

Retail



Security Is In The Air

Complying With The PCI DSS v1.2 Standard

Manav Khurana and Jon Green

Introduction

On May 4, 2007, the *Wall Street Journal* ran a front-page article titled “Breaking The Code; How Credit Card Data Went Out The Wireless Door” in which it reported the loss of 46 million credit card records due to a wireless network breach in stores owned by TJX Companies. A subsequent investigation revealed that nearly 96 million credit card records were in fact stolen¹. The TJX incident was the largest ever network breach, and while it focused attention on wireless LAN security, the problem was far more widespread than originally believed. OfficeMax, Boston Market, Barnes & Noble, Sports Authority, Forever 21, and DSW were also the victims of crime rings that used unprotected wireless networks as their points of entry².

The Javelin Research & Strategy group pegged the cost of credit and debit card fraud at \$17.9 billion in 2007³, and in their *2008 Identity Fraud Research Report*⁴ estimated that 3.58% of U.S. consumers had suffered from some form of credit card fraud. In more than 55% of cases the fraud involved either stealing or misusing a credit card number – theft of the card itself wasn’t involved.

Since wireless networks use an open medium, many organizations have hesitated to use them to transmit high value data, including credit and debit card transactions. This lulls merchants into a false sense of security because it was the retail corporate networks from which retail credit card information has stolen in the case of TJX and other thefts – the wireless network merely served as a portal. The wireless networks that were hacked were being used for non-cardholder applications such as inventory tracking, but they connected to wired networks used for credit and debit card transactions. The use of very rudimentary wireless encryption, WEP, and a lack of proper network segmentation, enabled the hackers to penetrate the corporate data networks on which they installed “sniffing” software to capture credit and debit card transactions sent over the wire.

In an effort to prevent cardholder data theft, the top five payment card brands – American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International – formed the Payment Card Industry (PCI) standards council. The PCI council defined mandatory security guidelines in the form of the PCI Data Security Standard (DSS) for use by all merchants and service providers that store, process and transmit cardholder data.

The PCI DSS standard specifies how to enhance payment account data security and includes twelve major steps for securing payment account information and testing methodologies to ensure that these requirements are met. Wireless LAN security is a core component of these requirements. These security requirements can be divided into three categories:

- No wireless LAN is in use;
- Wireless LANs are used for non-cardholder data applications;
- Wireless LANs are used for cardholder data transactions.

¹ <http://www.eweek.com/c/a/Security/TJX-Breach-More-Than-Twice-As-Bad-As-Reported/>

² http://www.darkreading.com/document.asp?doc_id=160888

³ <http://www.cujournal.com/article.html?id=20080516ZIR2IRTW&email=y>

⁴ http://www.javelinstrategy.com/uploads/803-1.R_2008IdentityFraudSurveyReportforIssuers_Brochure.pdf

Aruba Networks is a participating organization within the PCI council and supplies wireless LANs and secure mobility solutions that numerous leading merchants have used to comply with PCI standards and prevent network breaches. The sections that follow discuss the PCI requirements in the context of wireless network security, and explain how merchants can cost-effectively and reliably meet these requirements.

PCI Compliance Drivers

While PCI compliance is mandatory for any organization that accepts credit and debit cards, it applies primarily to retailers, hospitals and universities worldwide, collectively termed “merchants” in the PCI nomenclature. Besides the obvious benefit of enhancing security controls to prevent breaches, establishing and maintaining PCI compliance has additional direct and indirect business benefits. First and foremost, a security breach has a negative impact on a merchant’s brand name and consumer loyalty. The threat of identity theft to consumers is real. The onus of safeguarding customers’ private information is on the merchants who accept credit and debit cards for the services and products they provide.

Additionally, merchants risk bank-imposed monetary penalties should they be found out-of-compliance with PCI DSS standards. Conversely, compliant merchants can avail themselves of bank-offered incentives. These penalties and incentives vary by payment card brand, but often include one or more of the following:

- **Monthly non-compliance fines for out-of-compliance merchants:** This fine is levied on the payment processor that provides payment terminals and payment processing to merchants, however, in all cases it has been passed on to non-compliant merchants. The fines are set on a case-by-case basis. In December, 2006⁵ Visa said it would levy a \$25,000/month penalty on every non-compliant merchant. Visa USA alone had levied \$4.6 million in penalties in 2006, up from \$3.4 million in 2005. Visa USA fined TJX Companies \$880,000⁶ for their breach, including \$100,000/month retroactively for non-compliance, \$50,000 one-time penalty for violating the PCI standard, and \$500,000 in egregious fines based on “the seriousness of this security incident and the impact on the Visa system.”
- **Safe harbor for PCI-compliant merchants in the event of a breach:** Any merchant that loses cardholder data due to a breach, and is PCI compliant at the time of breach, is exempt from charges relating to credit and debit card replacements. Otherwise, the merchant is liable for \$80 - \$320 per credit and debit card number lost and replaced. The TJX Companies made a payment of \$40.9 million⁷ to Visa for such fines.
- **Access to lower interchange per transaction rates for PCI-compliant merchants:** merchants can only qualify for lower tiers of per-transaction card brand fees if they are PCI compliant.

