existing security mechanisms are inadequate to prevent our attack.

B. Attack Evaluation

We conduct comprehensive experiments to evaluate the impacts of our attack in the real world. We perform our attack in 122 real-world Wi-Fi networks, including various IPv4 and IPv6 Wi-Fi networks secured by WPA2 or WPA3. The experimental results illustrate that our attack can be constructed with a success rate of higher than 89% (109 out of 122) to hijack the victim's plaintext traffic in the Wi-Fi networks.

Experimental Setup. Our experiments consist of four types of devices, i.e., an AP, a victim supplicant, a remote server, and an attacker.

- *AP.* The AP in the public Wi-Fi networks broadcasts the SSID to allow the supplicants to access. In our experiments, the AP enables WPA2 or WPA3 to secure the traffic from its supplicants. When the attacker connects to a Wi-Fi network, the IP address of AP can be easily identified.
- *Victim Supplicant.* The victim supplicants affected by our attack include Linux 2.6.39 and beyond, FreeBSD 6.0 and beyond, Mac OS 10.0.4∼10.10.5, iOS 1∼8, and Android kernel version before 10.0 with ICMP redirects enabled by default. Particularly, we test Android devices (with kernel version before 10.0) from different manufacturers and confirm the impacts on the devices. Table II shows the details of the affected Android devices we test in practice (Figure 9 in Appendix shows the mobile devices in our tests). The victim is attached to the AP of the public Wi-Fi networks.
- *Remote Server.* We set Google's public DNS resolver (8.8.8.8) as the remote server. The remote server is requested by the victim supplicant for resolving domain names.

TABLE I
VULNERABLE WIRELESS ROUTERS ALLOWING CRAFTED ICMP REDIRECT MESSAGES TO PASS THROUGH

Wi-Fi router	Generation	WPA	Vendor	IPv6 Enabled	Security Metrics		
					MAC-ADDR Filtering	Anti-Flooding	Suspicious Packets Blocking
TL-XVR1800L	Wi-Fi 6	WPA3	TP-LINK	Yes	●	●	●
TL-XDR1860	Wi-Fi 6	WPA3	TP-LINK	Yes	●	○	○
TL-WAR1200L	Wi-Fi 5	WPA2	TP-LINK	Yes	●	●	●
TL-WDR7660	Wi-Fi 5	WPA2	TP-LINK	No	○	●	●
TL-WR845N	Wi-Fi 4	WPA2	TP-LINK	No	○	○	●
WAP150	Wi-Fi 5	WPA2	Cisco	Yes	●	●	●
WAP125	Wi-Fi 5	WPA2	Cisco	Yes	●	○	●
Ax12	Wi-Fi 6	WPA3	Tenda	Yes	●	●	●
AC23	Wi-Fi 5	WPA2	Tenda	Yes	●	●	○
AC11	Wi-Fi 5	WPA2	Tenda	No	●	○	○
AC10	Wi-Fi 5	WPA2	Tenda	Yes	●	●	●
AX3pro	Wi-Fi 6	WPA3	HUAWEI	Yes	●	●	●
AX2pro	Wi-Fi 6	WPA3	HUAWEI	Yes	●	○	●
WS5281	Wi-Fi 5	WPA2	HUAWEI	Yes	●	●	○
WS5102	Wi-Fi 5	WPA2	HUAWEI	Yes	●	○	○
V6G	Wi-Fi 6	WPA3	360	Yes	●	●	●
5Pro	Wi-Fi 5	WPA2	360	Yes	●	●	○
360mini	Wi-Fi 4	WPA2	360	No	○	●	○
GR-5400AX	Wi-Fi 6	WPA3	H3C	No	●	●	●
N21	Wi-Fi 5	WPA2	H3C	No	●	○	○
ER-8300G2	Wi-Fi 4	WPA2	H3C	No	●	●	○
RG-EW1800GX PRO	Wi-Fi 6	WPA3	Ruijie	No	●	○	●
RG-EW1200G PRO	Wi-Fi 5	WPA2	Ruijie	Yes	●	○	○
RG-EW1200 PRO	Wi-Fi 5	WPA2	Ruijie	No	●	○	○
Redmi AX9000	Wi-Fi 6	WPA3	Xiaomi	Yes	●	●	●
Redmi AX5 RA67	Wi-Fi 6	WPA3	Xiaomi	Yes	●	●	○
Mi 4C	Wi-Fi 4	WPA2	Xiaomi	No	●	○	○
X18G	Wi-Fi 6	WPA3	MERCURY	Yes	●	●	●
D121	Wi-Fi 5	WPA2	MERCURY	Yes	●	●	●
MW325R	Wi-Fi 4	WPA2	MERCURY	No	●	○	○
RAX50	Wi-Fi 6	WPA3	NETGEAR	Yes	●	●	●
RAX20	Wi-Fi 6	WPA3	NETGEAR	Yes	●	●	○

○ means that the security metric is not supported by the router, and ● means that the security metric is supported.

- *Attacker.* An attack machine is equipped with Linux 5.4.0. The attack machine is capable of crafting packets with a spoofed source IP address of the AP by using the Scapy tool. The attacker aims to hijack the victim supplicant's plaintext DNS requests (destined to the remote server) by performing our attack. Once the attack succeeds, the attacker will receive the DNS requests issued from the victim supplicant.

TABLE II
AFFECTED ANDROID DEVICES IN OUR TESTS.

Device	Android version	Device	Android version
HTC-S710e	2.2.1	HTC-X920e	4.1.1
HTC-609d	4.1.2	HTC-802t	4.4.2
Meizu-M040	4.4.4	Galaxy S4	5.0.1
Nexus 10	5.1	HUAWEI Honor 5	5.1
HUAWEI 5A	5.1	Xiaomi Mi 4	6.0.1
Galaxy S6	6.0.1	Lenovo Tab S6000	7.0
OnePlus 3	7.1.1	Xiaomi Mi 4	7.1.1
Xiaomi Mi 4	8.0.0	Nubia Z11	8.0.0
OnePlus 3	8.0.1	vivo X9s	8.1.0
Nexus 10	8.1.0	Xiaomi Mi 4	9.0
Galaxy S6	9.0	Pixel 3	9.0

Experimental Results. We evaluate our attack against 122 real-world Wi-Fi networks to cover most typical public Wi-Fi scenarios, e.g., Wi-Fi networks in coffee shops, hotels, shopping malls, airports, campuses, and office buildings. The experimental results illustrate that more than 89% of the real-world Wi-Fi networks (i.e., 109 out of the 122 evaluated networks) are vulnerable to our attacks, which allow an attacker to hijack the victim supplicants' plaintext traffic, thus causing privacy breach in the real world. Next, we elaborate our experimental results. The failures of our attack in 13 of the 122 evaluated networks (due to specific network policies that the networks enforce) are detailed in Section VI-A.

