

Overview

The following note covers information published in the PCI-DSS Wireless Guideline in July of 2009 by the PCI Wireless Special Interest Group Implementation Team and addresses version 1.2 of the PCI standard.

A full copy of the PCI Wireless Guideline can be found at the PCI Security Standards website at:

https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf

Summary of Key Findings

- **All organizations will need to meet basic standards of wireless auditing in order to meet PCI compliance even if they do not have wireless networks deployed.**
 - This includes the ability to detect rogue APs and Stations in all locations.
 - Must identify both Rogue APs and well as Rogue Clients
 - Specifically advises AGAINST using wired-side or SNMP-based monitoring solutions for rogue device detection, citing their high rate of false negatives and false positives and inability to detect rogue stations.
 - Wireless IDS/IPS systems are recommended for organizations with several locations where it would be impractical to regularly scan using mobile wireless analyzers.

- **The Wireless LAN is considered to be inside the Cardholder Data Environment (CDE) if any wireless traffic touches a network component that stores, processes or transmits card-holder data. The WLAN can easily be in the CDE even if the WLAN itself does not carry cardholder information.**

- **Recommendations for Wireless LANs that are in the CDE:**
 - Use a wireless monitoring system to track and locate all wireless devices.
 - If SNMP is not required on the network, the organization should disable SNMP altogether.
 - Use a centrally controlled wireless IDS/IPS to monitor for unauthorized access and detect rogues and misconfigured wireless devices.
 - Enable IPS features that automatically disable rogue wireless devices connecting to the CDE as well as accidental or malicious associations of wireless clients.
 - Coordinate logging events with other networking devices within the organization.
 - Maintain a current topology of all physical locations of access points.

Important Quotes

Who must comply with the standard?

“These are requirements that all organizations should have in place to protect their networks from attacks via rogue or unknown wireless access points (APs) and clients. They apply to organizations regardless of their use of wireless technology and regardless of whether the wireless technology is a part of the CDE or not. As a result, they are generally applicable to organizations that wish to comply with PCI DSS. ”

“Even if an organization that must comply with PCI DSS does not use wireless networking at all, the organization must verify that wireless networking has not been introduced into the CDE over time. Therefore, this CDE is in scope for PCI DSS and this guide, in that the organization must verify and continue to ensure that there are no WLANs attached to the network.”

Rogue Devices

“A rogue Access Point (AP) is any device that adds an unauthorized (and therefore unmanaged and unsecured) WLAN to the organization’s network. A rogue AP could be added by inserting a WLAN card into a back office server (C), attaching an unknown WLAN router to the network (F), or by various other means.”

“Ensure that the organization maintains an up-to-date hardware inventory so that known APs can easily be distinguished from rogue APs.”

“Wireless Scanning to Look for Rogue Access Points

PCI DSS requirement 11.1 clearly specifies the use of a wireless analyzer or a wireless IDS/IPS system for scanning. Relying on wired side scanning tools (e.g. tools that scan suspicious hardware MAC addresses on switches) may identify some unauthorized wireless devices; however, they tend to have high false positive/negative detection rates. Wired network scanning tools that scan for wireless devices often miss cleverly hidden and disguised rogue wireless devices or devices that are connected to isolated network segments. Wired scanning also fails to detect many instances of rogue wireless clients. A rogue wireless client is any device that has a wireless interface that is not intended to be present in the environment.”

*“The goal of all of these devices is to “sniff” the airwaves and “listen” for **wireless** devices in the area and identify them. Using this method, a technician or auditor can walk around each site and detect **wireless** devices. The person would then manually investigate each device to determine if it allows access to CDE and classify them as rogues or just friendly neighboring **wireless** devices. Although this method is technically possible for a small number of locations, it is often operationally tedious, error-prone, and costly for organizations that have several CDE locations. For large organizations, it is*

recommended that **wireless** scanning be automated with a **wireless** IDS/IPS system.”

3.2.1 Summary of recommendations:

A. Use a wireless analyzer or a wireless IDS/IPS to detect unauthorized/rogue wireless devices that could be connected to the CDE at least quarterly at all locations. For large organizations

having several CDE locations, a centrally managed wireless IDS/IPS to detect and contain unauthorized/rogue wireless devices is recommended.

