Closing Wireless Loopholes for PCI Compliance and Security

Personal information is under attack by hackers, and credit card information is among the most valuable. While enterprises have had years to develop security countermeasures to protect information on wired networks, wireless networks have created unique opportunities for exploitation. Increasingly, the trend is to capitalize on loopholes in network security through a wireless access point. Merchants who process payment cards need dedicated wireless monitoring systems that offer full traffic analysis and comprehensive security solutions to identify wireless security loopholes, provide solutions, and document compliance for audits.

PCI Guidelines for Wireless Networks

Compromising the cardholder data environment (CDE) through a wireless network has become such a concern that the PCI Data Security Standard (DSS) formed a "PCI Wireless Special Interest Group (SIG) Implementation Team." In July of 2009, this team published the PCI-DSS Wireless Guidelines, a supplement to version 1.2 of the PCI standard. The supplement provides guidance on how the PCI-DSS applies to wireless and communicates methods for merchants to deploy secure wireless LANs.

Frustrating to merchants is that even if an organization does not use wireless networking at all, "the organization must verify that wireless networking has not been introduced to the CDE over time," according to the PCI Wireless Guideline. "The organization must verify and continue to ensure that there are no WLANs attached to the network. This is because there are validation requirements that extend beyond the known wireless devices and require monitoring of unknown and potentially dangerous rogue devices… that can allow access to the CDE."

The guidelines are correct in that rogue devices are dangerous to cardholder data environments. By simply hooking up a wireless router for personal use, employees can unknowingly open up loopholes for hackers to gain access to private information. This paper will look at how to properly detect rogues in order to meet PCI compliance and how to close wireless security loopholes and actively protect the network with multiple layers of defenses, including intrusion detection systems (IDS).

PCI Core Requirements

Seven of core 12 requirements of the PCI-DSS are particular to wireless networks. It is these requirements that the PCI-DSS Wireless Guidelines further clarify and provide guidance to network operators.

Requirement 1:	Maintain a Firewall WIDS/WIPS ensure that devices meet standards set forth in internal and industry security policies track the flow of information, closing loopholes to achieve a standardized level of security.
Requirement 2:	Use Strong Passwords WIDS/WIPS automatically identifies when a device or wireless implementation has security vulnerabilities, such as default passwords, that leave confidential data open to exploitation.
Requirement 4:	Encrypt Transmission of Cardholder Data By June 30, 2010, all networks will be required to remove WEP in favor of WPA 2 or WPA.11i. WIDS/WIPS enables enterprises to validate that devices are using strong encryption components, and quickly identify those that are not.
Requirement 6:	Develop and Maintain Secure Systems and Applications The most effective method of catching weaknesses is through continual, automated monitoring with WIDS/WIPS that not only identifies when a device doesn't meet security policy, but also when a device changes.
Requirement 10:	Track and Monitor All Access The monitoring features within WLAN IDS enable automatic tracking and recording of information in audit logs that are stored in secure, centrally managed databases in compliance with PCI v1.2.
Requirement 11:	Regularly Test Security Systems and Processes Organizations need to perform quarterly scans using wireless analyzers for rogue device discovery, notification of unauthorized access or other security events. WIDS/WIPS systems are recommended for sites with multiple locations.
Requirement 12:	Maintain an Information Security Policy Once a comprehensive wireless policy is developed, violations can be quickly identified using WLAN IDS, automatically escalating issues to the IT or security team for investigation and mitigation, and documenting issues for compliance audits.

AIRMAGNET
now part of Fluke Networks

Rogue APs and Clients in Wireless and "No Wireless" Environments

In order to meet PCI compliance, all organizations need to meet basic standards of wireless auditing to detect rogue APs and rogue clients. Since a rogue device can show up in any location, all locations that store, process or transmit cardholder data must be manually scanned quarterly or have a wireless IDS/IPS implemented to automatically scan and protect the CDE.

Many rogue access points are brought in by employees looking for additional network access and mobility. They simply bring in their personal APs and plug them directly into the corporate LAN without authorization. This is very dangerous, as most users are not aware of all the security issues with their wireless device and that they may have opened up a loophole for an attacker to gain entry into the network. Also, disgruntled employees or attackers can deploy an AP on the network in seconds and connect to it at a later time or from a location over a mile away using a high-gain antenna. Without a combination of wireless and wired tracing, these devices may appear invisible to network managers.

PCI Requirement 11.1 Testing Procedure

- Verify that a wireless analyzer is used at least quarterly, or that a wireless IDS/IPS is implemented and configured to identify all wireless devices.