Figure 6 shows the overall measurement results. Among the 122 Wi-Fi networks, 109 of them are IPv4 enabled only and the rest 13 are IPv6 enabled. It is consistent with our expectation that the IPv6 deployment is still in the progress. Among the 109 IPv4 Wi-Fi networks, 39 of them adopt the security mode of WPA2-Personal, and 35 out of 39 (89.7%) are vulnerable to our attack. 46 IPv4 Wi-Fi networks adopt the security mode of WPA2-Enterprise, and 43 out of 46 (93.5%) are vulnerable to our attack. 23 IPv4 Wi-Fi networks adopt the security mode of WPA3-Personal, and the vulnerable rate is

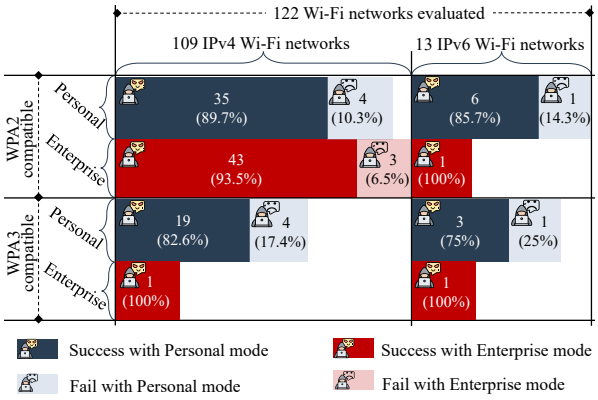


Fig. 6. Attacks evaluation based on 122 real-world Wi-Fi networks.

82.6% (19 out of 23). Since the WPA3-Enterprise-compatible Wi-Fi networks have not been widely deployed in practice, we only find one Wi-Fi network in an enterprise that enables the security mode of WPA3-Enterprise. We observe that the real-world WPA3-Enterprise-compatible Wi-Fi network is also vulnerable to the attack.

With respect to 13 IPv6 Wi-Fi networks, 7 of them adopt the security mode of WPA2-Personal, and the vulnerability rate is 85.7%. 1 of 13 IPv6 Wi-Fi networks adopts the WPA2-Enterprise mode, which is vulnerable to our attack as well. The rest 5 networks are WPA3-compatible. 4 of them adopt the WPA3-Personal model, and the vulnerability rate is 75%. The one WPA3-Enterprise-compatible IPv6 Wi-Fi network in our measurement is also vulnerable to our attack.

Our measurement results demonstrate that Wi-Fi networks widely deployed in the real world are vulnerable to our attack. As a result, our attack can be successfully constructed with a probability higher than 89%, i.e., totally 109 of the 122 Wi-Fi networks. 13 of 122 Wi-Fi networks are not affected by our attacks mainly due to two reasons. First, the mechanism of ICMP redirect is disabled in the network. Second, the communication between internal supplicants in the target Wi-Fi network is forbidden. We further discuss the issues that may affect the success rate of our attack in Section VI.

We elaborate more on the experimental results of 30 Wi-Fi networks in Table III. We take the first row of Table III as an example to analyze the results. In our study, a Wi-Fi network with the SSID of "Restaurant 1[5]" is publicly available in a restaurant, and the AP of the Wi-Fi network is produced by the vendor of Abloomy. This IPv4 Wi-Fi network supports the generation of Wi-Fi 4 and is secured by the WPA2-Enterprise mode. We can use our mobile phone numbers as credentials to pass the authentication and then access the Wi-Fi network. In this Wi-Fi network, we can hijack the victim supplicant's traffic with a success rate of 92%. The four failure cases in our 50 tests are due to the loss of the crafted ICMP redirect messages in the wireless channel of the target Wi-Fi network.

[5]We observe that the real-world SSID of a Wi-Fi network is always related with the name of the organization, which may result in the disclosure of the organization. Thus, due to the ethical considerations, we anonymized the real SSIDs of the Wi-Fi networks.

VI. Discussion

A. Factors Impacting Effectiveness

Supplicants with ICMP Redirects Disabled. According to ICMP specifications, ICMP redirects are used to reduce route hops and thus improve network performance. Hence, the ICMP redirect mechanism is enabled by default in a wide range of OSes, e.g., Linux 2.6.39 and beyond, FreeBSD 6.0 and beyond, Mac OS 10.0.4∼10.10.5, iOS 1∼8, and Android kernel version before 10.0. We observe that supplicants equipped with these OSes can be tricked into accepting the crafted ICMP redirects and then redirecting the plaintext traffic to the attacker. With respect to Windows systems (e.g., Windows 7 Professional 64-bit and Windows 10 Pro in our tests), although the ICMP redirect mechanism is enabled by default, we find that Windows will not be affected by our attack. When an ICMP redirect message arrives at supplicants equipped with Windows, Windows will discard the message simply and does not respond at all, even when the message is benign that is truly issued from the legitimate AP.

Supplicants equipped with OSes that do not enable the mechanism of ICMP redirect by default will not be affected by our attack directly. However, once the ICMP redirect mechanism is enabled (e.g., via the command of "`sysctl net.inet.icmp.drop_redirect=0`" on Mac OSes 10.11.6 and beyond), we observe that the supplicants will also be vulnerable to our attack.

Wi-Fi Networks with Specific Network Policies. The effectiveness of our attack may also be affected by specific network configurations enforced by the target Wi-Fi networks. In our measurement study on 122 real-world Wi-Fi networks, we find that 13 of them enforce specific network policies. Those Wi-Fi networks will be not impacted by our attack.

First, Wi-Fi networks may disable the mechanism of ICMP redirect in local networks. For example, in our evaluation on a Wi-Fi network with the SSID of "Watsons Free Wi-Fi" (secured by the WPA2-Enterprise mode), we identify that ICMP redirect messages will always be discarded by the network, regardless of whether the message is benign or crafted from attackers. This specific configuration will throttle our attack. Unfortunately, our measurement results show that, except the network with the SSID of "Watsons Free Wi-Fi", almost all Wi-Fi networks enable the ICMP redirect mechanism. Hence, the crafted ICMP redirect messages can be successfully forwarded in these networks.