⁵ <http://www.corporate.visa.com/md/nr/press667.jsp>

⁶ <http://www.eweek.com/c/a/Security/VISA-Fined-TJX-Processor-for-Security-Breach/>

⁷ <http://www.scmagazineus.com/TJX-agrees-to-41-million-settlement-with-Visa/article/99437/>

PCI Compliance Process

PCI compliance requires adhering to security requirements outlined in the PCI DSS. Merchants filing for first-time compliance, or submitting for annual re-compliance after January 1, 2009, must meet security requirements outlined in the new PCI DSS v1.2 standard. The compliance process varies depending on the “level” designation of a merchant, where the level is determined by the card brand and the annual number of credit and debit card transactions handled by a merchant. The higher the number of transactions, the more involved the certification process. In some instances third-party validation of compliance is required.

The following chart specifies how Visa USA defines merchant levels.⁸

Merchant Level*	Description
1	Any merchant—regardless of acceptance channel—processing over 6,000,000 Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.
2	Any merchant—regardless of acceptance channel—processing 1,000,000 to 6,000,000 Visa transactions per year.
3	Any merchant processing 20,000 to 1,000,000 Visa e-commerce transactions per year.
4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants—regardless of acceptance channel—processing up to 1,000,000 Visa transactions per year.

* New merchant level definitions effective of July 18, 2006.

** Any merchant that has suffered a hack that resulted in an account data compromise may be escalated to a higher validation level.

To achieve and maintain PCI compliance, merchants must undertake four internal initiatives:

1. **Gap Analysis:** the current cardholder data environment is documented and assessed against every requirement of the PCI DSS. This step is often completed with assistance from a Qualified Security Assessor (QSA).
 - a. For every requirement met, the QSA marks them as “In Place” and briefly describes the controls that have been implemented.
 - b. For every requirement not met, the QSA marks them as “Not in Place” and provides a brief description of what is not in place and a date of estimated completion where available.
 - c. For every requirement that does not apply, the QSA marks them as “Not in Place” and notes that they’re “Out of Scope.”
 - d. For every requirement that cannot be met but for which there are compensating controls in place, the QSA marks them as “In Place” and briefly describes the “compensating controls.” Documentation outlining the compensating controls is required and must include the reason(s) why the requirement can’t be met, what compensating controls are used instead, and how the compensating controls meet the intent of the original standard without sacrificing the level of security.

⁸ http://usa.visa.com/merchants/risk_management/cisp_merchants.html

-
2. **Remediation:** every security requirement identified as “Not in Place,” or requirements that are “Not in Place” but are going to be met at a defined date from step 1, must be addressed. This step often requires the implementation of a new process or technology.
 3. **Completion of PCI Compliance:** the cardholder data environment is reassessed against the PCI DSS post-remediation. A PCI-defined report of compliance (ROC) document is created and submitted to the pertinent bank or credit card brand, together with documentation listed below. Level 1 merchants must use the PCI-approved QSA for the ROC. Merchants at others levels may instead use a self-answered questionnaire.
 - a. Vulnerability scan(s) must completed by a PCI-Approved Scanning Vendor (ASV), and evidence of passing scan(s) must be submitted with the ROC.
 - b. A PCI-specified Attestation of Compliance document must be completed and submitted with the ROC.
 - c. Any other required supporting documentation must be submitted.
 4. **Ongoing Compliance:** the merchant must repeat steps 1-3 annually as well as conduct quarterly network security scans using automated tools. Any compensating controls will be reviewed and validated annually.

The PCI Compliance Standard

The PCI Data Security Standard was created to consolidate the varied security requirements of the different credit card brands. The first iteration of the standard, PCI DSS v1.0, went into effect in January 2005. On January 1, 2007, a new revision called PCI DSS v1.1 was put in place, replacing PCI DSS v1.0 and the VISA CISP standard. With PCI DSS v1.1 came new requirements and clarifications to reflect recent changes in the security landscape, and to offer alternatives in the form of merchant “compensating controls” to make compliance more practical.

On October 1, 2008, the PCI council released a second update to the PCI standard called PCI DSS v1.2. The new standard supersedes v1.1 starting January 1, 2009, and all new audits conducted after this date must adhere to the PCI DSS v1.2 specification. PCI DSS v1.2 clarifies v1.1 requirements that were previously open to interpretation. The new standard also updates requirements based on what the industry has learned about security breaches in the intervening years since v1.1 was issued.

The PCI DSS defines six primary goals, 12 major requirements, and over 200 sub-requirements. The following table summarizes the goals and requirements.

Goal	Requirements
Build and Maintain a Secure Network	<i>Requirement 1:</i> Install and maintain a firewall configuration to protect cardholder data. <i>Requirement 2:</i> Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	<i>Requirement 3:</i> Protect stored cardholder data. <i>Requirement 4:</i> Encrypt the transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	<i>Requirement 5:</i> Use and regularly update anti-virus software. <i>Requirement 6:</i> Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	<i>Requirement 7:</i> Restrict access to cardholder data by business need-to-know. <i>Requirement 8:</i> Assign a unique ID to each person with computer access. <i>Requirement 9:</i> Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	<i>Requirement 10:</i> Track and monitor all access to network resources and cardholder data. <i>Requirement 11:</i> Regularly test security systems and processes.
Maintain an Information Security Policy	<i>Requirement 12:</i> Maintain a policy that addresses information security.