"We don't have wireless networks at our restaurant locations – it's against policy," said Cameron Pumphrey, the Director of IT at Fuddruckers. Yet Pumphrey and his team discovered that employees were often connecting wireless routers for personal use at chain locations. "We realized we needed to deploy a WLAN IDS that would allow us to see when wireless devices were attached to the wired network," said Pumphrey. "Without it, our customer data could have been at risk and we could have been in violation of PCI compliance."

Insecure WLAN Inside the Cardholder Data Environment

The Wireless LAN is considered to be inside the CDE if any wireless traffic touches any 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. Again, the merchant must ensure audit the traffic to ensure the flow of information is secure.

Vulnerabilities including unauthorized wireless device connections and unapproved AP associations threaten security and compliance. For example, two devices may connect peer-to-peer to share information, bypassing the security infrastructure. Or a wireless client may begin to roam and accidentally (or as part of a malicious attack) connect to a hotspot across the street from the building. Another vulnerability that is common is having default configuration settings on APs such as admin passwords or SNMP remote access enabled.

"As cell phones with wireless Internet access began to flood cell phone retailers in close proximity to our stores, we noticed a huge influx of those types of devices trying to access our wireless network," noted an IT administrator at a retail chain. "That category of user is usually just trying to access any Wi-Fi connection they can see, and often times, they end up trying to get onto our network."

Some organizations separate the WLAN from the CDE by setting up stateful packet inspection firewalls between the wireless network and their wired, trusted core. Although the firewall is used to block wireless traffic from entering the CDE, it leaves wireless transmissions – even those originating behind the corporate firewall – unprotected, with no way to track the flow of information.

Recommendations for Closing Wireless Loopholes

The PCI Wireless SIG Implementation Team recommends that use of mobile wireless analyzers or WIDS/WIPS systems to monitor for rogue APs and clients, factory default passwords, automatic network connection functions and SNMP access – all of which violate wireless security policy and can leave the CDE vulnerable.

The PCI Wireless SIG Implementation Team specifically advises against using wired-side or SNMP-based monitoring solutions for rogue device detection due to their high failure rate and inability to detect rogue clients. Wired discovery methods are not enough to ensure wireless security. APs scan only in approved regulatory channels, leaving the 5 GHz "extended" channels open to hidden rogue devices.

It is further recommended that enterprises with multiple locations use WIDS/WIPS for wireless scanning. Only WIDS/WIPS technologies can offer the detection and containment necessary to track all devices, including clients, and protect against threats from rogues at all times.

AirMagnet Enterprise: The Best Choice for Compliance

AirMagnet Enterprise is a dedicated WIDS/WIPS solution for all enterprise wireless LANs. Using hardware sensors, AirMagnet Enterprise constantly monitors all WiFi channels, including the 200 extended 11a channels, identifying problems, threats, and blind spots where rogue devices can hide. The sensors can automatically block identified threats using both wired and wireless suppression methods. Individuals or departments can be immediately notified, per corporate policy.

Reports can be automatically generated, both at a high level for management validation, or down to the level of device or violation for analysis by the IT or security department. All events are recorded and kept in a secured database for detailed audit reporting.

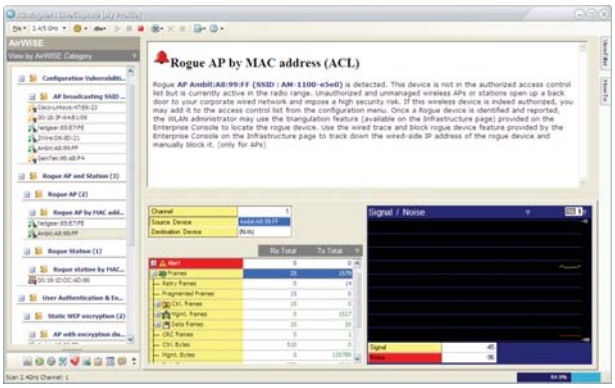
Sensors collect data from all locations. AirMagnet Enterprise compares data against PCI Compliance requirements and automatically produces a report with detailed Pass/Fail information.

Industry Leading Threat Detection

The AirMagnet Intrusion Research Team constantly investigates the latest hacking techniques, trends and potential vulnerabilities in the industry to keep ahead of evolving threats. Their research drives the AirMagnet AirWISE engine which constantly analyzes all wireless devices and traffic using a combination of frame inspection, stateful pattern analysis, statistical modeling, RF analysis, policy analysis and anomaly detection, enabling AirMagnet to detect hundreds of specific threats, attacks and vulnerabilities such as rogue devices, unnapproved connections, spoofed devices, DoS attacks, man-in-the-middle attacks, evil twins, as well as the most recent hacking tools and techniques such as MDK3, Karmetasploit and 11n DoS attacks. All threats can be traced, located and blocked as they happen.