Second, Wi-Fi networks may be enforced with special network policies to constrain the communication between internal supplicants, which may prevent our attack. For example, in our measurement study, we discover 12 Wi-Fi networks where internal supplicants under the same AP cannot communicate with each other. The supplicants can communicate with external hosts (e.g., public servers on the Internet) successfully. However, once the destination address of the wireless frames is not the AP's MAC address, i.e., internal communication happening between supplicants within the same network, the frame will be blocked by the AP. This special network config-

TABLE III
EXPERIMENTAL RESULTS OF TRAFFIC HIJACKING IN 30 WI-FI NETWORKS.

No.	SSID	AP vendor	IPv4/IPv6	Wi-Fi generation	WPA2/3 Enterprise/Personal	Success rate
1	Restaurant 1	Abloomy	◐	Wi-Fi 4	WPA2-Enterprise	46/50
2	Restaurant 2	TP-LINK	◐	Wi-Fi 5	WPA2-Enterprise	42/50
3	Restaurant 3	H3C	◐	Wi-Fi 4	WPA2-Personal	45/50
4	Campus 1	TP-LINK	●	Wi-Fi 5	WPA2-Enterprise	47/50
5	Campus 2	H3C	◐	Wi-Fi 5	WPA2-Enterprise	49/50
6	Campus 3	iKuai	◐	Wi-Fi 4	WPA2-Personal	44/50
7	Fast food restaurant 1	WiMaster	◐	Wi-Fi 5	WPA2-Enterprise	47/50
8	Fast food restaurant 2	Abloomy	◐	Wi-Fi 4	WPA2-Enterprise	44/50
9	Fast food restaurant 3	WiMaster-Mini	◐	Wi-Fi 5	WPA2-Enterprise	46/50
10	Coffee shop 1	WiMaster	◐	Wi-Fi 4	WPA2-Enterprise	49/50
11	Coffee shop 2	TP-LINK	◐	Wi-Fi 4	WPA2-Enterprise	47/50
12	Coffee shop 3	TP-LINK	◐	Wi-Fi 5	WPA2-Personal	49/50
13	Shopping mall 1	HUAWEI	◐	Wi-Fi 5	WPA2-Enterprise	45/50
14	Shopping mall 2	TP-LINK	◐	Wi-Fi 4	WPA2-Enterprise	46/50
15	Shopping mall 3	Tenda	◐	Wi-Fi 5	WPA2-Enterprise	44/50
16	Bookstore 1	360	◐	Wi-Fi 4	WPA2-Enterprise	44/50
17	Bookstore 2	Xiaomi	◐	Wi-Fi 6	WPA3-Personal	47/50
18	Bookstore 3	H3C	◐	Wi-Fi 6	WPA3-Personal	48/50
19	Office building 1	TP-LINK	◐	Wi-Fi 5	WPA2-Enterprise	46/50
20	Office building 2	Tenda	◐	Wi-Fi 5	WPA2-Enterprise	45/50
21	Office building 3	TP-LINK	●	Wi-Fi 6	WPA3-Personal	46/50
22	Experience store 1	Xiaomi	◐	Wi-Fi 6	WPA3-Personal	45/50
23	Experience store 2	H3C	●	Wi-Fi 5	WPA2-Personal	47/50
24	Experience store 3	Xiaomi	◐	Wi-Fi 5	WPA2-Personal	47/50
25	Cinema 1	Xiaomi	◐	Wi-Fi 5	WPA2-Enterprise	48/50
26	Cinema 2	HUAWEI	◐	Wi-Fi 6	WPA2-Enterprise	49/50
27	Hotel 1	Gee	◐	Wi-Fi 5	WPA2-Enterprise	48/50
28	Hotel 2	ZH-A0101	◐	Wi-Fi 4	WPA2-Enterprise	43/50
29	Enterprise 1	TP-LINK	◐	Wi-Fi 6	WPA3-Enterprise	46/50
30	Enterprise 2	TP-LINK	●	Wi-Fi 6	WPA3-Enterprise	44/50

uration prevents our attack. In our attack, the communications among supplicants need to be allowed so that victims can communicate with the attacker and the decrypted frames of the victim supplicant can be relayed to the attacker by the AP (see Figure 4). This particular network policy throttles our attack[6]; however, it may impact the network availability. As a result, we observe that less than 10% (12 out of 122) of the real-world Wi-Fi networks enforce this network policy.

B. ARP Poisoning in LANs

ARP poisoning is a typical attack by which an attacker associates its own MAC address with the IP address of a victim target (that is connected to the same network with the attacker) via crafting spoofed ARP reply messages. As a result, the traffic destined to the victim target will be mis-forwarded to the attacker [44], and the attacker successfully performs a MITM attack. ARP poisoning in wired or wireless LANs have been well prevented in recent years, e.g., discarding unsolicited ARP replies [45], [46] or retaining a mapping table between IP address and MAC address [47], [48].

[6]In our attack, a vulnerable AP is incapable of blocking spoofed packets and capable of forwarding benign packets. However, the APs in these two failure situations are set to drop the packets even if the packets may be benign. When we investigate more deeply on the AP routers, the network operators decline our request.

By contrast, our attack exploits the vulnerability incurred during the cross-layer interactions, instead of the vulnerability at a certain layer. As a result, all behaviors generated by our attack at the link layer are legal. In addition, compared with the ARP poisoning attack, our attack is stealthier since the attacker realizes the MiTM attack by crafting one ICMP redirect message to the victim supplicant, instead of broadcasting spoofed ARP replies in the LAN. Therefore, it is difficult to prevent our attack by leveraging existing security mechanisms, e.g., packet filtering and malicious traffic monitoring.