The complete PCI DSS v1.2 standard is available for download from https://www.pcisecuritystandards.org/security_standards/download.html?id=pci_dss_v1-2.pdf

What Are The Differences Between PCI DSS v1.1 and v1.2?

PCI DSS v1.2 includes clarifying modifications to several requirements to more precisely explain the controls that need to be implemented. Wireless LAN security was among the topics to which modifications were made. The following excerpt summarizes the updated wireless LAN security objective:

“If wireless technology is used to store, process, or transmit cardholder data (for example, point-of-sale transactions, “line-busting”), or if a wireless local area network (LAN) is connected to or part of the cardholder data environment (for example, not clearly separated by a firewall), the PCI DSS requirements and testing procedures for wireless environments apply and must be performed as well...”

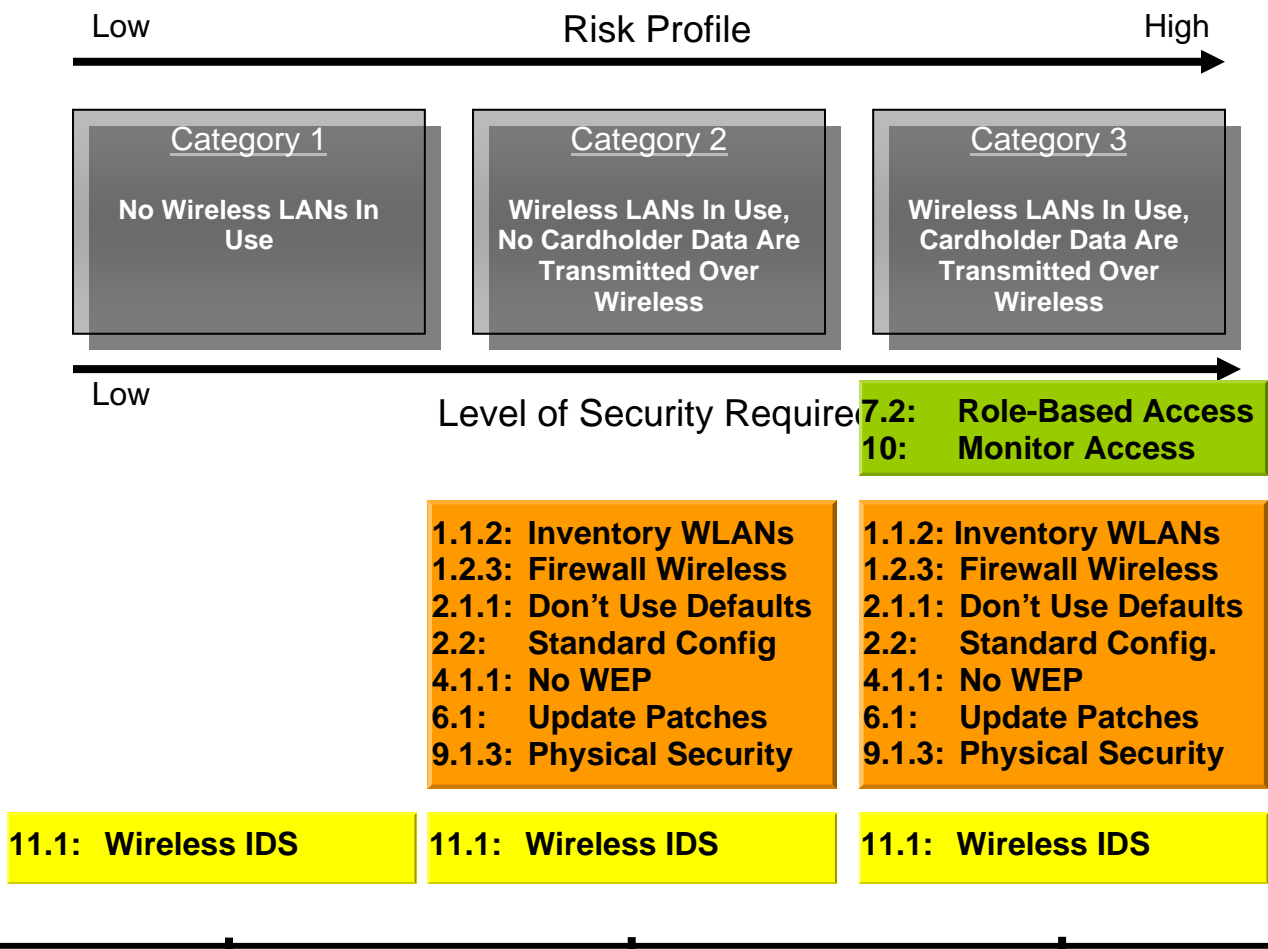
PCI DSS v1.2 compliance necessitates using firewalls, encryption, authentication, and wireless LAN intrusion detection (IDS) for all wireless LANs; some of these safeguards are also required even if the wireless LAN is not used to transmit cardholder data. The wireless LAN requirements that were modified as a part of PCI DSS v1.2 include explicit firewall wireless LAN configuration, elimination of WEP, and the use of wireless IDS:

1. **Firewall wireless LAN:** Requirement 1.2.3 states that a perimeter firewall must be used between any wireless LANs and networks that transmit cardholder data. The term “firewall” is defined to include “stateful inspection” or “dynamic packet filtering.”
2. **WEP is forbidden:** Requirement 4.1.1 prohibits WEP security starting March 31, 2009 for all new wireless LANs, and starting June 30, 2010 for all existing wireless LANs. This requirement applies to all wireless LANs transmitting or otherwise associated with cardholder data.
3. **Wireless IDS is mandatory:** Requirement 11.1 states that all stores, warehouses, and offices that have credit and debit card processing systems must be analyzed or scanned for unauthorized wireless devices. Wireless IDS systems are now an approved alternative to quarterly handheld wireless analyses.

A summary of all differences between PCI DSS v1.1 and v1.2 is available at https://www.pcisecuritystandards.org/pdfs/pci_dss_summary_of_changes_v1-2.pdf.

PCI Requirements Specific To Wireless LANs: Quick Reference

The PCI requirements specific to wireless LANs have been sorted into three levels of implementation in the illustration below. Each category has a different risk profile, and a distinct level of mandatory security controls. The PCI DSS v1.2 requirements that apply to merchants in each of the three categories are shown in the chart below.




Aruba's Solution For PCI Compliance

Aruba offers three levels of wireless LAN security to attain PCI compliance and beyond. The levels differ in terms of the security capabilities provided, how they overlay on top of existing networks, and cost.

Category 1: PCI Monitoring

AirWave Wireless Management




- **Server at HQ monitors all locations**
- **No dedicated sensor h/w required**
- **Monitors for and reports rogues**

The PCI monitoring option entails installing Aruba's AirWave Wireless Management Suite (AWMS) in the HQ (or data center) so that all remote locations and stores can be monitored in compliance with PCI requirements. AWMS is designed to inventory, monitor and manage multi-vendor wireless networks, and represents the most cost-effective approach to addressing applications in which legacy wireless networks are already in place - no hardware or software is required at any remote location.


This option enables merchants to outfit existing networks with wireless network PCI monitoring capabilities without replacing or re-architecting existing wired and wireless networks.

Category 2: Wireless IDS


AirWave Wireless Management



Controller



Sensor



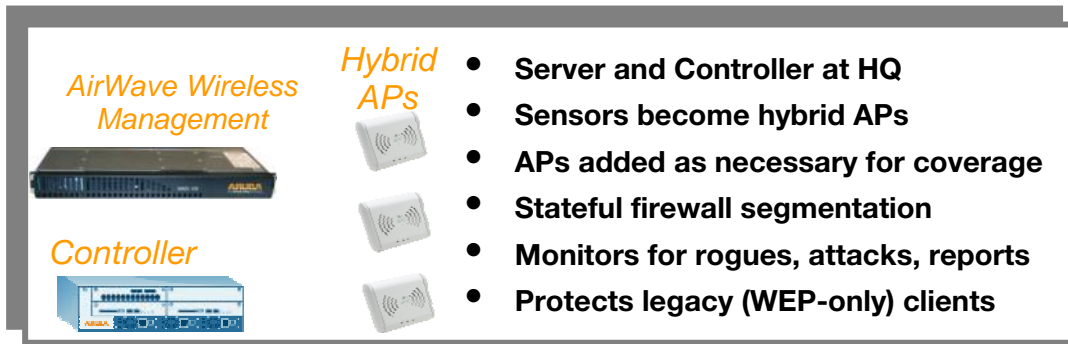
- **Server and Controller at HQ**
- **Sensors in stores scan RF**
- **No change to existing LAN or WLAN**
- **Monitors for rogues, attacks & reports**
- **Prevents rogues & attacks**

The wireless IDS option requires the installation of a dedicated air monitoring sensor in all remote locations. The sensor scans all wireless channels and captured traffic is forwarded to an Aruba Multi-Service Mobility Controller in the HQ (or data center) for analysis. The Controller compares wired and wireless traffic, identifying and locating any rogue devices, attacks originating from outside the building, and most importantly, automatically blocks rogue devices and attacks.

AirWave's PCI monitoring capabilities are enhanced when used in conjunction with WIDS, while greater RF granularity is obtained by using dedicated sensors.

As with the Category 1 solution, the AirWave + WIDS option enables merchants to outfit existing networks without replacing or re-architecting existing wired and wireless networks.

Category 3: Aruba Wireless LAN With IDS and Role-Based Access Control



The wireless LAN with IDS and role-based access control option integrates the functions of a centralized wireless LAN, built-in stateful firewall, built-in wireless IDS, and AirWave monitoring. Aruba Controllers in the data center and remote locations are managed centrally through the Airwave Management Platform, which aggregates all wireless network information and provides PCI compliance reports.

