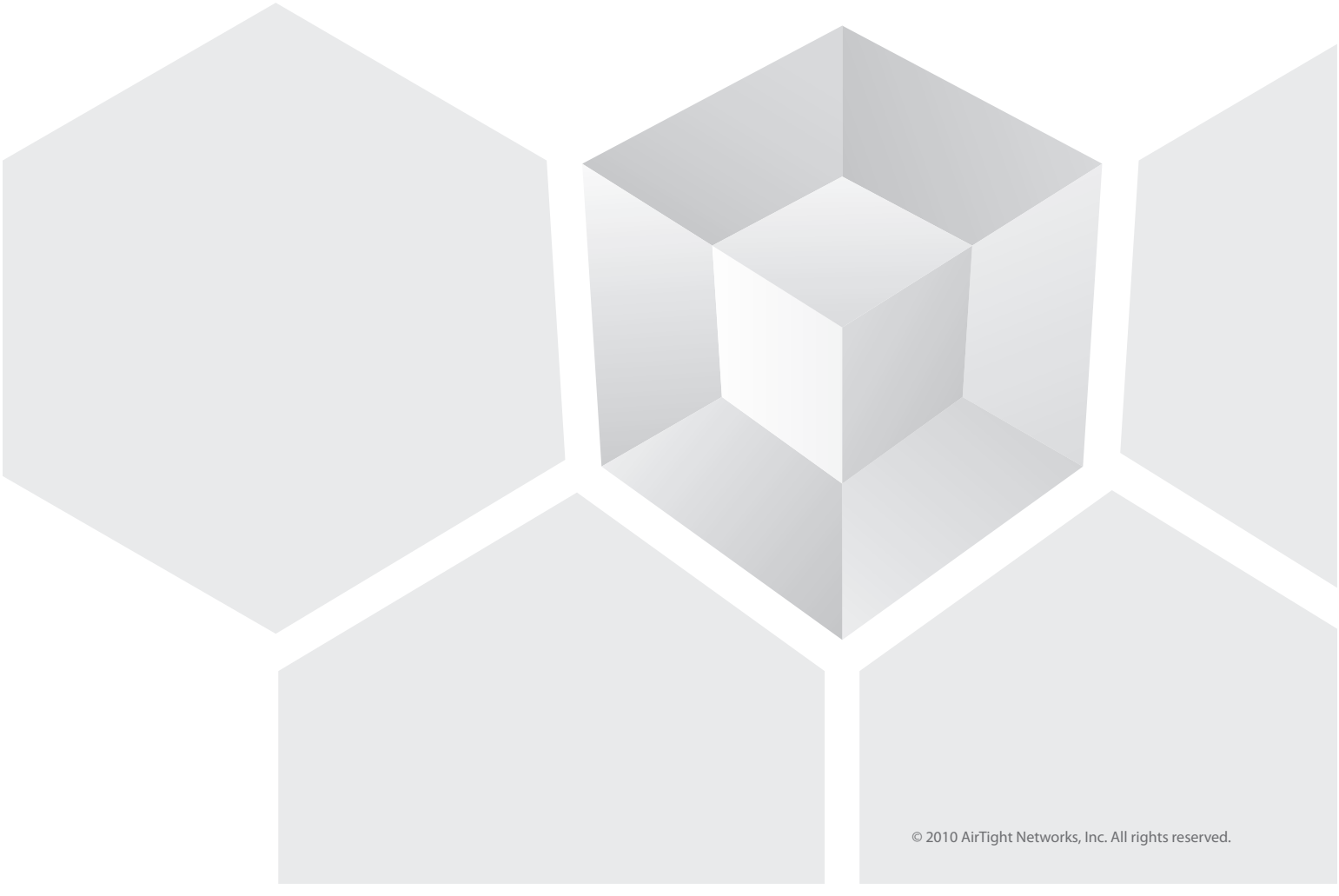
# WPA2 Hole196 Vulnerability: Exploits and Remediation Strategies

A Whitepaper by AirTight Networks, Inc.