VII. COUNTERMEASURES

Responsible Vulnerability Disclosure. We have reported the vulnerability of allowing a crafted ICMP redirect message to pass through to the ten affected AP vendors that we identified (see Figure 5) and the NPU chip manufacturers of Qualcomm and Hisilicon. Qualcomm and Hisilicon have confirmed the vulnerability and they are currently fixing it in their NPUs. NETGEAR, HUAWEI, TP-LINK, Tenda, H3C, and Ruijie have also confirmed the vulnerability. They will repair their AP routers after the chip manufacturers fix the vulnerability in the NPUs. For example, Ruijie plans to add an ICMP attack prevention module in the subsequent AP products. Besides, in our evaluations on the 109 real-world vulnerable

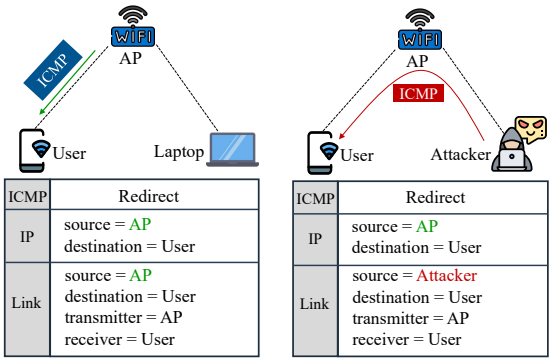
Wi-Fi networks, we reported the vulnerability to the network operators. 94 of them have confirmed the vulnerability and plan to fix their Wi-Fi networks to prevent the attack. The operators of the rest 15 networks are still investigating the vulnerability until now. We also reported the vulnerability of incorrectly processing crafted ICMP redirect messages to the communities of Linux, FreeBSD, and Google (as well as the affected Android manufacturers of HTC, Samsung, HUAWEI, Lenovo, Meizu, Xiaomi, Nubia, OnePlus, and vivo). Google has confirmed the vulnerability.

In this section, we propose two countermeasures to prevent the identified attack. The ICMP redirect mechanism is designed to improve network performance [14], [15] and is also helpful to network troubleshooting [49], hence it is not a good decision to disable ICMP redirects. Instead, we propose to perform more precise checks over the received ICMP redirect message at the supplicant side or allow APs in Wi-Fi networks to block the crafted ICMP redirect messages, thus throttling the MITM attack identified in this paper while preserving the normal functionality of ICMP redirects.

A. Enhancing Supplicants to Check Cross-Layer Interactions

Figure 7 shows the comparison between a legitimate ICMP redirect message issued from the AP and a forged ICMP redirect message crafted by a malicious attacker. We can see that users (i.e., victim supplicants) who receive a crafted ICMP redirect message can identify the message illegitimacy due to the inconsistency of the addresses in the message. As shown in Figure 7(a), the source IP address and the source link address (i.e., MAC address) of legitimate ICMP redirect messages (issued from the AP) are consistent. They are the IP address and the MAC address of the AP, respectively.

By contrast, if the ICMP redirect message is crafted by an attacker, the source IP address in the message will not be consistent with the source link address. As shown in Figure 7(b), in order to trick the victim user into believing that the crafted message is issued by the AP, the source IP address in the message is specified as the AP's IP address. However, at the link layer, the source address of the wireless frame is the attacker's MAC address. This violates the normal practice, i.e., the source address of the wireless frame should also be the AP's MAC address. The inconsistency in the crafted ICMP redirect message can be easily identified by supplicants in Wi-Fi networks. Therefore, we propose to enhancing the supplicants to detect such inconsistency and discard the crafted ICMP redirect message. Note that it is difficult for the attacker to change its MAC address into the AP's MAC address (i.e., the BSSID of the Wi-Fi network) to evade this countermeasure, since this will cause BSSID conflicts in the Wi-Fi network and the attacker's network adapter will lose the connection to the AP. As a result, the attacker will not be able to issue any message. Instead, if the attacker chooses to directly issue the ICMP redirect message to the user via radio, it needs to know the session key between the AP and the user.



(a) Legitimate ICMP redirect message issued from the AP. (b) Illegitimate ICMP redirect message crafted by an attacker.

Fig. 7. Differences between the legitimate and crafted ICMP errors.

we implement our countermeasure via modifying the function of "`static bool icmp_redirect (struct sk_buff *skb)`" in the Linux 4.18 kernel. We first identify the source MAC address of the received ICMP redirect message in the struct of "`sk_buff *skb`". Then, we call the function of "`__ipv4_neigh_lookup_noref()`" to get the corresponding MAC address of the ICMP redirect message's source IP address. Finally, we compare the two identified MAC addresses. If they are not equal, we discard the ICMP message (see Section A in Appendix for more details).

Through evaluations in the Wi-Fi network of our campus, we confirm that our countermeasure can foil the identified attack. The supplicant protected with our countermeasure and an attacker connect to our campus Wi-Fi network. The attacker issues a crafted ICMP redirect message to the supplicant to hijack the supplicant's traffic. In our experiments, the supplicant will identify the inconsistency in the received ICMP redirect message and thus discard the message. Meanwhile, our countermeasure preserves the normal redirect mechanism. The supplicant will respond to ICMP redirects issued from the legitimate AP. The supplicant-side countermeasure can protect the supplicant that concerns our MITM attack, and it does not rely on the AP of the attached Wi-Fi network.

B. Enhancing APs to Throttle Crafted ICMP Redirects

Alternatively, we can enhance APs to throttle the attack by filtering fake ICMP redirect messages. As we stated in Section V-A, the attacker needs to spoof the AP to craft an acceptable ICMP redirect message. The crafted message will be relayed by the AP from the attacker to the victim supplicant. Since the source IP address of the crafted ICMP redirect message is specified as the AP's IP address, the anomaly can be identified by the AP during the message forwarding.

It is difficult for the current design to prevent IP address spoofing inside Wi-Fi networks using existing security filtering mechanisms, because they are only enforced to ensure that packets entering or leaving the network are with legal IP addresses [41]–[43]. Thus, we propose to enhance APs to verify all received packets to actively identify such address anomalies, regardless of whether the packets are only forwarded internally or will be routed to enter or leave the

network. If a packet that the AP receives is forwarded from other hops, AP will filter the packet if its source IP address is the AP's IP address itself. This countermeasure can be widely deployed at APs to protect all supplicants attached to the AP from being manipulated by the crafted ICMP error messages. However, as we stated in Section V-A, this countermeasure relies on the collaboration between the chip manufacturers of the vulnerable NPUs and the AP vendors, and now we are discussing this countermeasure with the AP vendors.

