

WPA 2 Hole196 Vulnerability – FAQ

What is the “Hole196” vulnerability?

“Hole196” is a vulnerability in the WPA2 security protocol exposing WPA2-secured Wi-Fi networks to insider attacks. AirTight Networks uncovered a weakness in the WPA2 protocol, which was documented but buried on the last line on page 196 of the 1232-page IEEE 802.11 Standard (Revision, 2007). Thus, the moniker “Hole196.”

Central to this vulnerability is the group temporal key (GTK) that is shared among all authorized clients in a WPA2 network. In the standard behavior, only an AP is supposed to transmit group-addressed data traffic encrypted using the GTK and clients are supposed to decrypt that traffic using the GTK. However, nothing in the standard stops a malicious authorized client from injecting spoofed GTK-encrypted packets! Exploiting the vulnerability, an insider (authorized user) can sniff and decrypt data from other authorized users as well as scan their Wi-Fi devices for vulnerabilities, install malware and possibly compromise those devices.

In short, this vulnerability means that inter-user data privacy among authorized users is inherently absent over the air in a WPA2-secured network.

Can this vulnerability be exploited only by insiders, or can an outsider also hack into a WPA2 network using Hole196?

To exploit Hole196, a malicious user needs to know the group key (GTK) shared by the authorized users in that Wi-Fi network. So only an insider (authorized user) of a WPA2 network, having access to the GTK can exploit this vulnerability.

If Hole196 can be exploited only by insiders, should we really worry about it?

Extensive survey reports consistently show that insider attacks are the most common and costliest threat to enterprise data and network security. For instance, refer to the following two reports:

[2010 CyberSecurity Watch Survey by CERT, CSO and Deloitte](#)

[2010 Verizon Data Breach Investigation Report](#)

If your organization is sensitive about insider threats and you are already taking steps to mitigate insider attacks on the wired network, then the Hole196 vulnerability is significant as it enables one of the stealthiest insiders attacks known that can lead to leakage of sensitive data (e.g., intellectual property, trade secrets, financial information), espionage, unauthorized access to IT resources, identity theft, etc.

Does Hole196 enable or involve cracking of the WPA2 encryption key?

No! Exploiting the Hole196 vulnerability does not involve cracking of the encryption key. This is neither an attack on the AES encryption or the 802.1x (or PSK) authentication.

Does the malicious insider gain access to the private keys, i.e., the pairwise transient key (PTKs) of other authorized users in the WPA2 network?

No! The malicious insider does not gain access to the private keys (PTKs) of other authorized Wi-Fi users in the WPA2 network.

Then in what way can an insider exploit the Hole196 vulnerability?

Our findings show that an insider could exploit Hole196 in three ways: (1) for ARP poisoning and man-in-the-middle attack; (2) for injecting malicious code onto other authorized Wi-Fi devices; and (3) for launching a denial-of-service (DoS) attack without using disconnection frames.

In a WPA2 network, a malicious insider broadcasts fake packets (with the AP's MAC address as the transmitter's address) encrypted using the shared group key (GTK) directly to other authorized Wi-Fi clients in the network. One example of an exploit that can be launched using GTK is the classic ARP poisoning (man-in-the-middle) attack (demonstrated at Black Hat Arsenal 2010 and Defcon18).

In the ARP poisoning exploit, the insider can include for instance an ARP Request message inside the GTK-encrypted packet. The ARP Request has the IP address of the actual gateway, but the MAC address of the attacker's machine. All clients that receive this message will update their ARP table – mapping the attacker's MAC address with the gateway's IP address.

All "poisoned" Wi-Fi clients will send all their traffic, encrypted with their respective private keys (PTKs), to the AP, but with the attacker's MAC address as the destination. The AP will decrypt the traffic and forward it to the attacker, now encrypting it using the attacker's PTK. Because all traffic reaching the attacker (from the AP) is encrypted with the attacker's PTK, the attacker can decrypt the traffic (including login credentials, emails and other sensitive data).

The attacker can then choose to forward the traffic to the actual gateway of the network, so that the victim Wi-Fi clients do not see any abnormal behavior and continue their communication.

But ARP spoofing (and man-in-the middle) was always possible over Ethernet or even in a WPA2 network via the AP. So what's new?

ARP Spoofing (and man-in-the-middle) is a classic attack in both wired and Wi-Fi networks. 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 some network switches can readily catch and block this attack on the wire today. The subtle point (that many people seem to miss) about exploiting the GTK in WPA2 for

launching an ARP Spoofing attack is that the footprint of the attack is only in 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.