The integrated Aruba WLAN provides all of the security controls necessary to meet wireless LAN specific PCI requirements, offers security controls for some PCI wired LAN requirements, and includes security controls that go beyond PCI requirements to help prevent breaches. Competing solutions require 3x - 4x the amount of hardware and software to provide comparable functionality.

Aruba's hybrid Access Points (APs) are multiple function devices. First and foremost, they provide secure wireless LAN coverage for data, voice, and video applications. The same AP also functions as a wireless IPS sensor, a wireless mesh node, and a remote access VPN client. Hybrid APs installed in each remote location or store send all traffic to a centralized controller in the HQ (or data center) via an encrypted tunnel. Larger stores may require a small local Controller.

The central Controller aggregates all traffic, which is first inspected via role-based stateful firewall segmentation to ensure compliance with security policies, encryption/decryption requirements, and wireless intrusion detection and prevention services. Firewall segmentation can block vulnerable legacy WEP or WPA-PSK devices.

The Category 3 solution is ideal for merchants that need to replace existing, legacy wireless LANs in order to comply with security, management and application requirements.

Start Small, Grow As Needed

The three categories of solutions described above address three different security needs. That said, merchants can easily migrate to a higher Category, and thereby leverage existing investments, by simply adding the additional devices and/or software required by the higher Category - merchants can economically enable all or a subset of the capabilities. By way of example, an Aruba sensor can later be converted into a hybrid sensor/AP via software download over the network.

Aruba's Solution & PCI Compliance Requirements: Quick Reference

PCI Requirement	PCI Monitoring	Wireless IDS	Aruba WLAN
<i>Requirements For Category 1: No WLAN</i>			
11.1: Wireless IDS	✓	✓	✓
<i>Additional Requirements For Category 2: No Cardholder Data Over WLAN</i>			
1.1.2: Inventory WLAN	✓	✓	✓
1.2.3: Firewall WLAN			✓
2.1.1: Don't Use Defaults	✓	✓	✓
2.2: Standard Configuration	✓	✓	✓
4.1.1: No WEP			✓
6.1: Updated patches		✓	✓
9.1.3: Physical AP security			✓
<i>Additional Requirements For Category 3: Cardholder Data Over WLAN</i>			
7.2: Role-based control			✓
10: Monitor access	✓	✓	✓
<i>Additional Requirements For Wired LAN Security</i>			
5.2: Anti-virus enforcement			✓
8.3: Secure remote access			✓
8.5.6: Time-based control			✓
9.1.2: Secure public ports			✓

Detailed Compliance Requirements

This section steps through each PCI DSS v1.2 data security requirement related to wireless networks (and some related to wired networks) for environments that process, transmit and store credit and debit card data.

Category 1: No Wireless LANs Are In Use

Requirement 11.1: Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.

Requirement 11 states that regular tests and evaluations of systems must be conducted to ensure that new vulnerabilities are not present. As a sub-requirement, 11.1 mandates periodically monitoring of wireless networks and devices in order to detect the presence of unauthorized wireless networks or devices that open a backdoor to the card holder data environment. Two approaches to meeting this requirement are described:

1. Using a handheld wireless analyzer and survey the every location (stores and warehouses) to inventory all devices in use;
2. Using a wireless IDS system to scan every location automatically and create an inventory of all devices in use.

The AirWave Wireless Management Suite (AWMS) offers a User Session Report that provides a complete list of every device and user (by username, MAC address, SSID, etc.) that connects to an Aruba wireless LAN or a 3rd party wireless LAN within a given period. AWMS's New User Report lists any new devices (those that were not previously detected) that have connected to the network within a specified period. In addition, AWMS's RAPIDS Rogue AP detection module analyzes both wired and wireless networks and raises an alert upon detecting any unknown, unauthorized access points on the network.

Aruba APs function both as access devices servicing clients and as air monitors that scan on a periodic basis. Operating in monitoring mode, Aruba APs identify and record all other wireless devices detected in the area, including clients, APs, and bridges. All detected devices are presented on a central reporting screen, and detailed information up to and including full packet capture can be obtained for each device.

Using patented classification technology, Aruba's solution can automatically classify foreign APs or devices found as "interferers" or rogues. An interferer is an AP that is detected through radio transmissions, but is not treated as a security threat, e.g., an AP owned by a neighboring business or residence. A rogue AP is detected both on the wired and wireless networks, and is treated as a security threat. Detection of a rogue AP generates an alert to the network administrator, and the system can be configured to automatically shut down access to detected rogues. The network can also pinpoint the location of the rogue AP on a building floor plan.

Aruba's WIDS systems also incorporate wireless intrusion protection (WIPS) capability. Unlike standard network-based intrusion detection systems, WIPS focus specifically on attacks that occur over the wireless network. Attacks are validated against a automatically updated threat library and include denial of service, flooding, man-in-the-middle, impersonation, mis-configuration, and jamming. All attacks and suspected attacks are logged with identifying information such as time, MAC address, and physical location.

