LINKEDIN POST

Stop treating Wi-Fi client isolation as a security boundary.

By **Keith Parsons, CWNE #3** · 2026-08-19 · originally on LinkedIn

AirSnitch just proved why.

If you lean on station isolation, AP isolation, or PSPF to keep guest, hospitality, or BYOD clients apart, read this. Researchers tested 11 consumer and enterprise routers and APs, plus DD-WRT and OpenWrt. Every one was vulnerable to at least one of the attacks.

Be precise: AirSnitch does NOT break Wi-Fi encryption. It defeats client isolation, the convenience feature we have leaned on for years to separate same-SSID clients.

Three attack classes:

Group-key injection. Clients on a BSS share the GTK, so a broadcast frame carrying a unicast IP packet reaches a victim that isolation never inspects.

Gateway bouncing. When isolation lives only at L2, route around it through the gateway at L3.

Port stealing. Poison the bridging table to redirect another client's traffic through the attacker.

The root cause that matters: client isolation was never standardized by the IEEE. There is no 802.11 spec for it, so every vendor built it their own way, which is exactly why no single patch exists.

Disclosed at NDSS 2026 by UC Riverside and Mathy Vanhoef of KU Leuven, the researcher behind KRACK.

The fix is architectural. Apply your vendor's guidance, then segment at L3: untrusted clients on their own VLAN and subnet, firewalled from everything else. Same-subnet isolation was

never enough.

Were we ever right to treat L2 client isolation as a security control, or have we papered over a missing standard for a decade?

How are you segmenting guest and BYOD traffic in production today?

#WiFi #WLAN #WiFiSecurity #CWNP

By Keith Parsons, CWNE #3, Wireless LAN Professionals. Free to read and share. Facts