339 N. Bernardo Avenue, Suite 200, Mountain View, CA 94043
www.airtightnetworks.com



WPA2 Hole196 Vulnerability:
Exploits and Remediation Strategies


## Executive Summary

A Wi-Fi Protected Access version 2 (WPA2), with AES encryption and 802.1x based authentication, is considered the most secure configuration for Wi-Fi networks, and recommended as the "go-to" Wi-Fi security protocol by the Wi-Fi Alliance. Naturally, more organizations are relying on WPA2 to protect their enterprise Wi-Fi networks. WPA2 is also being increasingly adopted to secure guest Wi-Fi networks as well as Wi-Fi Hotspots and municipal Wi-Fi networks that were traditionally implemented over Open Wi-Fi.

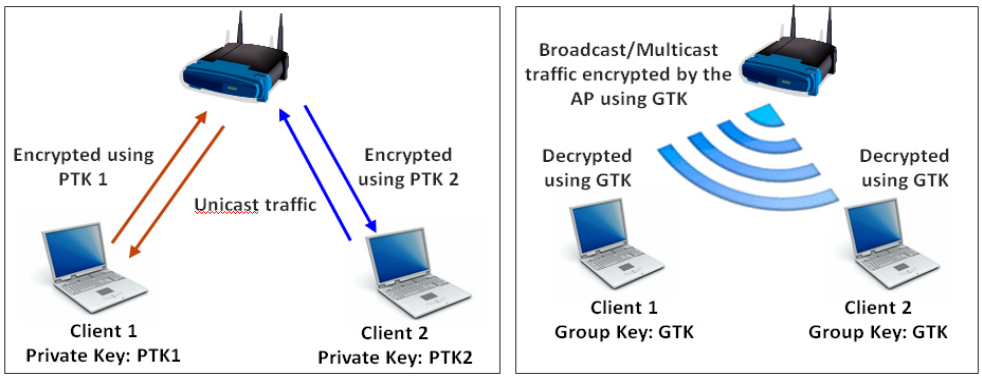
This paper presents a vulnerability, called *Hole196*[1], in the WPA2 protocol that makes all implementations of WPA- and WPA2-secured Wi-Fi networks (regardless of the authentication and encryption used) vulnerable to insider attacks. It discusses ways in which a malicious insider can exploit Hole196 to attack other authorized Wi-Fi users in a WPA2-secured wireless LAN (WLAN). It also explores remediation strategies at various levels that organizations can implement to mitigate this threat.

[1] The moniker 'Hole196' refers to the page number in the IEEE 802.11 Standard (Revision, 2007) where the vulnerability is buried.

## Background

In the WPA2 protocol standard two types of keys are used for data encryption: the Pairwise Transient Key (PTK) and the Group Temporal Key (GTK). Each client associated to a WPA2-secured access point (AP) receives a unique PTK that is used for securing over-the-air unicast data traffic between that client and the AP. A GTK, however, is shared by all clients associated with the AP; the GTK is used to secure over-the-air broadcast or multicast data traffic sent by the AP.

In other words, a PTK is a "two-way" private key and can be used by a client or the AP to encrypt and decrypt unicast data traffic. While the GTK is a "one-way" shared key that is to be used only by the AP for encrypting broadcast or multicast traffic and that is to be used by clients only for decrypting the broadcast or multicast traffic they receive from the AP.



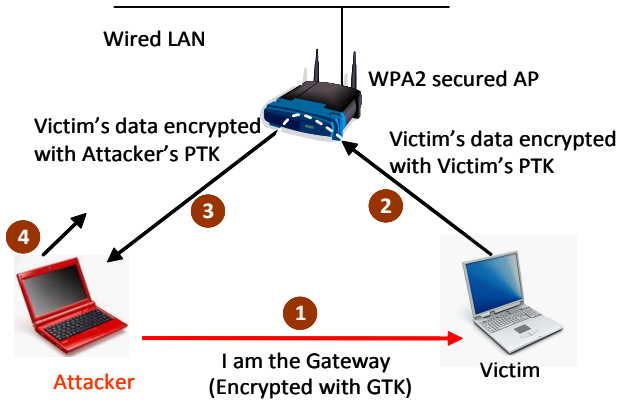

## Hole196 Vulnerability in WPA2

The GTK can be misused by a malicious insider (authorized user) in a WPA2 network. For instance, an insider can spoof the MAC address of the AP and inject a GTK-encrypted packet with broadcast destination address. An insider can leverage such spoofed GTK-encrypted packets to launch several attacks such as ARP Poisoning (Man-in-the-Middle).

