# AirSnitch: Demystifying and Breaking Client Isolation in Wi-Fi Networks

**Xin'an Zhou,** UC Riverside and now Palo Alto Networks
**Juefei Pu,** UC Riverside
**Zhutian Liu,** UC Riverside
**Zhiyun Qian,** UC Riverside
**Zhaowei Tan,** UC Riverside
**Srikanth V. Krishnamurthy,** UC Riverside
**Mathy Vanhoef,** KU Leuven

2/25/2026

# Prologue

- Some interesting academic questions during PhD:
  - *Can two hosts with the same MAC address exist on the same subnet?*
  - **Yes!** One can manipulate “**Ether**” to achieve this.
  - Unfortunately, Wi-Fi inherits this design error of Ethernet too!

# Manipulating “Ether”

- While physics abandoned the “ether” as illusion, we identify “ether” as attacker’s hidden substrate in Wi-Fi Security.
- AirSnitch can abuse “ether”, i.e., low-level **protocol-infrastructure interactions**, to bypass Wi-Fi client isolation.
- This “gem in the desert” has been **hidden since Wi-Fi is born**.
  - Affecting WEP up to WPA2/3!

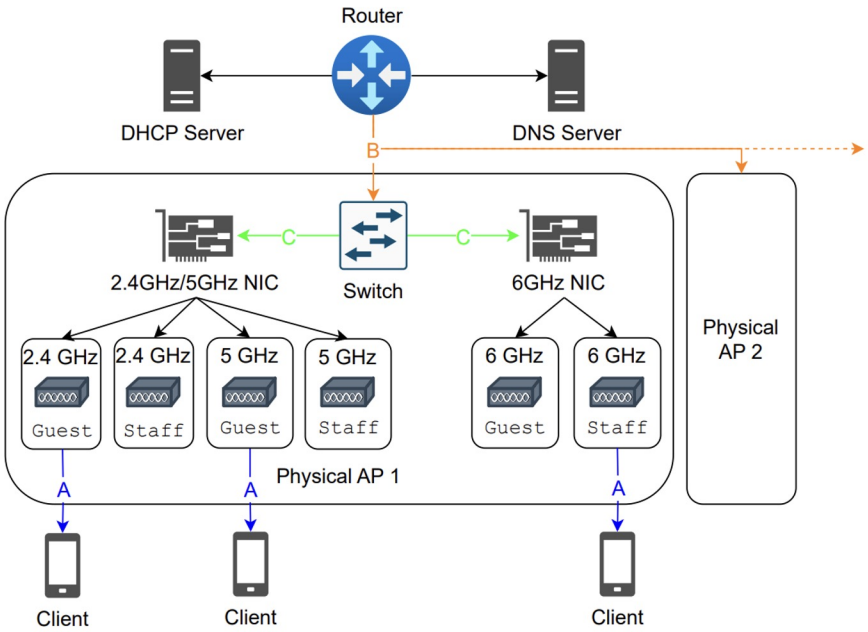
Image Credit: https://scalar.usc.edu/works/ethan-frome-a-digital-scholarly-edition/media/ether

# Introduction

- TL;DR: We bypass Wi-Fi client isolation to realize bidirectional MitM in modern Wi-Fi networks. Our attacks apply to all WPA2/3 configurations.
- We consider **insider attackers** since we aim to break client isolation, i.e., the adversary has legitimate access to the Wi-Fi network.
- To this end, we:
  (1) Demystify Wi-Fi client isolation.
  (2) Develop novel techniques that attack Wi-Fi standard.
  (3) Open-source our AirSnitch[1] tool for users to measure their networks.

[1] https://github.com/zhouxinan/airsnitch, and https://github.com/vanhoefm/airsnitch

# Demystifying Wi-Fi client isolation




(A): Wi-Fi encryption
(B): Routing
(C): Switching

Important Conclusion: WPA2/3-Enterprise encryption does not extend protection beyond link layer (layer 2)!

# More technically...

(1) WPA1/2/3 Enterprise prevents over-the-air sniffing.

(2) Intra-BSSID isolation (i.e., `ap_isolate=1` in `hostapd`) blocks direct communication between clients on the **same** BSSID.

(3) Inter-BSSID isolation blocks traffic between clients connected to **different** BSSIDs.

(4) Guest network configurations (i.e., separate and restricted SSIDs).

# Abusing Shared Keys - Techniques

1. Machine-on-the-Side: Works for *WPA2-Personal*, calculates victim PTK using shared passphrase and randomness, and then read/write frames over-the-air (OTA).

