2026 Wi-Fi Security Insights: Why Enterprise Wireless Is Still Being Compromised

https://www.linkedin.com/pulse/2026-wi-fi-security-insights-why-enterprise-wireless-de-oliveira-kfzwe

Your wireless network is running WPA3. Your RADIUS servers are online. Your certificates are deployed.

And you're still getting compromised.

That's the uncomfortable reality of enterprise Wi-Fi security in 2026. The protocols have matured. The tools are better than they've ever been. But the attack surface keeps expanding, attacker

capabilities are accelerating with AI, and the gap between what organisations *think* they've secured and what's actually exposed has never been wider.

Here's what the threat landscape actually looks like right now -- and what's still catching organisations out.

The Threat Landscape Has Changed

The 2025 version of this article covered the basics: weak passwords, outdated protocols, misconfigured RADIUS. Those issues haven't gone away. But they're no longer the headline.

What's changed in 2026:

AI-powered attacks are lowering the barrier to entry. Tools that used to require a skilled attacker can now be automated. AI-assisted tooling can mimic legitimate user behaviour, operate autonomously, and scale attacks in ways that manual techniques simply can't. According to Cisco's 2026 State of Wireless report, 35% of wireless leaders now cite AI-powered attacks as a top-three driver of increased wireless security threats.

Wireless vulnerabilities are accelerating. Bastille's 2026 State of Wireless Security report recorded an average of 2.5 new wireless vulnerabilities discovered per day throughout 2025. That's not a typo. Wireless is now one of the fastest-growing attack surfaces in enterprise environments.

Protocol trust is being challenged. Research presented at NDSS 2026 introduced a class of attacks called AirSnitch -- techniques that exploit subtle protocol-infrastructure interactions to break client isolation and intercept traffic, *even on properly configured WPA2 and WPA3-Enterprise networks*. These aren't theoretical. They affect major vendors and operate across Android, iOS, Windows, and macOS. The attack exploits how Wi-Fi handles low-level MAC address state, not the cryptographic layer itself. Your encryption is fine. Your infrastructure logic may not be.

What's Still Getting Organisations Compromised

1. Misconfigured EAP -- The Most Underestimated Issue

WPA3-Enterprise with EAP-TLS is the gold standard. Most organisations know this. Far fewer have actually deployed it correctly.

The most common failures:

- **No server certificate validation on the client side.** If clients don't validate the RADIUS server certificate, an attacker can stand up a rogue authentication server and harvest credentials with no warning to the user.
- **EAP-PEAP with MSCHAPv2 and no certificate pinning.** Still deployed widely. Still crackable offline once you've captured the authentication exchange.
- **Wildcard or expired certificates on RADIUS.** The network "works," so nobody notices. Until it matters.

If you haven't reviewed your EAP configuration recently -- specifically what clients will and won't accept during the authentication handshake -- that's where to start.

2. IoT and OT Devices as Wireless Entry Points

This one is growing fast. In Cisco's 2026 report, 36% of organisations reported disruptions tied to compromised IoT or OT systems. These devices connect to your wireless network, often to a shared SSID, with no endpoint security, no MDM, and firmware that hasn't been updated since deployment.

They're not just a compliance problem. They're a pivot point. A compromised wireless scanner, sensor, or camera on the same VLAN as production systems gives an attacker exactly the foothold they need.

Proper SSID segmentation with dedicated IoT VLANs and strict firewall policy between them is non-negotiable. If your IoT devices are on the same logical network as anything sensitive, that's a misconfiguration.

3. The Wireless Visibility Gap

Traditional security tooling -- firewalls, EDR, IP-based vulnerability scanners -- doesn't see the wireless air. Bastille's 2026 research highlights a critical visibility gap: personal Bluetooth peripherals, Zigbee sensors, transient guest devices, and cellular-connected equipment operating

completely outside your perimeter controls.

You can have a fully locked-down wired and Wi-Fi network and still have a Zigbee device bridging into your environment from three metres away. If you're not doing continuous passive RF monitoring, you don't have full visibility of your wireless attack surface -- full stop.

4. Deauthentication and Evil Twin Attacks -- Still Effective in 2026

802.11 management frame protection (802.11w / PMF) has been mandatory since Wi-Fi 6. And yet research continues to show that the majority of deployed networks remain vulnerable to deauthentication attacks, often because PMF hasn't been enforced (not just enabled) across all SSIDs, or because older client devices in mixed environments negotiate down.

Deauth is frequently a precursor -- knock a client off the legitimate network, force it to reassociate with a rogue AP, capture the credentials. It's a well-understood attack chain and it's still working.

5. PMKID Attacks -- Offline Cracking Without Interacting with a Client

PMKID-based attacks allow an attacker to capture the information needed for an offline brute-force attempt directly from the AP, without waiting for a client to connect. No deauth required. No active client interaction needed.

This is particularly relevant for any network still running WPA2-Personal with a passphrase that isn't truly random and complex. It's also a good reason why transitioning to WPA3's SAE handshake -- which resists offline dictionary attacks through its forward secrecy properties -- matters in practice, not just on paper.

Where Organisations Need to Focus

- **Audit your EAP configuration end-to-end.** Don't assume it's correct because it's working. Check client supplicant profiles, certificate validation settings, and RADIUS policy.

- **Enforce PMF on all SSIDs.** "Optional" PMF is not PMF. Required mode or it doesn't count.
- **Segment IoT and OT devices aggressively.** Dedicated SSIDs, dedicated VLANs, strict inter-VLAN policy. No exceptions.
- **Deploy WIDS/WIPS with active monitoring.** Passive detection of rogue APs, client misassociation, and evil twin attacks should be a baseline requirement.
- **Extend visibility beyond Wi-Fi.** Start looking at the wider RF environment -- not just 2.4 and 5 GHz. Bluetooth, Zigbee, and cellular-connected devices are part of your wireless attack surface whether you're monitoring them or not.
- **Migrate to EAP-TLS with certificate-based authentication.** PSKs and PEAP-MSCHAPv2 are operational risks. Every organisation still running them has a plan to move -- the question is whether that plan has a timeline.

Final Thought

The protocols aren't the problem. WPA3-Enterprise with EAP-TLS, properly implemented, is strong. The problem is the gap between what's been deployed and what's actually been *configured correctly* -- combined with an attack surface that now extends well beyond the Wi-Fi network itself.

In 2026, wireless security isn't a checkbox on a compliance form. It's an architecture decision that needs to be revisited regularly, audited seriously, and treated with the same rigour as any other critical infrastructure.

If you're not sure your wireless environment is as secure as it looks, it probably isn't.

Jarryd De Oliveira, CWNE #594, Chief Technical Architect at Renovotec Ltd.

Revision #1
Created 5 June 2026 04:20:47 by Jarryd
Updated 5 June 2026 04:21:08 by Jarryd