VIII. Related Work

Breaking Wi-Fi. Wi-Fi is a popular access method for end users to connect the Internet [50] and is an appealing target for attackers. 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 [51]. However, existing studies [1]–[3], [5]–[9], [52], [53] show that implementation vulnerabilities or design flaws have been discovered in these security mechanisms to compromise Wi-Fi networks. For example, due to the adopted vulnerable encryption algorithm of RC4 [2], WEP compatible Wi-Fi networks can be cracked in minutes [2], [3], even in seconds by leveraging automation tools of Aircrack-ng [3], [52]. Hence, WPA was proposed with the 802.11g Wi-Fi standard to supersede WEP. However, WPA was discovered to be vulnerable to key recovery attacks [1], [5], and Moskowitz demonstrated that WPA is also vulnerable to dictionary attacks [4].

WPA2 replaced TKIP in WPA with AES-CCMP [54] for the non-enterprise authentication, thus mitigating attacks that WPA suffered. However, existing studies show that WPA2 is vulnerable to the KRACK attack that allows attackers to reconstruct the keys of WPA2-compatible networks via forcing nonce reuse [6], [7]. Besides, Steube demonstrated that WPA2 PSK passwords can be cracked via exploiting RSNIE of a single EAPOL frame [53]. WPA3 replaced PSK in WPA2 with SAE that is designed to securely exchange the initial key in personal mode [55]. Recent studies show that WPA3 may still be vulnerable to downgrade attacks or dictionary attacks [8], [9]. Attackers may force WPA3-compatible APs to use weaker cryptography algorithms via altering the handshake procedure or force the devices to downgrade to WPA2, and then they perform the KRACK attacks [8]. Attackers can also exploit side channels to crack the network password or forge encrypted frames via malicious frame fragmentation [9]. However, it is still difficult to hijack other supplicants' traffic in plaintext in WPA3-compatible networks.

Attackers may deploy a rogue AP to perform an Evil Twins attack to hijack victim supplicants' traffic [10]–[13]. This attack requires broadcasting the same or similar SSID. Moreover, it is difficult to hijack existing Wi-Fi connections by performing this attack. 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.

Hijacking Traffic. Traffic hijacking has been extensively studied. For instance, via abusing the weaknesses in the ARP protocol, an attacker can corrupt the MAC-to-IP mappings of victims' devices on the same network. The attacker can craft spoofed ARP reply messages and thus perform an ARP poisoning attack to hijack the victims' traffic on the network [44]. Fortunately, ARP poisoning attacks have been well mitigated in recent years through MAC-IP address bindings [47], [48] and discarding unsolicited ARP reply messages [45], [46].

The ICMP redirect mechanism was abused previously to perform a MITM attack to hijack a victim's traffic [16]–[25]. However, previous ICMP redirect attacks can only succeed in the outdated hub-connected Ethernet in which attackers can eavesdrop on the victim's traffic to craft an evasive ICMP redirect message [16]–[21], or the victim does not perform any legitimacy checks on the received ICMP redirect messages [22]–[26]. ICMP echo messages were exploited by Kulas to craft evasive ICMP redirect messages against Windows 7 and certain Linux systems (i.e., excluding kernel version 3.6.x) in IPv4 LANs [56]. We develop a new method to evade the ICMP redirect legitimacy checks in Wi-Fi networks and present a new MITM attack to evade the security mechanisms of WPAs, thus hijacking the victim wireless traffic.

Hijacking TCP connections by leveraging side channels [57]–[61] allows off-path attackers to inject forged TCP segments into the target connection or terminate the connection. Via poisoning OSPF routing tables [62]–[64] and announcing anomalous BGP messages [65]–[67]), attackers can construct a routing hijacking attack on control planes. IP fragmentation is another widely abused technique to manipulate the traffic [68]–[72]. Off-path attackers may inject a fake IP fragment into the target connection. Once the fake IP fragment is mis-reassembled with the benign ones, the target traffic is poisoned. Fortunately, most of the attacks have been mitigated by the security communities [58], [59], [63], and some specific security mechanisms have been proposed to foil these attacks [73]–[76]. However, our MITM attack in Wi-Fi networks poses a new challenge to the security communities.

IX. Conclusion

In this paper, we study the vulnerability incurred by the cross-layer interactions between WPAs and ICMP in Wi-Fi networks. We uncover that the link-layer security mechanisms of WPA2 and WPA3 enforced in Wi-Fi networks, which encrypt wireless frames from being hijacked, can be broken by the ICMP errors handling at the IP layer. By leveraging one carefully crafted ICMP redirect message, an attacker can evade existing security mechanisms of WPAs and thus develop a MITM attack in modern Wi-Fi networks without using rogue APs. We demonstrate that our MITM attack can be successfully constructed in various Wi-Fi networks and thus cause serious damages in the real world. We responsibly disclosed the identified vulnerability and propose two countermeasures. We prototype our countermeasure at supplicants. The evaluations validate its effectiveness to foil the identified attack while preserving the functionality of ICMP redirects.

REFERENCES

[1] E. Tews and M. Beck, "Practical attacks against wep and wpa," in *Proceedings of the second ACM conference on Wireless network security*, 2009, pp. 79–86.

[2] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of rc4," in *International Workshop on Selected Areas in Cryptography*. Springer, 2001, pp. 1–24.

[3] W. H. TO, "Cracking wep passwords with aircrack-ng," https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wep-passwords-with-aircrack-ng-0147340/, Accessed March 2022.

[4] R. Moskowitz, "Weakness in passphrase choice in wpa interface," *http://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_wpa_interface.html*, 2003.

[5] T. Ohigashi and M. Morii, "A practical message falsification attack on wpa," *Proc. JWIS*, vol. 54, p. 66, 2009.

[6] M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in wpa2," in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 1313–1328.

[7] ——, "Release the kraken: new kracks in the 802.11 standard," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 299–314.

[8] M. Vanhoef and E. Ronen, "Dragonblood: Analyzing the dragonfly handshake of wpa3 and eap-pwd," in *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2020, pp. 517–533.

[9] M. Vanhoef, "Fragment and forge: Breaking wi-fi through frame aggregation and fragmentation," in *30th USENIX Security Symposium (USENIX Security 21)*, 2021.

[10] D. Gao, H. Lin, Z. Li, F. Qian, Q. A. Chen, Z. Qian, W. Liu, L. Gong, and Y. Liu, "A nationwide census on wifi security threats: prevalence, riskiness, and the economics." in *MobiCom*, 2021, pp. 242–255.