Category 2: No Card Data Over WLAN

Requirement 1.1.2: *Current network diagram with all connections to cardholder data, including any wireless networks*

As a part of a PCI audit, merchants are required to provide an inventory of all wireless devices and networks, and to keep this inventory updated at least on a quarterly basis. AWMS's device inventory report lists every component of the wireless infrastructure, including brand, model, version, IP address, MAC address, SSID, and notes on physical location. AWMS's VisualRF module identifies the physical location of every device a sitemap for documentation purposes.

Requirement 1.2.3: *Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.*

This requirement mandates the installation and maintenance of a firewall to prevent unauthorized access and hacker attacks originating from a wireless network and targeting the network carrying cardholder data.

Aruba is the only wireless vendor to integrate an ICSA-certified stateful firewall into its wireless LAN, ensuring that parameters such as security, suitability for a task, default configuration, and logging / audit trails have been validated. The firewall meets PCI DSS requirements for stateful inspection (as specified in requirement 1.3.6).

The default posture of an Aruba firewall is to deny all traffic from the wireless network. Firewall rules to permit traffic are applied on a "role" basis, with each user and device on the network mapped to a specific role. Roles identify the purpose, access rights, quality of service (QoS), bandwidth limits, time-of-day, and location restrictions assigned to a device or user. Examples of roles include:

- Point-of-sale (POS) device in a retail store that must send credit and debit card data, inventory status, and price updates, and for which the Aruba role-based firewall restricts sources and destinations of specific protocols;
- Store manager on a laptop who may require access to in-store or corporate database servers and general Internet access, but does not have access to cardholder data systems;
- PC-based kiosk for use by the general public that is allowed internal and external web browsing, but is denied all other network access;
- Clerk logged into a shared workstation with privileges necessary to do his or her job, but no access to the Internet or central servers or databases in which cardholder data are stored;
- Inventory tracking barcode scanner that is allowed to send and receive bar code data, but does not access corporate databases, including credit card data.

The role of a user or device is typically determined through authentication. Authentication through a secure method such WPA2 is preferred, but MAC address authentication may be used for less capable devices. Once the role of a user or device is assigned, the corresponding firewall policies are applied to all network traffic to and from the wireless device. The firewall policies are tightly bound to the user's identity and authentication state to prevent man-in-the-middle and spoofing attacks. The user state information is also coupled with Aruba's wireless IDS to provide integrated protection against a host of wireless attacks

Requirement 2.1.1: *For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.*

The requirement mandates changing default security configuration settings for any wireless equipment used to transmit, or connected to network that transmits, cardholder data. AWMS helps merchants meet this requirement by automatically discovering wireless APs and controllers, and then automatically pushing group-based configuration policies to overwrite any default settings, i.e., WEP keys, SSIDs, etc. AWMS validates the configuration settings by automatically scanning the network using factory default credentials to ensure that no devices respond.

Upon initial power-up of an Aruba WLAN, the network administrator must assign passwords, SSIDs, encryption keys, and other parameters – thereby overwriting default settings. For automated deployments at remote sites, default configurations are automatically changed upon power-up and then synchronized with AWMS or master Controllers at HQ (or in the data center). WPA and WPA2 are supported, as are multiple SSIDs using different encryption techniques.

Traditional wireless solutions required extensive configuration of security parameters, including RADIUS shared secrets, passwords, administrative logins, and SNMP communities. As part of good security practices, these parameters need to be rotated periodically, sometimes for thousands of devices, resulting in an extensive management burden. Aruba prevents AP or device mis-configuration by using a centralized Multi-Service Mobility Controller in which all configuration, security, and management are implemented, and a line of “thin” APs. These APs act as wireless extensions of the Controller, and only the Controller needs to be configured or secured. Aruba APs and Controllers can be deployed across a WAN, with remote APs establishing secure encrypted connections back to the central Controller. This architecture prevents the mis-configurations typical of both legacy and traditional wireless deployments.

Requirement 2.2: *Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.*

During a PCI audit merchants are required to explain what configuration standards are used and how they are enforced. These requirements also apply for any wireless networks in use. AWMS defines the configuration policies centrally for wireless networks on a group-by-group basis so that specific configuration policies can be defined for retail stores vs. distribution centers vs. corporate headquarters. AWMS supports most leading hardware brands and models, including legacy devices, and thereby services as a single location at which configuration policies are defined and enforced for the entire network.

AWMS also provides automated Custom Compliance Audits that check the configuration of every network device against defined policies. A high-priority alarm is generated whenever a violation is detected, and the merchant can instruct AWMS to automatically correct any violations or use the Audit Report to create a full list of mis-configured devices and specifying the settings that do not comply with established policies.

Requirement 4.1.1: *Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission. For new wireless implementations, it is prohibited to implement WEP after March 31, 2009. For current wireless implementations, it is prohibited to use WEP after June 30, 2010.*

This requirement specifies the use of strong encryption for wireless transmission whether or not credit and debit card data are transmitted, and strict timelines on the elimination of the compromised security mechanism, WEP. Prior to PCI DSS v1.2, this requirement applied only if the wireless networks were transmitting credit card data.

There are two approaches to complying with Requirement 4.1.1.