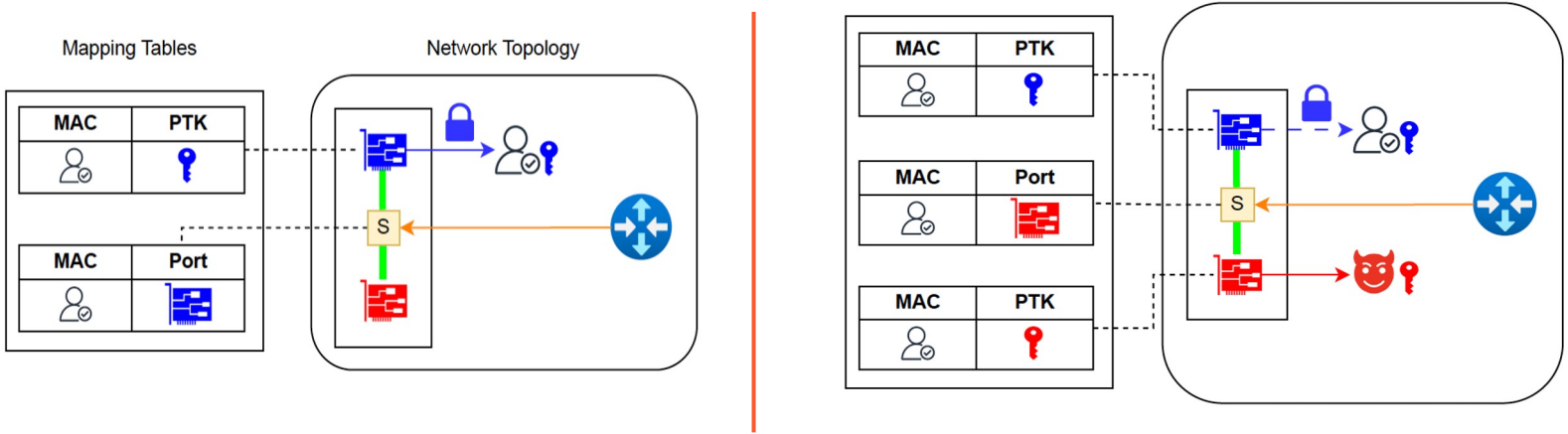
2. Rogue AP Bypass: Works for *WPA2/3-Personal*, by cloning the AP using the shared passphrase.

3. Abusing GTK: Works for *WPA2/3-Personal/Enterprise*, by abusing per-BSSID shared GTK to deliver frames to victims OTA.

# Attacking Switching / Manipulating “Ether”

1. Wi-Fi can inherit same vulnerabilities from Ethernet, letting two hosts with the same MAC address **co-exist**.

2. In Wi-Fi, every BSSID on the same AP can be viewed as a virtualized hardware port (layer-1 port, NOT layer-3 TCP/UDP port).




(a) AP - Before Spoofing

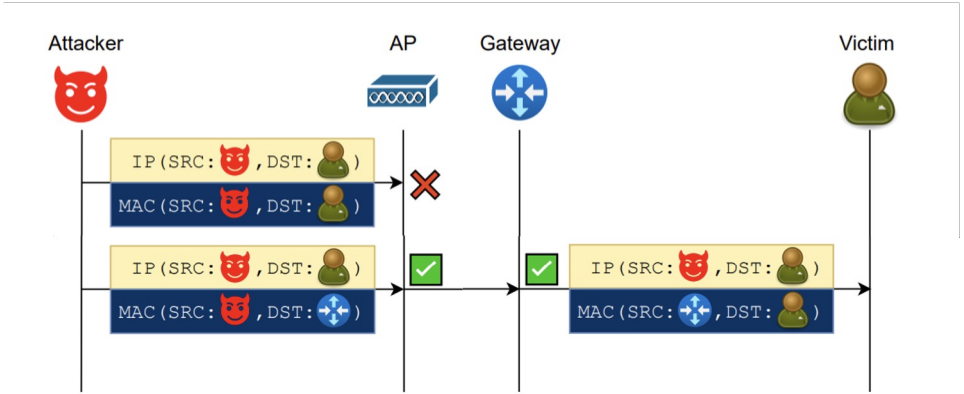
(b) AP - After Spoofing

# Lookback

- Spoofed frames must use correct WPA PTK on another BSSID than the victim BSSID.
- One reason the attacks work is because there is no strong synchronization between identities at different layers, i.e., between Wi-Fi keys, MAC addresses, and IP addresses.

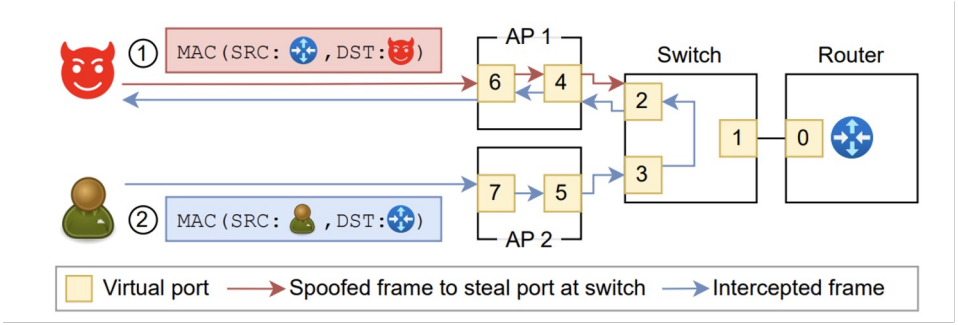
# Attacking Routing

- Gateway Bouncing bypasses client isolation at layer 3.