[11] H. Han, B. Sheng, C. C. Tan, Q. Li, and S. Lu, "A timing-based scheme for rogue ap detection," *IEEE Transactions on parallel and distributed Systems*, vol. 22, no. 11, pp. 1912–1925, 2011.

[12] A. M. Alsahlany, A. R. Almusawy, and Z. H. Alfatlawy, "Risk analysis of a fake access point attack against wi-fi network," *International Journal of Scientific & Engineering Research*, vol. 9, pp. 322–326, 2018.

[13] R. Orsi, "Understanding evil twin ap attacks and how to prevent them," https://www.darkreading.com/attacks-breaches/understanding-evil-twin-ap-attacks-and-how-to-prevent-them, 2018.

[14] J. Postel, "Internet Control Message Protocol," Internet Requests for Comments, Internet Engineering Task Force, RFC 792, September 1981. [Online]. Available: http://www.rfc-editor.org/rfc/rfc792.txt

[15] T. Narten, E. Nordmark, W. A. Simpson, and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)," Internet Requests for Comments, Internet Engineering Task Force, RFC 4861, September 2007.

[16] C. Low, "Icmp attacks illustrated," https://www.sans.org/reading-room/whitepapers/threats/paper/477, Accessed March 2022.

[17] R. Myers, "Attacks on tcp/ip protocols," https://www.utc.edu/center-academic-excellence-cyber-defense/pdfs/course-paper-5620-attacktcpip.pdf, Accessed March 2022.

[18] S. Waichal and B. Meshram, "Router attacks-detection and defense mechanisms," *International Journal of Scientific & Technology Research*, vol. 2, no. 6, 2013.

[19] A. Ornaghi and M. Valleri, "Man in the middle attacks," in *Blackhat Conference Europe*, vol. 1045, 2003.

[20] S. M. Bellovin, "Security problems in the tcp/ip protocol suite," *ACM SIGCOMM Computer Communication Review*, vol. 19, no. 2, pp. 32–48, 1989.

[21] ——, "A look back at "security problems in the tcp/ip protocol suite"," in *20th Annual Computer Security Applications Conference*. IEEE, 2004, pp. 229–249.

[22] W. Du, *Computer & Internet Security: A Hands-on Approach*. Wenliang Du, 2019.

[23] Ivan, "Icmp redirect attacks with scapy," https://ivanitlearning.wordpress.com/2019/05/20/icmp-redirect-attacks-with-scapy/, Accessed March 2022.

[24] J. Thyer, "Better spoofing of icmp host redirect messages with scapy," http://blog.packetheader.net/2010/06/better-spoofing-of-icmp-host-redirect.html, Accessed March 2022.

[25] A. Ayer, "Icmp redirect attacks in the wild," https://www.agwa.name/blog/post/icmp_redirect_attacks_in_the_wild, Accessed March 2022.

[26] Zimperium, "Doubledirect," https://blog.zimperium.com/doubledirect-zimperium-discovers-full-duplex-icmp-redirect-attacks-in-the-wild/, Accessed March 2022.

[27] R. Braden, "Requirements for Internet Hosts - Communication Layers," Internet Requests for Comments, Internet Engineering Task Force, RFC 1122, October 1989. [Online]. Available: http://www.rfc-editor.org/rfc/rfc1122.txt

[28] R. Beverly, R. Durairajan, D. Plonka, and J. P. Rohrer, "In the ip of the beholder: Strategies for active ipv6 topology discovery," in *Proceedings of the Internet Measurement Conference 2018*, 2018, pp. 308–321.

[29] G. Song, L. He, Z. Wang, J. Yang, T. Jin, J. Liu, and G. Li, "Towards the construction of global ipv6 hitlist and efficient probing of ipv6 address space," in *2020 IEEE/ACM 28th International Symposium on Quality of Service (IWQoS)*. IEEE, 2020, pp. 1–10.

[30] G. Song, J. Yang, Z. Wang, L. He, J. Lin, L. Pan, C. Duan, and X. Quan, "Det: Enabling efficient probing of ipv6 active addresses," *IEEE/ACM Transactions on Networking*, 2022.

[31] B. Leiner, R. Cole, J. Postel, and D. Mills, "The darpa internet protocol suite," *IEEE Communications Magazine*, vol. 23, no. 3, pp. 29–34, 1985.

[32] S. Shakkottai, T. S. Rappaport, and P. C. Karlsson, "Cross-layer design for wireless networks," *IEEE Communications magazine*, vol. 41, no. 10, pp. 74–80, 2003.

[33] P. Srisuresh and K. B. Egevang, "Traditional IP Network Address Translator (Traditional NAT)," Internet Requests for Comments, Internet Engineering Task Force, RFC 3022, January 2001. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3022.txt

[34] P. Srisuresh, B. Ford, S. Sivakumar, and S. Guha, "NAT Behavioral Requirements for ICMP," Internet Requests for Comments, Internet Engineering Task Force, RFC 5508, April 2009. [Online]. Available: http://www.rfc-editor.org/rfc/rfc5508.txt

[35] Scapy, "Packet crafting for python2 and python3," https://scapy.net/, Accessed March 2022.

[36] K. Man, Z. Qian, Z. Wang, X. Zheng, Y. Huang, and H. Duan, "Dns cache poisoning attack reloaded: Revolutions with side channels," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2020, pp. 1337–1350.

[37] K. Man, X. Zhou, and Z. Qian, "Dns cache poisoning attack: Resurrections with side channels," in *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2021, pp. 3400–3414.

[38] D. Wu, D. Gao, R. K. Chang, E. He, E. K. Cheng, and R. H. Deng, "Understanding open ports in android applications: Discovery, diagnosis, and security assessment," 2019.

[39] B. Mitchell, "Understanding infrastructure mode in wireless networking," https://www.lifewire.com/infrastructure-mode-in-wireless-networking-816539, Accessed March 2022.