B. Enable automatic alerts and containment mechanisms on the wireless IPS to eliminate rogues and unauthorized wireless connections into the CDE.

C. Create an “Incident Response Plan” to physically eliminate rogue devices immediately from the CDE in accordance with PCI DSS requirement 12.9.5.

Defining WLANs as in or out of the CDE

“In the case where an organization has decided to deploy a WLAN for any purpose whatsoever, and connect the WLAN to the CDE, then that WLAN is now a part of the CDE and is therefore in scope within the **PCI DSS** and within the scope of this document. In this case, the WLAN Access Point (AP) is connected directly to the wired network within the CDE. Even though the organization is only using WLAN technology for inventory control, and no cardholder data is being passed back and forth, the WLAN is nevertheless within the CDE by the fact that the network traffic is **not segmented** away.”

“In the case where a WLAN is added outside of the CDE, so that no traffic whatsoever from the WLAN passes into the CDE, then that WLAN can be considered out of scope for the **PCI DSS**.”

To Separate a WLAN from a CDE

3.3.1 Summary of recommendations:

A. Use a stateful packet inspection firewall to block wireless traffic from entering the CDE.

Augment the firewall with a wireless IDS/IPS.

B. Do not use VLAN based segmentation with MAC address filters for segmenting wireless networks.

C. Monitor firewall logs daily and verify firewall rules at least once every six months.

Physical Security

A. Mount APs on ceilings and walls that do not allow easy physical access.

B. Use APs with chassis and mounting options that prevent physical access to ports and reset features. APs housed in tamper-proof chassis are recommended.

C. Secure handheld devices with strong passwords and always encrypt PSKs if cached locally.

D. Use a **wireless** monitoring system that can track and locate all **wireless** devices and report if one or more devices are missing.

Changing Default Settings on APs

"If SNMP is not required on the network, the organization should simply disable SNMP altogether."

4.2.1 Summary of recommendations:

- A. Enable WPA or WPA2 and make sure that default PSKs are changed. Enterprise mode is recommended.
- B. Disable SNMP access to remote APs if possible. If not, change default SNMP passwords and use SNMPv3 with authentication and privacy enabled.
- C. Do not advertise organization names in the SSID broadcast.
- D. Synchronize the APs' clocks to be the same as other networking equipment used by the organization.
- E. Disable all unnecessary applications, ports, and protocols.

Wireless Intrusion Prevention and Access Logging

Wireless IDS/IPS provides several types of security capabilities intended to detect

misconfiguration, misuse, and malicious activity. These capabilities can be grouped into three categories: (i) rogue **wireless** device containment, (ii) detection of unsafe activity or configurations, (iii) detection of denial of service attacks, and **wireless** intrusion attempts.

Unauthorized **wireless** devices connected to the CDE must be detected and disabled. A **wireless**

IPS should be able to find these rogue devices even when they are configured to not broadcast information about themselves or present in isolated network segments. In addition to rogue containment, organizations should evaluate the automatic device classification capabilities of the **wireless** IDS/IPS for situations when connectivity cannot be determined. A **wireless** IDS/IPS should be able to observe all APs and clients, on all operational channels, and classify each device as authorized, unauthorized/rogue or neighboring. Many **wireless** IPS systems provide the ability to prevent clients from associating with an unauthorized AP or disable an ad hoc network; efficacy of these techniques vary widely and can provide adequate temporary mitigation of the risk. However, unauthorized devices should be physically and/or logically removed from the CDE as soon as possible.

A **wireless** IDS/IPS can detect misconfigurations and unsafe activity by monitoring and analyzing **wireless** communications. Most can identify APs and clients that are not using the proper security controls. This includes detecting misconfigurations and the use of weak WLAN protocols. This is accomplished by identifying deviations from organization-specific policies for configuration settings such as encryption, authentication, data rates, SSID names, and channels. For example, they could detect that a **wireless** device is using WEP instead of WPA2. Some **wireless** IDS/IPS use anomaly and/or behavior based detection methods to detect unusual WLAN usage patterns. For example, if there is a higher than usual amount of network traffic between a **wireless** client and an AP, one of the devices might have been compromised, or unauthorized parties might be using the WLAN. Some

systems can also alert if any WLAN activity is detected during off-hours periods.

