Alcatel·Lucent

TECHNOLOGY WHITE PAPER

Payment Card Industry Data Security Standard (PCI DSS) Primer Version 1.1

Applying PCI to wireless LANS and compliance requirements

Credit card theft is costing the U.S. economy an estimated $500 million a year (Department of Homeland Security) and the cost to the economy has increased at 21% annually over the last two years (January 005 Study, Consumer Sentinel). In an effort to curb the sharp rise and strikingly large impact of credit card theft, the top five payment card brands – American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International – have formed the Payment Card Industry (PCI) standards council. This council has defined security guidelines in the form of the PCI Data Security Standard or the PCI DSS that applies globally to all merchants and service providers that store, process and transmit credit card data.

Table of Contents

Introduction

The PCI DSS standard consists of "a set of comprehensive requirements for enhancing payment account data security" that includes twelve major security requirements to secure payment account information and testing methodologies to ensure these requirements are met. The PCI security standard can be found at https://www.pcisecuritystandards.org/ tech/download_the_pci_dss.htm

On January 1, 2007, a new revision of the PCI DSS, called PCI DSS v1.1, went into effect. PCI DSS v1.1 succeeds the PCI DSS January 2005 (a.k.a., PCI v1.0), which succeeds the VISA CISP standard. With PCI DSS v1.1, requirements have been added to, clarified and modified to reflect changes in the security landscape since 2004 and to offer alternatives for retailers to make compliance more practical. A good summary of changes in PCI v1.1 can be found at http://www.eweek.com/article2/0,1895,2016873,00.asp

The increasing adoption of WLANs creates a new set of security threats and vulnerabilities to networks in retail stores that carry credit card data. To this end, PCI DSS v1.1 provides specific security requirements for different wireless LAN applications – from wireless in-store inventory applications to applications such as wireless point-of-sale that wirelessly transmits payment card information. There are even requirements for retailers that do not operate wireless LANs, but may come in contact with them in ways that could impact the security of the retailer's connection to the credit card processing network.

This paper describes the requirements and solutions that relate to wireless LANs in the new PCI DSS v1.1.

PCI Compliance

PCI compliance, mandatory for retailers worldwide, has direct and indirect business benefits. First, no retailer who is PCI-compliant has ever been a victim of credit card theft. More than the direct cost savings of avoiding a breach, there is a tacit benefit to the retailer's brand. The threat of identity theft to consumers is real. Consumers are not likely to remain loyal to brands to which they can't trust their private information.

Secondly, there are bank imposed monetary penalties that apply if a retailer is found out-of-compliance. While the PCI standards council defines the security standard and facilitates the compliance process, compliance is enforced by each of the payment card brands. As an example, Visa USA (the US arm of one of the five major banks) stated that it alone levied $4.6 million in penalties in 2006. Penalties levied on a retailer vary based on numerous parameters such as the number and magnitude of incidents, etc. Penalties are imposed in the form of monthly cash payments, lump-sump cash payments or increases in credit card transaction fees.

Getting PCI compliance requires adhering to security requirements outlined in the PCI security standard. Retailers filing for first-time compliance or submitting for annual re-compliance after January 1, 2007 must meet security requirements outlined in the PCI DSS v1.1 standard. The PCI standards council has outlined a compliance process that includes security assessments, security scans and questionnaires. The exact process varies depending on the "level" to which a retailer belongs. This level is usually determined by the number of credit card transactions a retailer handles per year. The higher the number of transactions, the more involved is the certification process, including third-party validation.

What's New With PCI V1.1?

In May, 2006, the PCI DSS was updated to version 1.1 to "foster broad adoption by acknowledging practical implementation issues, incorporating partner and customer feedback, while maintaining the robustness of security measures." The updates to the standard fall into three general categories:

- Clarification of requirements set forth in the first version of the standard.
- Adding an element of flexibility with compensating controls to allow for technology or business constraints.
- Addition of security measures to keep up with the latest trends and vulnerabilities.

A detailed definition of the changes from PCI DSS v1.0 to v1.1 can be found at:
https://www.pcisecurity standards.org/pdfs/pci_summary_of_pci_dss_changes_v1-1.pdf

A key change from v1.0 to v1.1 as it relates to wireless LAN usage is in requirement 11.1. With the updated standard, every retail store must use wireless analyzers periodically to ensure that there is no unauthorized wireless network or device connected to the network that is transmitting credit card data. The wireless analyzer requirement applies even if there is no authorized wireless LAN used for inventory or any other applications.

WLAN Specific PCI Requirements: Summary

The following table lists all of the PCI v1.1 requirements that relate to wireless LANs. The requirements are broken up in to three categories. Each category corresponds to a different profile of threat to credit card data – based on the type of wireless LAN access and mobile applications that are implemented.

