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

Xin'an Zhou*, Juefei Pu*, Zhutian Liu*, Zhiyun Qian*, Zhaowei Tan*, Srikanth V. Krishnamurthy*, Mathy Vanhoef†
*University of California, Riverside †DistriNet, KU Leuven
{xzhou114,jpu007,zliu272}@ucr.edu, {zhiyunq,ztan,krish}@cs.ucr.edu
mathy.vanhoef@kuleuven.be

Abstract

To prevent malicious Wi-Fi clients from attacking other clients on the same network, vendors have introduced client isolation, a combination of mechanisms that block direct communication between clients. However, client isolation is not a standardized feature, making its security guarantees unclear.

In this paper, we undertake a structured security analysis of Wi-Fi client isolation and uncover new classes of attacks that bypass this protection. We identify several root causes behind these weaknesses. First, Wi-Fi keys that protect broadcast frames are improperly managed and can be abused to bypass client isolation. Second, isolation is often only enforced at the MAC or IP layer, but not both. Third, weak synchronization of a client's identity across the network stack allows one to bypass Wi-Fi client isolation at the network layer instead, enabling the interception of uplink and downlink traffic of other clients as well as internal backend devices. Every tested router and network was vulnerable to at least one attack. More broadly, the lack of standardization leads to inconsistent, ad hoc, and often incomplete implementations of isolation across vendors.

Building on these insights, we design and evaluate end-to-end attacks that enable full machine-in-the-middle capabilities in modern Wi-Fi networks. Although client isolation effectively mitigates legacy attacks like ARP spoofing, which has long been considered the only universal method for achieving machine-in-the-middle positioning in local area networks, our attack introduces a general and practical alternative that restores this capability, even in the presence of client isolation.

I. Main Content

This work [1] was recently accepted to The Network and Distributed System Security (NDSS) Symposium 2026 and the assigned DOI is: https://dx.doi.org/10.14722/ndss.2026.241282. The original abstract and author list are shown above.

References

[1] X. Zhou, J. Pu, Z. Liu, Z. Qian, Z. Tan, S. V. Krishnamurthy, and M. Vanhoef, "Airsnitch: Demystifying and breaking client isolation in wi-fi networks," in *NDSS*, 2026.

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

Xin'an Zhou*, Juefei Pu*, Zhutian Liu*, Zhiyun Qian*, Zhaowei Tan*, Srikanth V. Krishnamurthy*, Mathy Vanhoef†

*University of California, Riverside †DistriNet, KU Leuven

NDSS SYMPOSIUM

Introduction

- Client isolation is a widely deployed defense in Wi-Fi networks to block direct communication between clients.
- We examine the robustness of client isolation mechanisms against insider adversaries across encryption, switching, and routing layers.
- We aim to determine whether Wi-Fi networks remain vulnerable to machine-in-the-middle attacks despite client isolation, given its ad hoc and non-standardized implementations.
- Yes, your Wi-Fi and OS are affected too!

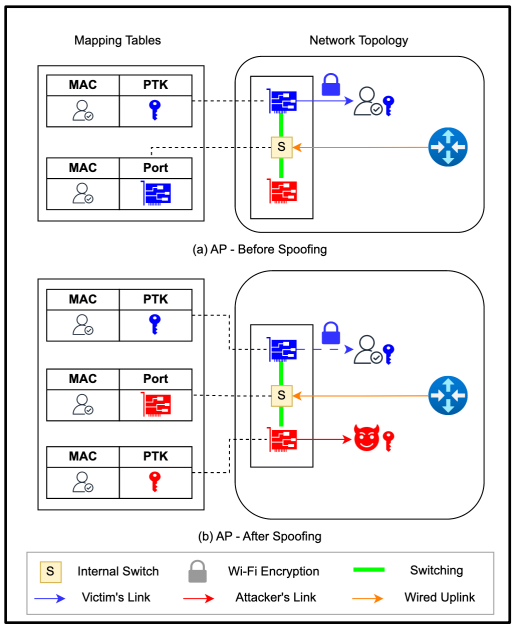
Technical Approach and Novel MitM Techniques (selected)

Threat Modeling

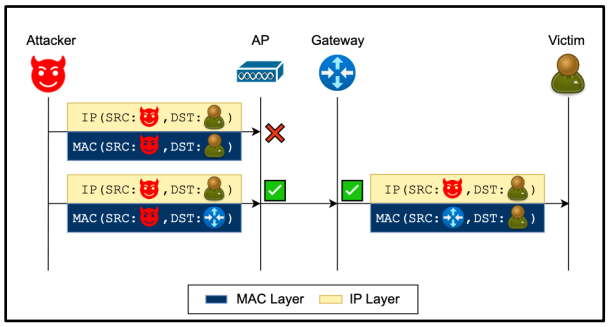
- Attacker as an authenticated Wi-Fi client who aims to bypass client isolation to intercept or inject traffic.
- Attacker that transmits and receives wireless frames over-the-air, possibly across multiple channels with multiple NICs.
- Attacker that controls an Internet server to accept exfiltrated traffic or facilitate higher-layer attacks.

Attack Techniques Developed

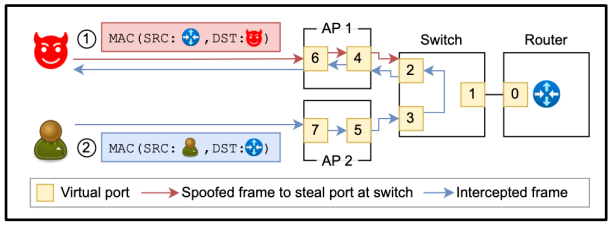
- Port Stealing ①
- Gateway Bouncing ②
- Rogue AP, Machine-on-the-side
- Abusing GTK
- Broadcast Reflection
- Server/Client-triggered Port Restoration
- Inter-NIC Relaying



Port Stealing ① exploits switching on APs



Gateway Bouncing ② exploits IP routing to inject packets.



Cross-AP MitM attacks are practical

Evaluation Method

- We analyze packet forwarding behaviors across Wi-Fi encryption, switching, and routing layers.
- We test commodity routers, open-source firmware, and enterprise APs with client isolation enabled.
- We perform controlled lab experiments and in-the-wild measurements on university networks.

Evaluation Results

MEASUREMENT OF THE FEASIBILITY OF INJECTING TRAFFIC FOR SELECTED SINGLE APS. ALL TESTED WITH CLIENT ISOLATION ENABLED. TOP DEVICES ARE HOME ROUTERS, BOTTOM DEVICES ARE ALL-IN-ONE ENTERPRISE ROUTERS.

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; $X \to Y$: whether a client in network X can inject a packet towards another client in network Y.

Impact

- **All tested routers and networks were vulnerable to at least one client isolation bypass.**
- **Even WPA2/3-Enterprise and university deployments leaked traffic.**

Future Work

- Design mitigations that tightly bind Wi-Fi identities (MAC, IP, keys) across layers.
- Discover more building blocks for MitM attacks.
- Track and follow up on vendor mitigations.