Rogue Detection

AirMagnet Enterprise uses multiple detection mechanisms to find rogue devices in the environment. Devices are traced using a suite of wired and wireless tracing methods to quickly determine if a device is connected to the wired network.

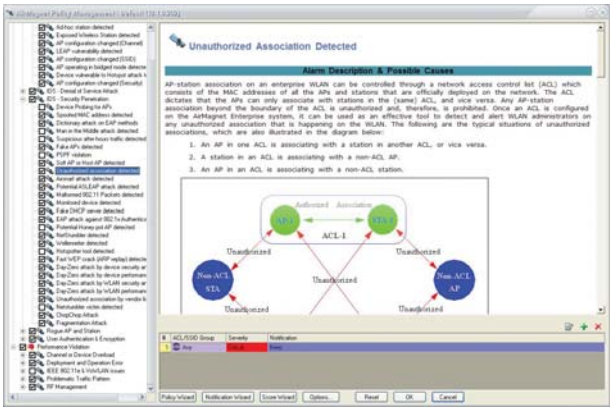


Threats can be manually or automatically remediated with a combination of both wired and wireless threat suppression. Wireless blocking targets a threat at the source and specifically blocks the targeted wireless device from making any wireless connections. Wired blocking automatically closes the wired switch port where a threat has been traced. Threats and devices can be located on a floorplan and set to trigger rogue alarms based on the device's location.

Managers have access to over a dozen notification and escalation mechanisms, making it easy to alert specific staff members of issues or integrate wireless event data into larger enterprise management systems and operations.

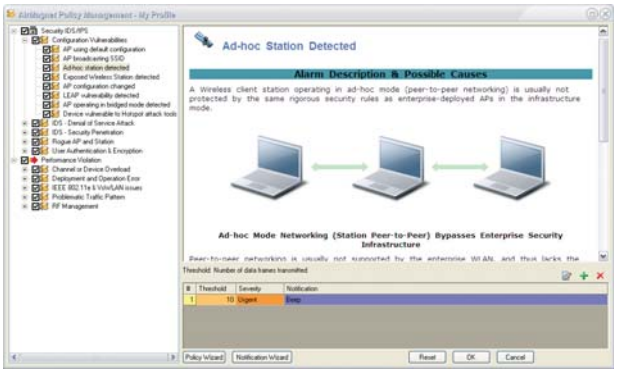
Vulnerability Detection

AirMagnet Enterprise uses built-in WLAN expertise to understand unexpected events in the environment which may leave an organization vulnerable. In this example, AirMagnet is alerting of an unauthorized AP association that could be due to a roaming configuration issue or due to a malicious attacker attempting to lure an AP to connect outside the organization.



Unauthorized Connections

Unsecured and unapproved device connections can open the door to malicious attacks. AirMagnet can look for problems such as Ad-hoc devices that are connected to one another without going through an access point. By connecting peer-to-peer, these devices may bypass detection for appropriate authentication and encryption and circumvent the security infrastructure.



Periodic Scanning Vs. Full-Time Monitoring

AirMagnet offers both a mobile wireless analyzer for local scanning and a WIDS/WIPS solution for remote, full-time monitoring and security. While both AirMagnet Enterprise and AirMagnet WiFi Analyzer can be used to achieve PCI compliance, only AirMagnet Enterprise is the always-on solution best suited to enterprise clients with multiple locations.

	AirMagnet Enterprise	AirMagnet WiFi Analyzer
Detect Rogues and Vulnerabilities	X	X
Interactive Network Testing	X	X
Compliance Reporting	X	X
Device Inventory	X	X
Full-time Monitoring	X	
Proactive Containment	X	
Remote Monitoring and Reporting	X	

About AirMagnet

AirMagnet Inc., a Fluke Networks company, 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 8,200 customers worldwide, including 75 of the Fortune 100.

Corporate Headquarters
830 E. Arques Avenue
Sunnyvale, CA 94085 - USA
Tel: +1.408.400.0200
Fax: +1.408.744.1250

EMEA Headquarters
6-9 The Square, Stockley Park, Uxbridge
Middlesex, UB11 1FW - United Kingdom
Tel: +44.203.178.7926
Fax: +44.870.139.5156