REQUIREMENT NUMBER	**RETAIL ENVIRONMENT**	
	Apply even if no wireless is installed	
11.1	Use wireless analyzers periodically	**Yes**
	Also apply if using any in-store wireless applications	
1.3.8	Use firewalls for data protection between wireless and wired	**No**
2.1.1	Do not use wireless connectivity defaults	**No**
5	Use and regularly update anti-virus software	**Yes**
6	Maintain secure systems	**Yes**
9.1.3	Physical security	**No**
	Also apply if wireless point-of-sale is used	
4.1.1	Encrypt wireless link carrying payment card information	**Yes**
7.1 & 7.2	Restrict access by need to know	**No**
10.3	Track and monitor network access	**No**

WLAN Specific PCI Requirements

The following sections detail the PCI v1.1 data security requirements that pertain to wireless LAN use in retail environments that process, transmit and store credit card data. In addition, for each of the requirements that apply to wireless LANs, there is a description of how Alcatel-Lucent's OmniAccess Wireless meets these requirements using built-in security components.

Apply even if no wireless is installed

REQUIREMENT 11.1: REGULAR VULNERABILITY TESTING WITH WIRELESS ANALYZERS

Test security controls, limitations, network connections, and restrictions annually to assure the ability to adequately identify and to stop any unauthorized access attempts. Use a wireless analyzer at least quarterly to identify all wireless devices in use.

Requirement 11 discusses the need to conduct regular tests and evaluations of systems to ensure that new vulnerabilities are not present. Requirement 11.1 requires periodic monitoring of wireless networks and devices, specifically to detect and prevent the presence of an unauthorized wireless network that may be creating a backdoor into the network carrying card holder data.

Alcatel-Lucent solution: All Alcatel-Lucent access points function both as an access device servicing clients as well as an air monitoring device on a periodic basis. In monitoring mode, Alcatel-Lucent devices identify and record all other wireless devices detected in the area, including clients, APs, and bridges. All devices can be viewed from a central reporting screen, and detailed information up to and including full packet capture can be obtained for each device.

Using patented classification technology, the Alcatel-Lucent OmniAccess Wireless system can automatically classify foreign APs or devices found as "interferers" or "rogues." An interfering AP is detected through radio transmissions, but is not treated as a security threat – a common example of an interfering AP is an AP owned by a neighboring business or residence. A rogue AP, on the other hand, is detected both on the wired network as well as the wireless network, and is treated as a security threat. Alerts are generated to the network administrator when a rogue AP is found, and the system may be configured to automatically shut down access to rogue APs. An administrator located at the data center also has the ability to see the pinpointed location of the found AP or device on a floor plan.

Alcatel-Lucent OmniAccess Wireless systems also incorporate a wireless intrusion protection (WIP) system. Unlike standard network-based intrusion detection systems, WIP focuses specifically on attacks that occur over the wireless network. Attacks detected 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.

The Alcatel-Lucent OmniVista Quarantine Manager and the Alcatel-Lucent OmniSwitches provide additional means for protecting the network from rogue APs. A network administrator using the Quarantine Manager can identify the specific switch and switch port where the rogue AP is connected to the network. In addition, the Quarantine Manager can send commands to the Alcatel-Lucent OmniSwitches to block all traffic in the network originating from the rogue AP. The combination of wireless and wired isolation of rogue APs provides a strong protection for the retail network.

Apply if any in-store wireless applications are implemented

REQUIREMENT 1.3.8: USE FIREWALLS FOR DATA PROTECTION BETWEEN WIRELESS AND WIRED

Installing perimeter firewalls between any wireless networks and the cardholder data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic (if such traffic is necessary for business purposes)

This requirement establishes the need to install and maintain a firewall to prevent unauthorized access and hacker attacks to the network that is carrying cardholder data that originated from the wireless network.

Alcatel-Lucent OmniAccess Wireless solution: Alcatel-Lucent has integrated an ICSA-certified stateful firewall as a part of its wireless LAN solution. The firewall has passed the rigorous requirements of ICSA Labs. Because the Alcatel-Lucent product meets the strict ICSA criteria, network managers can be assured of such parameters as security, suitability for a task, default configuration, and logging / audit trails. ICSA certification of a firewall also ensures that other requirements of PCI DSS, such as the need for a firewall to do stateful inspection (specified in requirement 1.3.4) are met.

The default posture of an Alcatel-Lucent OmniAccess Wireless firewall is to deny all traffic from the wireless network. Firewall rules to permit traffic are then 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, and time-of-day and location restrictions assigned to a device or user. Examples of roles include:

- A point of sale (POS) device that must send credit card data as well as download inventory and price updates. This device would be limited to communicating with specific servers using specific protocols.
- A store manager on a laptop. This person may require access to in-store or corporate database servers, and may also require general Internet access.
- A PC-based kiosk for use by the general public. This device should be permitted to do Web browsing, for example to browse a website with store information, but should be denied all other network access.
- A clerk logging into a shared workstation. The clerk should have only that privilege necessary to do his or her job, but should not be given Internet access or have access to central servers or databases where cardholder data is stored.