And note that ARP spoofing is just one example of an exploit over this vulnerability. More sophisticated attacks are possible.

Can this vulnerability be practically exploited?

Unlike the WPA-TKIP vulnerability (announced in November 2008) that was largely of theoretical interest, the Hole196 vulnerability can be practically exploited using existing open source software such as madwifi driver and wpa supplicant, and adding ten lines of code. The man-in-the-middle attack using ARP spoofing was demonstrated at Black Hat Arsenal 2010 and Defcon18. Other attacks such as port scanning, exploiting OS and application vulnerabilities, malware injection, DNS manipulation, denial of service, etc. are possible by misusing GTK.

Are all WPA and WPA2 implementations vulnerable to this attack?

Yes! Hole196 is a fundamental vulnerability in the protocol design. All Wi-Fi networks using WPA or WPA2, regardless of the authentication (PSK or 802.1x) and encryption (AES) they use, are vulnerable.

Are WLAN architectures using stand-alone APs and those using WLAN controllers vulnerable to Hole196?

This vulnerability is fundamental to the WPA/WPA2 protocol design. So as long as a WLAN architecture (stand-alone AP or controller based) is following the standard, it is vulnerable to Hole196.

Is there a fix in the 802.11 protocol standard which I can implement with a software upgrade to protect against this vulnerability?

Unlike in the case of earlier vulnerabilities in Wi-Fi encryption and authentication protocols, there is no immediate fallback in the 802.11 standard that can be used to fix or circumvent this vulnerability.

Can I use the client isolation (or PSPF) feature on my WLAN infrastructure to protect against WPA2 Hole196?

Client isolation is not part of the 802.11 standard, but a proprietary feature that is available on some APs and WLAN controllers. The implementation of the feature is likely to vary from vendor to vendor. Turning ON the

Client isolation (or PSPF) feature on an AP or WLAN controller can prevent two Wi-Fi clients associated with an AP from communicating with each other via the AP. This means that while a malicious insider can continue to send spoofed GTK encrypted packets directly to other clients in the network, the data traffic from the victim clients will not be forwarded by the AP to the attacker's Wi-Fi device.

However, an attacker can bypass the Wi-Fi client isolation feature, by setting up a fake gateway on the wired network, poison the ARP cache on authorized Wi-Fi devices using GTK and redirect all data traffic to the fake gateway instead of redirecting it directly to his Wi-Fi device. Plus, other attacks such as malware injection, port scanning, denial of service, etc. are still possible using only the first step (sending GTK-encrypted packets)

Is there something I can install on my laptop to protect it against WPA2 Hole196?

Software (such as Snort or DecaffeintID) can be installed on some Windows and Linux laptops to detect ARP poisoning, though it's not practical to manually install software on large number of endpoints. Further, the software is not supported on most endpoints (e.g., iPhones, iPads, Blackberry, Windows Mobile, Windows 7, etc.) that will continue to be at risk from the WPA 2 Hole196 vulnerability. Besides, those softwares cannot stop a malicious insider from launching other Hole196 based attacks such as malware injection, port scanning, denial of service, etc.

Can a wire-side solution like an IDS/IPS or ARP Poisoning detector on the LAN switch detect this attack?

The footprint of WPA2 Hole196 based insider attacks is limited to the air, making them among the stealthiest of insider attacks known. As a result, no wireline security solution (wired IDS/IPS, firewall, or switch-based ARP Poisoning detection) can detect these attacks.

Can a wireless intrusion prevention system (WIPS) detect this attack?

Hole196 is yet another example of a wireless vulnerability that calls for a multi-layered wireless security approach. A wireless intrusion prevention system (WIPS) can detect attacks based on Hole196 and provide that additional layer of security to comprehensively protect enterprise networks from wireless threats such as rogue APs, misbehavior of Wi-Fi clients, misconfigurations in your WLAN infrastructure, and vulnerabilities in the Wi-Fi security protocols.

Can WLAN AP vendors design a proprietary fix to the vulnerability while maintaining interoperability?

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, it is possible to turn OFF broadcast traffic transmission from the APs over the air and instead use the WLAN controller as the ARP proxy. In other words, in this configuration, the GTK does not get used. But 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 and still allow interoperability (backward compatibility) with all standard Wi-Fi client devices. And there will be minimal cost associated with this change in terms of reduced data throughput.

In absence of an ARP proxy, an AP could send broadcast traffic over the air as unicast to individual clients, though this will potentially result in degradation in the WLAN data throughput depending on the amount of broadcast traffic.

In the long term, this approach of deprecating the use of a shared GTK could be adopted in the IEEE 802.11 standard and only PTK could be used.