# Cross-AP attacks and higher-layer attacks

- Cross-AP attacks are practical.




- Higher-layer attacks can be enabled.
  - TCP hijacking and DNS cache poisoning.
  - RADIUS secret guessing.

# Measurements

| Device Model | Direct L2 Forwarding | | | | Abusing GTK | | Gateway Bouncing | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | G→M | M→M | G→G | M→G | M→M | G→G | G→M | M→M | G→G | M→G |
| Netgear Nighthawk X6 R8000 | × | ✓ | × | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Tenda RX2 Pro | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | × | ✓ | ✓ | × |
| D-Link DIR-3040 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| TP-Link Archer AXE75 | × | ✓ | × | × | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| ASUS RT-AX57 | ✓ | × | ✓ | × | ✓ | ✓ | × | ✓ | × | ✓ |
| DD-WRT v3.0-r44715 | × | ✓ | × | × | ✓ | ✓ | × | ✓ | × | × |
| OpenWrt 24.10 | × | × | ✓ | × | ✓ | ✓ | × | ✓ | × | × |
| Ubiquiti AmpliFi Alien Router | × | ✓ | ✓ | × | ✓ | ✓ | × | ✓ | ✓ | ✓ |
| Ubiquiti AmpliFi Router HD | × | ✓ | ✓ | × | ✓ | ✓ | × | ✓ | ✓ | ✓ |
| Cisco Catalyst 9130 | × | × | × | × | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| LANCOM LX-6500 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

M: Main network, G: Guest network; $X \rightarrow Y$: whether a client in network $X$ can inject a packet towards another client in network $Y$.

(1) Traffic Injection is prevalent!

| Device Model | Downlink Port Stealing | | | | Uplink Port Stealing | | | |
|---|---|---|---|---|---|---|---|---|
| | G←M | M←M | G←G | M←G | G←M | M←M | G←G | M←G |
| Netgear Nighthawk X6 R8000 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | × | × |
| Tenda RX2 Pro | × | × | × | × | N/A★ | ✓ | N/A★ | N/A★ |
| D-Link DIR-3040 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| TP-Link Archer AXE75 | ✓ | × | ✓ | ✓ | ✓ | ✓ | × | ✓ |
| ASUS RT-AX57 | × | ✓ | × | × | ✓ | ✓ | ✓ | ✓ |
| DD-WRT v3.0-r44715 | × | × | × | × | × | ✓ | × | × |
| OpenWrt 24.10 | × | × | × | × | × | × | × | × |
| Ubiquiti AmpliFi Alien Router | × | ✓ | ✓ | × | × | ✓ | × | × |
| Ubiquiti AmpliFi Router HD | × | ✓ | ✓ | × | × | ✓ | × | × |
| Cisco Catalyst 9130 | ✓ | ✓ | ✓ | ✓ | × | × | × | × |
| LANCOM LX-6500 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

★ Tenda RX2 Pro does not support guest SSIDs under AP mode. M: Main network, G: Guest network.
$X \leftarrow Y$: whether a client in network $X$ can intercept traffic of another client in network $Y$.

(2) Traffic Interception is prevalent!

| OS | group-ping | group-ping6 | group-arp-unicast |
|---|---|---|---|
| **Windows 11** | | | |
| Firewall On | × | ✓ | ✓ |
| Firewall Off | ✓ | ✓ | ✓ |
| **Others** | | | |
| macOS 15.4 | ✓ | ✓ | ✓ |
| iOS 18.3.2 | ✓ | ✓ | ✓ |
| Android 14 | ✓ | ✓ | ✓ |
| Ubuntu 22.04 | ×* | ✓ | ✓ |

✓: Test case passed (OS replied to the probe).
×: Test case failed (OS did not reply).
∗: When `drop_unicast_in_l2_multicast` is enabled, the group-ping test case does not result in a reply.

(3) Mainstream OSes are vulnerable!

| Exp. | Setup | Performance | | | |
|---|---|---|---|---|---|
| | Attacker | Loss | Throughput | Jitter | Success |
| Base | Near AP | 1.7% | 8.89 Mbps | 1.23ms | 5/5 |
| Distance | Far | 3.1% | 8.93 Mbps | 0.61ms | 5/5 |
| Barrier | Wall-sep. | 7.0% | 8.59 Mbps | 2.08ms | 5/5 |

† Loss = loss rate ignoring initial disruption; Success = end-to-end success rate.

(4) Attackers could succeed end-to-end.

# Defense

- Improving Network Isolation.
- Spoofing Prevention.
- Group Key Security.
- Using Device-to-device Encryption to Protect Wi-Fi Traffic.
- Standardizing client isolation.

# Takeaways

- WPA encryption protocols proven secure
- However, the protocol-infrastructure interaction is not secure.

# Thank you! Questions?

Github Link (open-source date: 2/25/2026):

https://github.com/zhouxinan/airsnitch

https://github.com/vanhoefm/airsnitch

Contacts:

xinan.zhou@email.ucr.edu

zhiyunq@cs.ucr.edu

mathy.vanhoef@kuleuven.be