The role of a user or device is typically determined through authentication. Authentication through a secure method such as WPA or 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 or from the wireless device. These 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 Alcatel-Lucent's Wireless Intrusion Protection (WIP) system to provide integrated protection against a host of wireless attacks

REQUIREMENT 2.1.1: DO NOT USE DEFAULT PASSWORDS AND CONFIGURATION

For wireless environments, change wireless vendor defaults, including but not limited to, wired equivalent privacy (WEP) keys, default service set identifier (SSID), passwords, and SNMP community strings. Disable SSID broadcasts. Enable Wi-Fi protected access (WPA and WPA2) technology for encryption and authentication when WPA-capable

This requirement deals with changing the default passwords and configuration of equipment. The requirement further calls out the need to change default configuration for wireless equipment.

Alcatel-Lucent OmniAccess Wireless solution: Alcatel-Lucent assists in compliance with these requirements by not assigning default parameters to the system. Upon initial power-up, the network administrator must assign passwords, SSIDs, encryption keys, and other parameters. For automated deployments in remote sites, the default configuration is automatically changed upon power-up and is synchronized with Alcatel-Lucent management platforms or WLAN switches in the data center. WPA and WPA2 are supported, as well as multiple SSIDs using different encryption techniques.

In addition, the Alcatel-Lucent system prevents AP or device mis-configuration. 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. Alcatel-Lucent's OmniAccess Wireless architecture consists of a centralized WLAN switch where all configuration, security, and management are implemented, and a line of "thin" APs (access points). Unlike conventional "fat" APs, Alcatel-Lucent APs are not configured or managed devices. These APs act as wireless extensions of the WLAN switch, so that only the switch needs to be configured or secured. Alcatel-Lucent APs and WLAN switches can be deployed across a WAN, with remote APs establishing secure encrypted connections back to a central WLAN switch. This architecture prevents the mis-configuration common in traditional wireless deployments.

REQUIREMENT 5: USE AND REGULARLY UPDATE ANTI-VIRUS SOFTWARE

Many vulnerabilities and malicious viruses enter the network via employees' e-mail activities. Anti-virus software must be used on all systems commonly affected by viruses to protect systems from malicious software.

This requirement specifies the need for anti-virus software to be installed and regularly updated.

Alcatel-Lucent OmniAccess Wireless solution: Alcatel-Lucent WLAN switches support a unique integration with client integrity and endpoint compliance systems such as Bradford Networks, and Zonelabs that can ensure that clients attempting to access the network are up to date. 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 Alcatel-Lucent OmniAccess Wireless LAN switch places the device into a restricted role and redirects traffic to a self-service remediation server where updates may be performed. Alcatel-Lucent wireless systems 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 issues for both managed and unmanaged devices.

REQUIREMENT 6: MAINTAIN SECURE SYSTEMS

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches. All systems must have the most recently released, appropriate software patches to protect against exploitation by employees, external hackers, and viruses. Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

This requirement defines the need to develop and maintain systems in a secure manner.

Alcatel-Lucent OmniAccess Wireless solution*:* Alcatel-Lucent's Customer Support team alerts customers to any security-related issues and updates. The rest of the process is simplified by centralizing all configuration and management in the WLAN switch. System updates are accomplished by uploading a new software image to the WlAN switch, followed by a system reset. Upon booting the new image, all access points managed by the WLAN switch are instantly updated as well, without intervention by the network administrator. In this way, retail chains with hundreds of locations can all be updated to the latest software at the same time. Alcatel-Lucent OmniAccess Wireless is unique in offering a programmable architecture that allows non-disruptive evolution in security posture as the security threat landscape continues to change. This capability offers organizations unprecedented savings in both CAPEX and OPEX versus non-integrated solutions. For example, in traditional wireless systems, a change to an existing encryption standard or addition of a new encryption standard would typically require hardware upgrades or replacement of each access point. In an Alcatel-Lucent OmniAccess Wireless deployment, such developments would only require a software update to the WLAN switch.

REQUIREMENT 9.1.3: PHYSICAL SECURITY

Restrict physical access to wireless access points, gateways, and handheld devices.

This 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.

Alcatel-Lucent OmniAccess Wireless solution*:* Alcatel-Lucent recommends that APs be kept physically secure to avoid theft, but is unique in the industry in that the APs are designed for hostile deployments where physical security may not be assured. Alcatel-Lucent APs do not store encryption keys, passwords, or other configuration information. If physical access to the AP is obtained or if it is physically taken off the network, there is no risk of information exposure.