[40] F. Baker, "Requirements for IP Version 4 Routers," Internet Requests for Comments, Internet Engineering Task Force, RFC 1812, June 1995. [Online]. Available: http://www.rfc-editor.org/rfc/rfc1812.txt

[41] T. Killalea, "Recommended Internet Service Provider Security Services and Procedures," Internet Requests for Comments, Internet Engineering Task Force, RFC 3013, November 2000. [Online]. Available: http://www.rfc-editor.org/rfc/rfc3013.txt

[42] J. Wu, J. Bi, X. Li, G. Ren, K. Xu, and M. I. Williams, "A Source Address Validation Architecture (SAVA) Testbed and Deployment Experience," Internet Requests for Comments, Internet Engineering Task Force, RFC 5210, June 2008. [Online]. Available: http://www.rfc-editor.org/rfc/rfc5210.txt

[43] J. Wu, J. Bi, M. Bagnulo, F. Baker, and C. Vogt, "Source Address Validation Improvement (SAVI) Framework," Internet Requests for Comments, Internet Engineering Task Force, RFC 7039, October 2013. [Online]. Available: http://www.rfc-editor.org/rfc/rfc7039.txt

[44] S. Hijazi and M. S. Obaidat, "Address resolution protocol spoofing attacks and security approaches: A survey," *Security and Privacy*, vol. 2, no. 1, pp. 1–9, 2019.

[45] Linux, "Arp spoofing protection for linux kernels," http://burbon04.gmxhome.de/linux/ARPSpoofing.html, Accessed March 2022.

[46] Materialize and DominikTV, "csploit," http://www.csploit.org/, Accessed March 2022.

[47] S. Y. Nam, S. Jurayev, S.-S. Kim, K. Choi, and G. S. Choi, "Mitigating arp poisoning-based man-in-the-middle attacks in wired or wireless lan," *EURASIP Journal on Wireless Communications and Networking*, vol. 2012, no. 1, pp. 1–17, 2012.

[48] M. F. A. Rahman and P. Kamal, "Holistic approach to arp poisoning and countermeasures by using practical examples and paradigm," *International Journal of Advancements in Technology*, vol. 5, no. 2, pp. 82–95, 2014.
[49] T. Fortunato, "Network analysis: Investigating icmp redirects (here's why you should pay attention to icmp redirects in network troubleshooting)," https://www.networkcomputing.com/networking/network-analysis-investigating-icmp-redirects, Accessed March 2022.
[50] USRobotics, "Wireless lan networking," https://support.usr.com/download/whitepapers/wireless-wp.pdf, Accessed March 2022.
[51] W.-F. Alliance, "Discover wi-fi security," https://www.wi-fi.org/discover-wi-fi/security, Accessed March 2022.
[52] B. Robinson, "How secure is wi-fi really," https://www.wwt.com/article/how-secure-is-wifi-really/, Accessed March 2022.
[53] J. Steube, "New attack on wpa/wpa2 using pmkid," https://hashcat.net/forum/thread-7717.html, Accessed March 2022.
[54] S. Alblwi and K. Shujaee, "A survey on wireless security protocol wpa2," in *Proceedings of the international conference on security and management (SAM)*. The Steering Committee of The World Congress in Computer Science, Computer . . . , 2017, pp. 12–17.
[55] W.-F. Alliance, "Wpa3 specification," https://www.wi-fi.org/download.php?file=/sites/default/files/private/WPA3_Specification_v3.0.pdf, Accessed March 2022.
[56] D. Kulas, "Type=5, code=1 (or lady in the middle)," https://hackinparis.com/archives/2016/#talk-2016-lady-in-the-middle, Accessed March 2022.
[57] X. Feng, C. Fu, Q. Li, K. Sun, and K. Xu, "Off-path tcp exploits of the mixed ipid assignment," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, 2020, p. 1323–1335.
[58] Y. Cao, Z. Qian, Z. Wang, T. Dao, S. V. Krishnamurthy, and L. M. Marvel, "Off-path tcp exploits: Global rate limit considered dangerous," in *25th USENIX Security Symposium (USENIX Security 16)*, 2016, pp. 209–225.
[59] ——, "Off-path tcp exploits of the challenge ack global rate limit," *IEEE/ACM Transactions on Networking*, vol. 26, no. 2, pp. 765–778, 2018.
[60] W. Chen and Z. Qian, "Off-path tcp exploit: How wireless routers can jeopardize your secrets," in *27th USENIX Security Symposium (USENIX Security 18)*, 2018, pp. 1581–1598.
[61] X. Feng, Q. Li, K. Sun, C. Fu, and K. Xu, "Off-path tcp hijacking attacks via the side channel of downgraded ipid," *IEEE/ACM Transactions on Networking*, vol. 30, no. 1, pp. 409–422, 2022.
[62] G. Nakibly, A. Kirshon, D. Gonikman, and D. Boneh, "Persistent ospf attacks." in *NDSS*, 2012.
[63] G. Nakibly, A. Sosnovich, E. Menahem, A. Waizel, and Y. Elovici, "Ospf vulnerability to persistent poisoning attacks: a systematic analysis," in *Proceedings of the 30th Annual Computer Security Applications Conference*, 2014, pp. 336–345.
[64] Y. Song, S. Gao, A. Hu, and B. Xiao, "Novel attacks in ospf networks to poison routing table," in *2017 IEEE International Conference on Communications (ICC)*. IEEE, 2017, pp. 1–6.
[65] O. Nordström and C. Dovrolis, "Beware of bgp attacks," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 1–8, 2004.
[66] P. Sermpezis, V. Kotronis, A. Dainotti, and X. Dimitropoulos, "A survey among network operators on bgp prefix hijacking," *ACM SIGCOMM Computer Communication Review*, vol. 48, no. 1, pp. 64–69, 2018.
[67] S. Cho, R. Fontugne, K. Cho, A. Dainotti, and P. Gill, "Bgp hijacking classification," in *2019 Network Traffic Measurement and Analysis Conference (TMA)*. IEEE, 2019, pp. 25–32.
[68] Y. Gilad and A. Herzberg, "Fragmentation considered vulnerable: Blindly intercepting and discarding fragments," in *Proceedings of the 5th USENIX conference on Offensive technologies*. USENIX Association, 2011, pp. 2–2.
[69] ——, "Fragmentation considered vulnerable," *ACM Transactions on Information and System Security (TISSEC)*, vol. 15, no. 4, p. 16, 2013.
[70] A. Herzberg and H. Shulman, "Fragmentation considered poisonous, or: One-domain-to-rule-them-all. org," in *2013 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2013, pp. 224–232.
[71] M. Brandt, T. Dai, A. Klein, H. Shulman, and M. Waidner, "Domain validation++ for mitm-resilient pki," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2018, pp. 2060–2076.
[72] A. Herzberg and H. Shulman, "Towards adoption of dnssec: Availability and security challenges," *IACR Cryptology ePrint Archive*, vol. 2013, p. 254, 2013.
[73] J. McCann, S. Deering, and J. Mogul, "Path mtu discovery for ip version 6," Internet Requests for Comments, Internet Engineering Task Force, RFC 1981, August 1996. [Online]. Available: http://www.rfc-editor.org/rfc/rfc1981.txt
[74] J. Mogul and S. Deering, "Path mtu discovery," Internet Requests for Comments, Internet Engineering Task Force, RFC 1191, November 1990. [Online]. Available: http://www.rfc-editor.org/rfc/rfc1191.txt
[75] M. Lepinski and K. Sriram, "BGPsec Protocol Specification," Internet Requests for Comments, Internet Engineering Task Force, RFC 8205, September 2017. [Online]. Available: http://www.rfc-editor.org/rfc/rfc8205.txt
[76] M. Bhatia, V. Manral, M. J. Fanto, R. I. White, M. Barnes, T. Li, and R. J. Atkinson, "OSPFv2 HMAC-SHA Cryptographic Authentication," Internet Requests for Comments, Internet Engineering Task Force, RFC 5709, October 2009. [Online]. Available: http://www.rfc-editor.org/rfc/rfc5709.txt