1. Eliminate the WEP security by reconfiguring existing wireless networks to use 802.11i-specified security such as WPA or WPA2. Given hardware and software restrictions of legacy devices in use, this approach may require a replacement of certain wireless devices such as barcode scanners and embedded wireless devices.
2. Segment the wireless network and devices to quarantine WEP-based devices from the cardholder environment using PCI-defined segmentation techniques. Doing so shifts WEP-only devices “out-of-scope” of PCI compliance. This approach can shield merchants from the cost and complexity of replacing legacy systems already in place.

Aruba specifically recommends against the use of WEP because of security concerns. To this end, an Aruba wireless LAN simultaneously supports all of the following encryption and authentication protocols:

- WPA (802.1x authentication with TKIP encryption);
- WPA2 (802.1x authentication with AES-CCM encryption);
- IPSEC (3DES or AES-CBC encryption) ;
- PPTP (VPN technology using MPPE encryption);
- xSec (802.1x authentication with AES-CBC-256 encryption designed for Federal and sensitive commercial applications).

Legacy barcode scanners present a specific challenge with respect to WEP, and in many cases legacy scanners do not support alternate encryption and authentication protocols. Aruba’s integrated ICSA-certified, role-based firewall can segment these WEP devices and thereby move them outside the scope of PCI compliance. The role-based firewall also enables Aruba to prevent unauthorized access to the cardholder environment, blacklisting any unauthorized devices that attempt to penetrate the Aruba wireless LAN.

Requirement 6.1: *Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.*

Aruba's Wireless Security Incident Response Team (WSIRT) automatically alerts customers of any security-related issues and updates. Additionally, Aruba's wireless IDS systems are linked with the Wireless Vulnerability and Exploits systems hosted at www.wve.org, a comprehensive and up-to-date threat library from which signatures for new threats can be downloaded.

The other processes are simplified by centralizing configuration and management in the Aruba Controller and AWMS system. New system updates simply need to be uploaded to the Controller, and following by a system reset all managed access points will be instantly updated without intervention by the network administrator. Retail chains with hundreds or thousands of locations can thus be updated to the latest software at the same time.

Aruba's unique programmable architecture allows non-disruptive evolution of security postures as the security threat landscape evolves. Organizations can achieve unprecedented savings in both capital and operational expenses compared with non-integrated solutions. For example, in traditional wireless systems changing an encryption standard would typically require hardware upgrades or replacement of every AP. In an Aruba wireless LAN, this can be easily accomplished by loading a Controller software update..

Requirement 9.1.3: *Restrict physical access to wireless access points, gateways, and handheld devices.*

This requirement establishes the need for good physical security, under the principle that any electronic security mechanism can be compromised if physical access is available. Specifically, requirement 9.1.3 calls out the need to secure physical access to wireless APs.

Aruba recommends that APs be kept physically secure to avoid theft. However, Aruba limits the risk of information exposure should physical security be compromised by maintaining encryption keys, passwords, and other configuration information in the Controller and not in the APs.

Category 3: Card Data Over WLAN

Requirement 7.2: *Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.*

This requirement addresses the recommended security practice of "principle of least privilege" whereby access to data, systems, and networks is restricted based on a user's identity. Aruba enforces the principle of least privilege by identifying users or devices, placing them into separated roles, and permitting or denying access to network resources or protocols based on those roles. As described earlier, this capability allows a POS terminal to be treated differently than a manager on a laptop, a public kiosk, or an employee on a shared-use terminal. Aruba logically separates all traffic and permits access only to the level specifically granted by the administrator based on business needs.

Aruba's wireless LANs also integrate with existing user databases to look-up and enforce access privileges on managed devices. For unmanaged devices, Aruba's wireless LAN pushes a captive portal Web page to identify the user and restrict access for specified users, locations and time.

For administrative and IT access to wireless LAN equipment, AWMS offers flexible, role-based administrative access so the level of access available to each IT administrator can be established according to job function, i.e., read-write privileges for network engineers or read-only privileges for the Help Desk.

Requirement 10.3: *Record at least the following audit trail entries for all system components for each event, including User identification, Type of event, Date and time, Success or failure indication, Origination of event, Identity or name of affected data, system component, or resource.*

Requirement 10.3 establishes a baseline for system logging, monitoring, and auditing that must be undertaken for user access to servers and administrative IT actions for a year. AWMS provides audit logs for administrative actions for up to two years, as well as detailed audit trails and system logging of all activities on the wireless network. Logs for Aruba's wireless LANs are stored on the system, and may be exported in real-time to one or more syslog servers. Available logs include:

- Wireless associations, including time, MAC address, AP number, and physical location;
- Authentication attempts, including time, username, MAC address, IP address, AP number, and physical location;
- Network traffic - whether permitted or denied – including time, username, MAC address, IP address, AP number, and physical location;
- All access to the controller management interface, including configuration changes made to the system. Logs include time, IP address, username, and the configuration that was changed;
- Wireless attacks and intrusion attempts, including time, MAC address, AP number, and physical location.

