Review and Recommendations for AirSnitch

Contents

Introduction

This document describes a review of the Airsnitch white paper, with possible recommendations and actions. It applies to On-Prem and Cloud deployments

Summary

On 26 February 2026, researchers published a paper titled "AirSnitch: Demystifying and Breaking Client Isolation in Wi-Fi Networks." In this paper, the researchers presented methods for bypassing vendor-specific implementations of unicast client isolation protections for wireless clients within the same SSID. It must be noted that the proposed client isolation attacks are "insider attacks (malicious insider)" requiring the attacker to be associated and authenticated to the wireless infrastructure prior to launching the attack. These methods of bypass are not due to vulnerabilities in wireless specifications or products. There is also no vulnerability in the methods for encryption within the wireless network. These attacks are seen as opportunistic and would likely be unsuccessful in an enterprise network deployed with best-practice layered security for wireless, switching, and routing.

The primary goal of the AirSnitch attacks is to achieve a Machine-in-the-Middle (MitM) position, allowing an attacker to intercept, read, and modify traffic between a victim client and the Internet, even when client isolation is enabled. The study categorizes these bypasses into three layers:

- **Shared Key Abuse:** Exploiting the fact that broadcast/multicast keys (GTK) are shared among all clients within a Basic Service Set on an Access Point.
- **Injection Attacks at the Routing Layer (Gateway Bouncing):** Exploiting ARP injection/MAC address compromise at the network/IP layer.
- **Switching Layer (Port Stealing):** Exploiting the internal MAC-learning behavior of Access Points (APs) and switches.

Within the context of the consumer/SOHO AP, all capabilities are typically run within the single device (wireless AP, switch, and layer 3 router), leaving devices susceptible to misconfiguration or poor isolation between layers. For the enterprise, each vendor has best-practice network design to enable segmentation and isolation using Zero Trust principles within each layer of the network.

Also of note: no logging/alarming or management console was utilized in the enterprise scenario where typical alarms, such as duplicate MAC or IP address detection, were enabled—which most modern enterprise devices report and log.

The implication is that these insider attacks, specifically in the enterprise scenario, were launched within an unmanaged/unmonitored network or one where telemetry was not configured to be delivered to a security console (Security Incident and Event Monitoring software).

Affected Products

The attacks outlined in the paper on Enterprise APs might be successful when leveraged against Cisco Wireless Access Point products and Cisco Meraki Wireless Products (MR) where no additional best-practice

security configurations are deployed on the access points, wireless controllers, switching, and routing infrastructure.

Recommendations

To reduce the potential for the attacks outlined in the paper, Cisco recommends using best-practice defense-in-depth security within every layer of the network. General guidance and a summary of best practices follow:

- **Shared Key Abuse:** The abuse of shared keys (unicast or group) has been widely known since the vulnerabilities were disclosed with WPA2-Personal. Even with the advent of WPA3-Personal, the concept of shared keys results in any leakage of the key (handing it out, sharing between devices, social engineering) compromising not only the SSID but the entire enterprise network by allowing access to the network infrastructure. If deploying passphrase-based networking in the enterprise, care must be taken in monitoring and profiling those devices attaching to the network. Once the passphrase/password is delivered to a malicious insider, it is trivial to set up a "rogue AP" to institute a Machine-in-the-Middle attack. Shared Key networks (WPA2/WPA3-Personal) must not be considered "enterprise secure" unless active measures are taken to understand the devices on the network and employ other segmentation technologies (VLANs, VRFs, Fabrics, Firewalls, and so on.) as well as frequent rotation of the passphrase.

With regard to abusing the shared IGTK, telemetry within an enterprise-grade wireless network could alert based on seeing a WNM sleep message using the shared IGTK.

Cisco also recommends implementing transport layer security to encrypt data in transit whenever possible, because it would render the acquired data unusable by the attacker.

- **Injection Attacks at the Routing Layer (Gateway Bouncing) and Layer 2 Port Stealing:** The premise of this attack is that a malicious insider is allowed to route Layer 3 packets (or impact the ARP table of other devices within the BSS). Specifically, "we find that an attacker can send data packets with the destination IP address being that of the victim and the destination MAC address being that of the network’s gateway"—multiple mechanisms exist within enterprise-grade networking infrastructure that would mitigate and alert this type of malicious activity. Layer 2 and Layer 3 capabilities that are recommended within the enterprise are:

- **DHCP Snooping:** This prevents an attacker from spoofing a DHCP server and helps build a binding table of legitimate IP/MAC pairs.
- **Dynamic ARP Inspection (DAI):** Uses the DHCP Snooping binding table to intercept and discard ARP packets with invalid MAC-to-IP bindings, preventing the reconnaissance phase of MitM attacks.
- **Port Security:** Limits the number of MAC addresses allowed on a single physical port (the access points uplink) to prevent an attacker from flooding the switch with spoofed MAC addresses.
- **VLAN Access Control Lists (VACLs) / Router ACLs:** Explicitly deny traffic where both the source and destination IP addresses belong to the same client subnet. This prevents Gateway Bouncing by ensuring the router drops internal "hairpin" traffic.
- **IP Source Guard (IPSG):** Prevents IP spoofing by filtering traffic based on the DHCP Snooping binding database. If an attacker tries to send a packet with the IP address used by the victim, the switch drops it at the ingress port.
- **Unicast Reverse Path Forwarding (uRPF):** Helps ensure that packets arriving at an interface come from a legitimate, reachable source address, mitigating some forms of IP spoofing.

Conclusion

The research presented in the AirSnitch paper serves as a critical reminder that "Client Isolation" is a

localized feature rather than a comprehensive security boundary. While the researchers successfully demonstrated bypasses using their specific configurations that might not be aligned with vendor best practices, it is important to categorize these as opportunistic insider attacks that exploit a lack of security configuration between network layers rather than inherent flaws in wireless encryption protocols defined in 802.11 or the Wi-Fi Alliance.

For the enterprise, the primary takeaway is that security cannot rely on a single "on/off" toggle. The vulnerabilities identified—such as Gateway Bouncing and Port Stealing—are effectively neutralized when a defense-in-depth strategy is applied. By moving away from shared-key environments (WPA2/3-Personal) toward identity-based authentication (WPA3-Enterprise) and implementing robust Layer 2 and Layer 3 protections—including DHCP Snooping, Dynamic ARP Inspection (DAI), VACLs, and robust segmentation and classification of devices—organizations can ensure that client traffic remains isolated even if an adversary gains authenticated access to the SSID.

Furthermore, the lack of management telemetry in the researchers' enterprise test cases highlights the importance of visibility. In a managed Cisco environment, the anomalous behaviors required to execute these attacks—such as duplicate MAC addresses, IP spoofing, or unauthorized WNM messages—would trigger immediate alerts within a Security Incident and Event Management (SIEM) system.

Final Recommendation

Cisco customers must review their wireless deployments to ensure they are applying established Zero Trust architectures. By integrating wireless security with wired infrastructure protections and maintaining active monitoring, the risks posed by AirSnitch-style attacks are significantly mitigated, ensuring a secure and resilient network environment.