APPENDIX

A. Implementation of Enhancing Supplicants to Check the Received ICMP Redirect Messages

Figure 8 shows part of the source code for implementing our countermeasure in Linux 4.18 that enhances supplicants to perform a more precise check on the received ICMP redirect message. If source IP address and source MAC address of the received ICMP redirect message are inconsistent, i.e., a crafted message from attackers (see Figure 7(b)), the supplicant protected by our countermeasure will discard the message to prevent potential attacks.

```
1. static bool icmp_redirect (struct sk_buff *skb)
2. {
       .....
3.     /*identify source MAC address of the received ICMP redirect message*/
4.     struct ethhdr *eth = (struct ethhdr *) skb_mac_header (skb);
5.     memcpy (source_mac, eth->h_source, ETH_ALEN);
6.     /*identify source IP address of the message*/
7.     struct iphdr* firstiph = ip_hdr (skb);
8.     u32 src_ip = firstiph->saddr;
9.     /*locate the network adapter*/
10.    struct rtable *rt = skb_rtable (skb);
11.    struct net_device *dev = rt->dst.dev;
12.    /*identify MAC address of source IP of the received message*/
13.    struct neighbour *neigh = __ipv4_neigh_lookup_noref (dev, src_ip);
14.    memcpy (ap_real_mac, neigh->ha, 6);
15.    /*check whether source MAC address of the received message is equal to
         the identified MAC address of the message's source IP, if not, discard it*/
16.    if (strncmp (source_mac, ap_real_mac, ETH_ALEN) != 0){
17.        return false;
18.    }
19.    /*the message is legal and delivered to be handled*/
20.    icmp_socket_deliver (skb, icmp_hdr(skb)->un.gateway);
21.    return true;
22. }
```

Fig. 8. Implementation of enhancing supplicants to check the received ICMP redirect message in Linux 4.18.

We modify "`static bool icmp_redirect(){}`" in Linux kernel 4.18 to implement our countermeasure. First, we identify source MAC address of the received ICMP redirect message in the struct of "`sk_buff *skb`" and store the

identified MAC address into "source_mac" (as shown in line 4 and line 5 of Figure 8). Then, we identify source IP address of the message and store the identified IP address into "src_ip" (see line 7 and line 8 in Figure 8). Before calling the function of "__ipv4_neigh_lookup_noref()" in line 13 to get the corresponding MAC address of "src_ip", we have to locate the network adapter of the supplicant used to access the Wi-Fi network. Once the MAC address of "src_ip" is identified, we then store it into "ap_real_mac" (see line 13 and line 14).

Finally, we compare the two identified MAC addresses "source_mac" and "ap_real_mac". If they are not equal, we discard the ICMP message (see line 16 and line 17). Instead, if "source_mac" and "ap_real_mac" are equal (the message is legal and is issued from the legitimate AP), we deliver the message to be handled in line 20, i.e., updating the supplicant's gateway.

Our countermeasure can block the crafted ICMP redirect message issued from attackers, thus foiling the MITM attack presented in this paper. Meanwhile, it does not rely on the AP routers and preserves the normal functionality of the redirect mechanism defined in ICMP specifications. If the ICMP redirect message is truly issued from the legitimate AP, the supplicant protected by our countermeasure will respond to the message to optimize its routing accordingly.

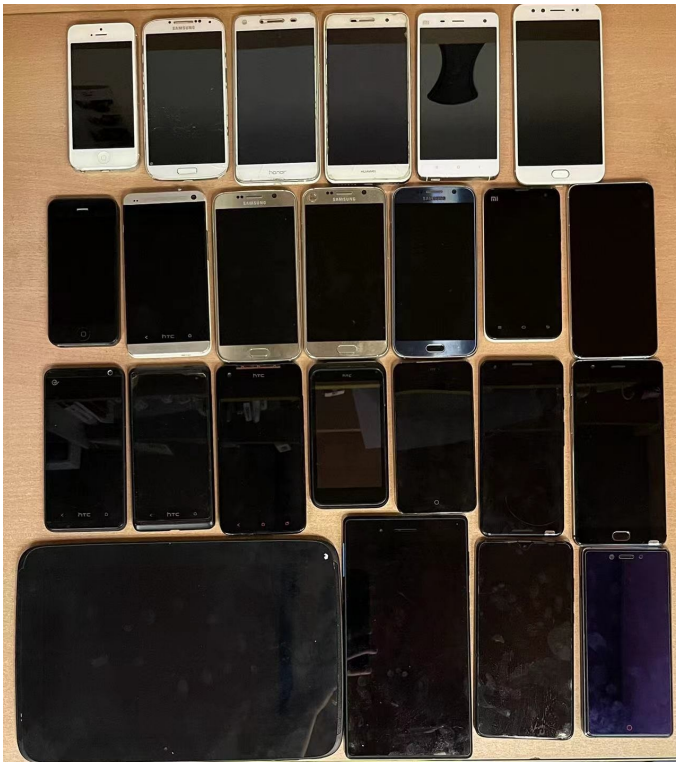


Fig. 9. Mobile devices in our tests.