In the ARP Poisoning attack based on Hole196, the malicious insider uses the GTK-encrypted packets to advertise itself as the gateway to other authorized Wi-Fi clients, in turn tricking them into redirecting their data to the insider via the AP. The authorized clients that receive the spoofed GTK packet, send their data traffic, encrypted using their respective PTKs, to the AP. The AP then forwards that data, encrypted with the insider's PTK, to the insider's machine where the data can now be decrypted. Thus, the insider is able to bypass inter-user data privacy and see private data traffic from other authorized Wi-Fi users in the network.

Note this attack is neither a brute force attack on the authentication nor does it involve cracking the private keys (PTKs) of other users in the network. In fact, the attacker does

not require the PTKs of other users because the AP is tricked into doing all the work — decrypting the data from victim clients and then forwarding the data to the attacker by encrypting it in the attacker's PTK!

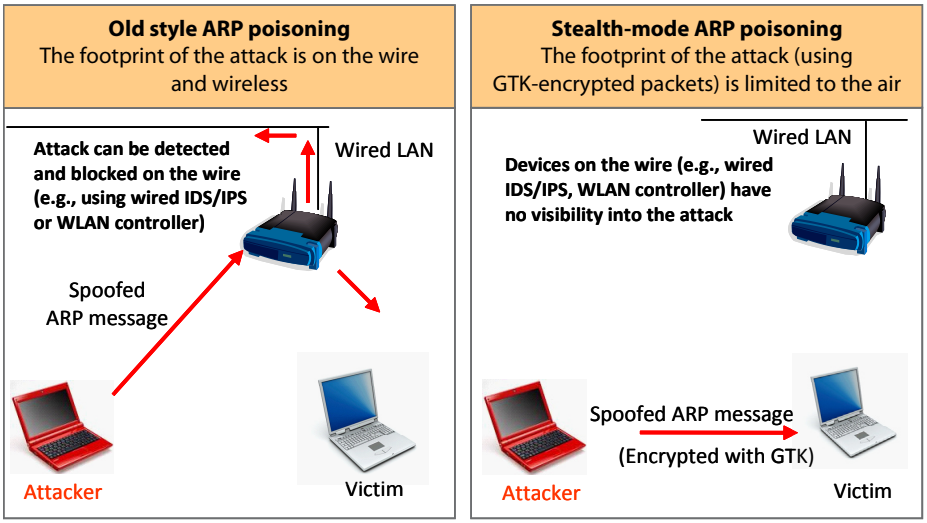



1. Attacker broadcasts a fake ARP message to poison the ARP table of other Wi-Fi clients in the WPA2 network, mapping the IP address of the actual gateway to the MAC address of the attacker's device.
2. Victim sends all its PTK-encrypted traffic data traffic to the AP with the Attacker's device MAC address as the destination (gateway)
3. AP forwards Victim's data to the Attacker encrypting it in the Attacker's PTK. Using his own PTK, the Attacker can decrypt private data from the Victim.
4. The Attacker then forwards the data traffic to the actual gateway so that the attack is transparent to the Victim who continues the communication as normal.

**The same old ARP poisoning! So what's new?**

ARP poisoning is a classic attack that could be already launched on the Ethernet or even through a WPA2-secured AP. However, in this old way of launching the attack, the AP forwards the spoofed ARP messages on the wireless as well as the wired network. The messages that go on the wire are in the clear (unencrypted). Wired network security has evolved over the years to the point that wired IDS/IPS and even network switches can readily catch and block this attack on the wire today.

But launching an ARP poisoning attack using spoofed GTK-encrypted frames limits the footprint of the attack only to the air and the payload is encrypted. So no wire-side security solution is ever going to catch this attack over WPA2, nor will existing APs see anything abnormal. So unless a wireless intrusion prevention system (WIPS) is in place that scans the airspace and detects the anomalous behavior exhibited by the attacker over the air, this attack cannot be detected.