Also apply if wireless point-of-sale applications are implemented

REQUIREMENT 4.1.1: ENCRYPT WIRELESS LINK CARRYING CREDIT CARD DATA

For wireless networks transmitting cardholder data, encrypt the transmissions by using Wi-Fi protected access (WPA or WPA2) technology, IPSEC VPN, or SSL/TLS. Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN. If WEP is used, do the following:

- Use with a minimum 104-bit encryption key and 24 bit-initialization value
- Use ONLY in conjunction with Wi-Fi protected access (WPA or WPA2) technology, VPN, or SSL/TLS
- Rotate shared WEP keys quarterly (or automatically if the technology permits)

This requirement specifies the need to encrypt credit card data when transmitted across wireless networks, which occurs when wireless point-of-sale applications are implemented.

Alcatel-Lucent OmniAccess Wireless solution*:* Alcatel-Lucent OmniAccess Wireless supports all listed encryption protocols simultaneously, and agrees with the recommendation not to trust WEP alone. Alcatel-Lucent specifically recommends against the use of WEP because of security concerns, but recognizes that the base of installed equipment does not always permit the total elimination of WEP. Alcatel-Lucent WLAN switches support multiple authentication and encryption methods, and can permit devices with different capabilities to connect in the most appropriate way. Alcatel-Lucent authentication and encryption capabilities include:

- 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 government and sensitive commercial applications)

REQUIREMENT 7.1 & 7.2: RESTRICT ACCESS BY NEED-TO-KNOW

These requirements pertain to restricting access to data, systems, and networks based on identity and need-to-know.

Limit access to computing resources and cardholder information to only those individuals whose job requires such access.

Establish a mechanism for systems with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

Alcatel-Lucent OmniAccess Wireless solution*:* This closely follows the general security practice of "principle of least privilege." Alcatel-Lucent enforces the principle of least privilege in the network by identifying users or devices, placing them into separate roles, and permitting or denying access to network resources or protocols based on those roles. As described in the section regarding Requirement 1 above, this can mean that a POS terminal is treated differently than a manager on a laptop, a public kiosk, or an employee on a shared-use terminal. Alcatel-Lucent OmniAccess Wireless keeps all traffic logically separate and permits only the access level specifically granted by the administrator based on business needs.

REQUIREMENT 10.3: TRACK AND MONITOR NETWORK ACCESS

Record at least the following audit trail entries for all system components for each event:

- User identification
- Date and time
- Origination of event
- Type of event
- Success or failure indication
- Identity or name of affected data, system component, or resource.

Requirement 10 establishes a baseline for system logging, monitoring, and auditing that must be done.

Alcatel-Lucent OmniAccess Wireless solution: Alcatel-Lucent systems provide detailed audit trails and system logging of all activities on the wireless network. Logs are stored on the system, and may be exported in real-time to one or more syslog servers. Alcatel-Lucent wireless systems can produce the following types of log information:

- A point of sale (POS) device that must send credit card data as well as download inventory and price updates. This device would be limited to communicating with specific servers using specific protocols.
- 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 if available, and the configuration that was changed.
- Wireless attacks and intrusion attempts, including time, MAC address, AP number, and physical location.

Conclusion

The new PCI DSS v1.1 standard imposes a range of new wireless LAN requirements on retailers that accept credit cards. These requirements, which impact firewalls, anti-virus software, encryption methods and more, are designed to enhance credit card security and minimize fraud. Alcatel-Lucent has a comprehensive plan in place to enable retailers to use its OmniAccess Wireless product line to meet these requirements.

About Alcatel-Lucent

Alcatel-Lucent (Euronext Paris and NYSE: ALU) provides solutions that enable service providers, enterprises and governments worldwide, to deliver voice, data and video communication services to end-users. As a leader in fixed, mobile and converged broadband networking, IP technologies, applications, and services, Alcatel-Lucent offers the end-to-end solutions that enable compelling communications services for people at home, at work and on the move. With operations in more than 130 countries, Alcatel-Lucent is a local partner with global reach. The company has the most experienced global services team in the industry, and one of the largest research, technology and innovation organizations in the telecommunications industry. Alcatel-Lucent achieved adjusted proforma revenues of Euro 18.3 billion in 2006 and is incorporated in France, with executive offices located in Paris. [All figures exclude impact of activities transferred to Thales]. For more information, visit Alcatel-Lucent on the Internet: http://www.alcatel-lucent.com

www.alcatel-lucent.com

Alcatel, Lucent, Alcatel-Lucent and Alcatel-Lucent logo are trademarks of Alcatel-Lucent. All other trademarks are the property of their respective owners. The information presented is subject to change without notice. Alcatel-Lucent assumes no responsibility for inaccuracies contained herein.
© 2007 Alcatel-Lucent. All rights reserved. 031942-00 Rev B 9/07