TECHNICAL BRIEF

Understanding the WPA2 “Hole196” Attack

Vulnerabilities & Motorola WLAN Countermeasures

Executive Summary

On July 22, 2010, AirTight Networks disclosed a new attack, labeled "Hole196", which revealed a vulnerability in the WPA & WPA2 protocol used by enterprises to secure Wi-Fi networks. While the practical exposure from the attack is limited, it does lead to the possibility of an insider man-in-the-middle vulnerability which cannot be detected from the wired network. This paper provides an overview of the vulnerabilities introduced by the attack, as well as the countermeasures available through the Motorola Wireless LAN solution to mitigate the new threat.

Attack Details

Wi-Fi protected access (WPA and WPA2) and the IEEE 802.11i standard defined a wireless security protocol in response to several serious weaknesses discovered in the previous generation of Wi-Fi encryption, wired equivalent privacy (WEP). The goal of these new protocols is to address the weakness of WEP and offer wireless traffic the same level of security as if it had been sent over a secure wired network. WPA and WPA2 operate in two modes: Personal, which utilizes a pre-shared key (PSK), and Enterprise which takes advantage of an IEEE 802.1x authentication server. Both modes of WPA or WPA2 are vulnerable to the "Hole196" attack — even the most secure 802.1x authenticated and AES encrypted networks. However, execution of this attack does require the user be successfully authenticated to the network and has been termed an insider attack.

As a client connects to a WPA or WPA2 network, two sets of temporal keys are generated, which are used to encrypt individual frames on the wireless network. The pairwise transient keys (PTK) for unicast traffic are unique to each connection and groupwise transient keys (GTK) for broadcast/multicast traffic, which are shared amongst all the devices on the network. Using the shared GTK the attacker can send spoofed broadcast or multicast packets directly to other wireless clients on the network. The benefit of this approach for the attacker is circumventing passing the traffic over the wired network where other systems and protection mechanisms may detect that an attack has occurred. The most common application of this attack is to perform address resolution protocol (ARP) spoofing in which the malicious user masquerades as the default router for all traffic on the wireless network. The victim machine then forwards all traffic intended for the access point to the malicious insider creating a man-in-the-middle attack. Another possible attack is wireless denial of service (DoS). The attacker sends a malicious broadcast frame with a high packet number, causing victim clients to ignore legitimate frames with packet numbers less than the number set by the malicious frame.

Summary of Vulnerabilities

1. This is not a key recovery attack. No keys are compromised and it does not lead to decryption of all subsequent frames.
2. This does not allow an attacker to decrypt any unicast wireless traffic transmitted by any other device on the network.
3. The attack affects all WPA and WPA2 deployments, regardless of whether they use pre-shared keys (PSK) or the more robust enterprise mode with IEEE 802.1x authentication.
4. The attacker must have access to the network to exploit the vulnerability.
5. This is an "over the air" exploit, not visible from the wired side of the network.
6. The most common attack scenario is man-in-the-middle attack through ARP spoofing.
7. Wireless DoS is also possible, causing victim clients to ignore legitimate broadcast/multicast frames.

Motorola WLAN Countermeasures

The Motorola WLAN solution includes several countermeasures already built into the product to mitigate the new "Hole196" attack. Motorola recommends that enterprises continue to use AES-CCMP encryption with their WPA or WPA2 deployments to secure wireless access. As all WPA and WPA2 deployments are vulnerable to this insider attack Motorola recommends organizations follow these additional safeguards to prevent or minimize the impact of the attack:

Client Isolation

Client isolation is a feature on Motorola WLAN infrastructure, preventing a wireless client from directly communicating with another peer. Enabling client isolation would prevent the execution of the man-in-the-middle attack by blocking all communication between the victim and attacker clients. The Motorola infrastructure implements this feature as "Disable MU-to-MU Communication" or allow "Client-to-Client Communication".

Note that client isolation will have limited effectiveness when implemented in independent wireless AP deployments as communication would not be prevented between two wireless clients associated to two different APs.

Wireless Firewall

Motorola implements the industry's only true wireless firewall which can lock down and limit the effectiveness of this attack at the edge of the network. The wireless firewall allows rules to be created and assigned to filter traffic as it enters and exits the WLAN, preventing malicious activity from reaching the core. In any deployment, wireless firewall best practices dictate that wireless to wireless device communication be limited to only what is absolutely necessary, limiting the scope of man-in the-middle exploits that leverage anomalous client-to-client traffic. The specific configuration of these rules would depend on the wireless applications running on the WLAN. However, they would typically include both an inbound rule set and outbound rule set assigned to each WLAN. In cases where no access is needed to the local Layer 3 segment, Layer 2 rules can be applied to explicitly limit communication with the default gateway, preventing ARP based man-in-the-middle exploits described above.

Motorola AirDefense Wireless Intrusion Prevention

The Motorola WLAN solution features the industry-leading AirDefense Wireless Intrusion Prevention System (IPS). Motorola AirDefense wireless IPS capabilities also help contain the attack. The wireless IPS is capable of detecting MAC address spoofing that occurs when the adversary pretends to be an authorized AP during the attack. The AirDefense wireless IPS can also detect excessive wireless-to- wireless traffic and alert on those traffic patterns which manifest during the man-in-the-middle attack. The wireless IPS can generate an alarm, send SNMP traps to notify various security event management systems, alert an administrator via email/pager, etc. In addition, leveraging the integration between Motorola AirDefense and Motorola WLAN, the offending device can be blacklisted, and all further frames from it are ignored for the blacklist timeout period.

MOTOROLA

motorola.com/airdefense

Part number TB-WPA2Hole196. Printed in USA 08/10.