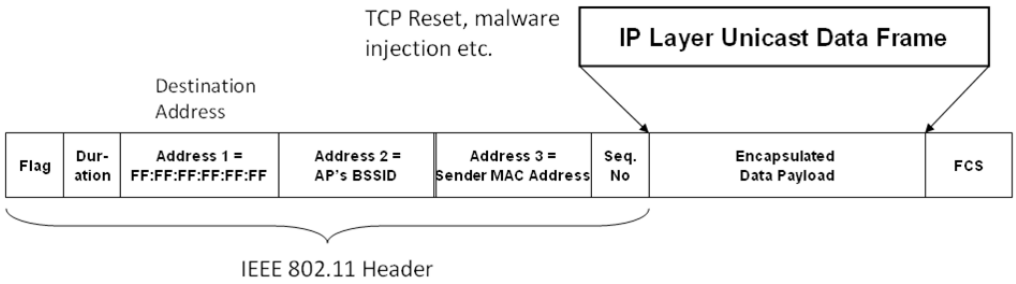

In short, the WPA2 GTK vulnerability enables a malicious insider to launch classic attacks like ARP poisoning, while staying hidden, making it among the stealthiest insider threats. And given the sophisticated hacking tools (e.g., SSLStrip) that are freely available and can be used on top of this exploit, this is a significant risk for security sensitive organizations (e.g., government, finance, and retail) that have to protect national security and cardholder data from insider threats and espionage.

### Denial of Service (DoS)

A malicious insider can misuse the replay protection framework in WPA2 to launch a DoS attack on other authorized Wi-Fi devices in a WPA2 network. For instance, the attacker could broadcast a GTK-encrypted packet with a packet number (PN) much higher than the current PN counter for GTK messages. All clients receiving that message will update their PN counter to the large number advertised by the attacker. After that, all legitimate broadcast messages coming from the AP will be dropped by the victimized clients resulting in a denial of service. Applications that rely on broadcast and multicast messages (e.g., ARP updates) will stop working.

### Higher layer exploits

A malicious insider could choose to include other malicious payloads inside the spoofed GTK-encrypted packets. For instance, a malicious insider could launch a targeted IP layer attack by including a payload with the IP address of a specific target Wi-Fi user device in the WPA2 network. Other Wi-Fi devices would drop this packet at the IP level. Using this technique, several TCP/UDP and application layer exploits are possible, e.g., TCP reset, TCP indirection, DNS manipulation, port scanning, malware injection, privilege escalation, etc.




**IP packet encapsulated into a group addressed IEEE 802.11 data frame**

## Remediation Strategies

### Client isolation

Many WLAN controllers and APs have a "client isolation" feature (also known as PSPF). Using this data communication between two Wi-Fi clients associated to the same AP (or APs controlled by the same controller) can be disabled. While an insider could still send out spoofed GTK-encrypted broadcast packets directly to other clients in the network, he will no longer be able to receive data traffic from a victim if both are associated to the same AP or to APs controlled by the same WLAN controller.

But, client isolation is a "first aid" solution and should not be relied on as the ultimate solution because a variant of the ARP poisoning and man-in-the-middle attack can bypass client isolation. For instance, the attacker could poison the victim such that the data traffic from the victim is redirected to a fake gateway over the wire (by using the Ethernet MAC address of the Attacker's Wi-Fi laptop that is also plugged into the Ethernet LAN or by using a separate machine on the wired network). Further, other attacks (e.g., DoS, malware injection) can be launched using just Step 1 (injecting spoofed GTK-encrypted broadcast packets), which will bypass client isolation.

Note that client isolation is a proprietary feature and the implementation is likely to vary among WLAN vendors. Further, it may not always be practical to use client isolation, for instance, if certain enterprise applications running over Wi-Fi (e.g., VoIP over WiFi) require Wi-Fi clients to communicate with one another via the AP.