Additional Non-Wireless LAN Requirements Addressed By Aruba

Requirement 5: *Malicious software, commonly referred to as “malware”— including viruses, worms, and Trojans—enters the network during many business approved activities including employees’ e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.*

This requirement specifies the need to install and enforce the use of anti-virus software, and to keep such systems regularly updated. Aruba's Multi-Service Mobility Controllers integration with Aruba's Endpoint Compliance System, Juniper's Unified Access Control, and Zonelabs – among others – to ensure that clients attempting to access the network are up to date with the latest virus definition files. These software packages check for a variety of conditions, including the presence and configuration of anti-virus and personal firewall software, operating system patches and updates, registry settings, and system configuration. If a device is found to be out of compliance, the Controller puts the device into a restricted role and redirects traffic to a self-service remediation server from which updates can be obtained.

Aruba can also enable network-based antivirus protection for systems that cannot run host-based protection, making it the only WLAN system that offers a holistic approach to endpoint compliance for both managed and unmanaged devices.

Requirement 8.3: *Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.*

This requirement specifies that remote access to corporate networks is adequately secured in order to prevent unauthorized or malicious users from gaining access to the cardholder environment.

Aruba's Remote Access Point (RAP) software can be loaded into any Aruba access points to enable secure remote access without complex and hard-to-manage software VPN systems. RAP sets up a secure VPN tunnel over any hard-wired or 3G wide area connection to provide corporate network access to remote users. The built-in VPN client obviates the need for additional VPN software on client devices. Additionally, the same strong multi-factor authentication mechanisms used on a LAN are extended to remote users. Aruba minimizes the complexity and cost of competing systems that require the set-up, management and client revision control of multiple authentication systems.

Requirement 8.5.6: *Enable accounts used by vendors for remote maintenance only during the time period needed.*

This requirement specifies controls to prevent cases in which network access for system maintenance is accidentally left open.

Aruba's role-based firewall implements and log roles for guest or contractor access for pre-defined time windows – access is denied once the window closes. Easily used interfaces permit scheduling guest and contractor access, so that non-technical personnel can manage temporary access registration.

Requirement 9.1.2: *Restrict physical access to publicly accessible network jacks.*

This requirement mandates the use of controls so that publicly accessible network ports in conference rooms, lobbies and open areas are protected from malicious users.

Aruba's role-based firewall enforces identity-based access control to both the wireless and wired networks with up to 80Gbps of packet throughput capacity available on a per-Controller basis. It is very common for large enterprises to obtain high levels of identity-based security on wired networks by tunneling public network ports in conference rooms and other open areas to an Aruba Controller. Doing so presents unauthorized users from gaining access to the network by simply plugging into an open port.

Summary

The PCI DSS v1.2 standard defines mandatory requirements that must be met by all organizations that accept credit and debit cards. The standard's strict wireless LAN security requirements impact firewalls, authentication and encryption methods, monitoring and management systems, and can in some instances require costly and complex upgrades to existing networks. The cost of implementing previous versions of the PCI standard made some enterprises reticent to fully embrace the security requirements, leaving their wireless networks open to attack. Under the new PCI DSS v1.2 standard wireless security controls must be implemented or expensive fines will be levied.

Aruba's secure mobility solutions offer a cost-effective means of achieving PCI compliance. By providing an integrated solution, and eliminating the need to purchase and integrate multiple disparate network technologies, Aruba simplifies the task of securing a wireless network. Aruba also offers a range of solutions intended to fit varying needs for security controls on existing or legacy wireless networks, preventing the need for a wholesale upgrade.

- **Significant capital and operational cost savings:** Built-in security capabilities address every wireless LAN-specific PCI requirement (and many wired LAN requirements).
- **Easy to integrate:** Fits on top of your existing networks and thereby eliminates the need to redesign or replace legacy network infrastructure. Aruba's solutions extend the same high security paradigm to remote locations and stores, providing one common model for the entire enterprise.
- **Protects existing investments:** Securely segments legacy WEP-only devices to move them outside the scope of PCI compliance, thereby avoiding costly device upgrades.

Learn more about Aruba's secure retail solutions at <http://www.arubanetworks.com/applications/retail.php>.

About Aruba Networks, Inc.

People move. Networks must follow. Aruba securely delivers networks to users, wherever they work or roam. Our mobility solutions enable the Follow-Me Enterprise that moves in lock-step with users:

- Adaptive 802.11a/b/g/n Wi-Fi networks optimize themselves to ensure that users are always within reach of mission-critical information;
- Identity-based security assigns access policies to users, enforcing those policies whenever and wherever a network is accessed;
- Remote networking solutions and fixed mobile convergence ensure uninterrupted access to applications as users move;
- Multi-vendor network management provides a single point of control while managing both legacy and new wireless networks from Aruba and its competitors.

The cost, convenience, and security benefits of our secure mobility solutions are fundamentally changing how and where we work. Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at <http://www.arubanetworks.com>.

WP_PCI12_US_081016



1344 Crossman Ave. Sunnyvale, CA 94089-1113
Tel. +1.408.227.4500 | Fax. +1.408.227.4550 | info@arubanetworks.com
<http://www.arubanetworks.com>