A **wireless** IDS/IPS can analyze **wireless** traffic to look for malicious activity such as Denial of

Service (DoS) and individual attacks on devices. This task, as in wired IDS/IPS, requires the system to look for attempts to disrupt the **wireless** network, a device on the network, or to gain unauthorized access to the network. If these detections are signature-based, then organizations should ensure the signatures are updated when new threats are discovered.

Most **wireless** IDS/IPSs can identify the physical location of a detected threat by using signal strength triangulation. Triangulation is the process of estimating the threat's approximate distance from multiple sensors by the strength of the threat's signal received by each sensor, then calculating the physical location at which the threat would be located to satisfy the distance criteria from each sensor. This allows an organization to send physical security staff to the location to address the threat.

An IDS/IPS system can generate a lot of **wireless** threat information. In order for the organization to be able to use this information, the information has to be properly logged. This implies that the logs from the IDS/IPS have to be coordinated with other logging systems on the network (if there are any). In this case, the organization must ensure that at least the following logging items are coordinated correctly:

- A. The log file prefix (used to identify the device conducting the logging).
- B. The level of logging (the types of events to log).
- C. The log auto-roll setting (whether a new log file is created when the device is restarted, or the maximum log size is reached).
- D. The log maximum (log age in days).

After gathering the information within the IDS/IPS, the organization must **read and respond to the IDS/IPS reports**. If there are anomalies, they must be resolved. It is not enough to merely purchase and properly configure the IDS/IPS. This is a device doing the legwork of watching out for potential problems. However, what it can't do is stop a potential cardholder data breach without personnel interaction. The organization's policies and procedures must take into account the reading and taking action on the logs provided by this and other key monitoring devices.

4.3.1 Summary of recommendations:

- A. Use a centrally controlled **wireless** IDS/IPS to monitor for unauthorized access and detect rogues and misconfigured wireless devices.
- B. Enable historical logging of wireless access that can provide granular wireless device information and store event logs and statistics for at least 90 days.
- C. Enable IPS features that automatically disable rogue wireless devices connecting to the CDE as well as accidental or malicious associations of wireless clients.
- D. Ensure the IPS signature set is regularly updated as new threats are discovered.
- E. Coordinate logging events with other networking devices within the organization.
- F. Add processes and policies that will regularly read and act on the data provided by the IDS/IPS.
- G. Maintain a current topology of all physical locations of access points.

Strong Authentication and Encryption

Recent attacks against the TKIP encryption algorithm have revealed some flaws in the protocol that can allow an attacker to decrypt small frames encrypted using TKIP such as Address Resolution Protocol (ARP) frames in about 15 minutes. Further, the attack revealed that it is possible to reuse the compromised encryption keystream to inject 7-15 arbitrary packets into the network using QoS mechanisms without triggering the replay protection countermeasures available in TKIP. While the attack does not lead to a compromise of the PSK, it is recommended that organizations use AES encryption, which is immune to the attack.

Recommendations

- A. WPA or WPA2 Enterprise mode with 802.1X authentication and AES encryption is recommended for WLAN networks.*
- B. It is recommended that WPA2 Personal mode be used with a minimum 13-character random passphrase and AES encryption.*
- C. Pre-Shared Keys should be changed on a regular basis.*

About AirMagnet

AirMagnet, now part of Fluke Networks, is the leader in security, performance and compliance solutions for wireless LANs. The company's innovative products include AirMagnet Enterprise, the leading 24x7 WLAN security and performance management solution, and AirMagnet WiFi Analyzer – which is known as the "de facto tool for wireless LAN troubleshooting and analysis." Other products provide WLAN site survey and design, RF interference detection, remote diagnostics, and the world's first voice over Wi-Fi analysis solution. AirMagnet has more than 8,500 customers worldwide, including 75 of the Fortune 100.

Corporate Headquarters

830 E. Arques Ave.
Sunnyvale, CA 94085
United States
Tel: +1 408.400.1200
Fax: +1 408.744.1250
www.airmagnet.com