### Fix in the WLAN infrastructure

The WLAN AP vendors can circumvent the Hole196 vulnerability by stopping the use of a shared group key (GTK). In most controller-based WLAN architectures today, the APs do not transmit broadcast traffic over the air and instead the WLAN controller maintains an ARP table. In other words, the GTK does not get used. However, according to current WPA2 protocol standard, a GTK needs to be assigned by the AP to each client during the association (four-way handshake) process. AP vendors can implement a patch to their AP software to assign a unique, randomly generated GTK to each client instead of sharing the same GTK among all clients. Using unique GTKs will neutralize the Hole196 vulnerability.

WPA2 Hole196 Vulnerability:
Exploits and Remediation Strategies

**About AirTight Networks**

**AirTight Networks is the global leader in wireless security and compliance solutions providing customers best-of-breed technology to automatically detect, classify, locate and block all current and emerging wireless threats. AirTight offers both the industry's leading wireless intrusion prevention system (WIPS) and the world's first wireless vulnerability management (WVM) security-as-a-service (SaaS). AirTight's award-winning solutions are used by customers globally in the financial, government, retail, manufacturing, transportation, education, health care, telecom, and technology industries. AirTight owns the seminal patents for wireless intrusion prevention technology with 18 U.S. patents granted or allowed, two international patents granted (UK and Australia), and more than 20 additional patents pending. AirTight Networks is a privately held company based in Mountain View, CA. For more information please visit www.airtightnetworks.com**



And there will be no cost associated with this change in terms of reduced data throughput, unless broadcast traffic is sent by the AP over the air using unique GTKs.

In the long term, this approach of deprecating the use of a shared GTK can also be adopted in the IEEE 802.11 standard.

### WIPS as an additional layer of defense

A wireless intrusion prevention system (WIPS) provides a protective layer of defense and a faster path for managing emerging threats and vulnerabilities until appropriate fixes are implemented in the infrastructure. AirTight® Networks' SpectraGuard® Enterprise WIPS has successfully protected organizations against Wi-Fi vulnerabilities (such as WEP cracking, WPA-TKIP vulnerability, and Cisco Skyjacking) in the past, and the Hole 196 vulnerability is no exception.

AirTight's SpectraGuard Enterprise WIPS is built on top of basic building blocks such as MAC spoofing detection, packet-based anomaly detection, and device behavioral analysis that have in the past provided security frameworks, including WEPGuard™, WPAGuard™ and VLAN Policy Mapping™ to protect organizations from vulnerabilities in Wi-Fi security protocols. A combination of the same building blocks can detect and locate attacks based on WPA2-Hole196 vulnerability and close the window of exposure until a WPA2 protocol fix is provided in the standard or in the interim, by WLAN infrastructure vendors.

## Concluding Remarks

The 'Hole196' vulnerability exposes all WPA and WPA2 networks, regardless of the authentication (e.g., 802.1x, PSK, dynamic PSK) and encryption (e.g., TKIP, AES), to insider attacks. A malicious insider can exploit 'Hole196' to bypass inter-user data privacy in WPA and WPA2 and decrypt data traffic from other authorized Wi-Fi clients in the network. A variety of classic attacks such as ARP poisoning, man in the middle, denial of service, malware injection, etc., can be launched.

Enterprises can consider using remediation strategies based on client isolation and endpoint security software, but the effectiveness of these solutions is limited. WLAN infrastructure vendors can provide a proprietary solution by means of a software patch or upgrade to their AP software so that APs provide unique GTKs to its associated clients. This will neutralize the 'Hole196' vulnerability without breaking the interoperability with Wi-Fi clients.

While the vulnerability gets fixed, a wireless intrusion prevention system (WIPS) such as SpectraGuard Enterprise can provide an additional layer of defense for protecting enterprise networks 24/7 not only from exploits based on Hole196, but also from other wireless threats such as Rogue APs, soft APs, mis-configurations, and Wi-Fi client misbehavior.



**AirTight Networks, Inc.** 339 N. Bernardo Avenue #200, Mountain View, CA 94043
T +1.877.424.7844 T 650.961.1111 F 650.961.1169 **www.airtightnetworks.com info@airtightnetworks.com**



AirTight® NETWORKS