A SPECTRALINK WHITE PAPER

Executive Summary

The focus of this white paper is to provide guidance on achieving PCI DSS compliance for wireless LANs (WLANs) using Spectralink handsets to run VoWLAN. VoWLAN is defined as "the use of a wireless broadband network for the purpose of vocal conversation, using Wi-Fi or the IEEE 802.11 standard network and wireless access points. Within the six main objectives and 12 requirements of PCI DSS, there are many technical implications for wireless LANs and many best practices that should be considered. However, PCI DSS does provide the flexibility to its constituents to segment their networks through the use firewalls, subnets, and Virtual Private Networks (VPNs) so that the entire network is not subject to its requirements. This segmentation can reduce the cost, scope, and difficulty of implementing DSS.

Introduction and Background

The PCI Security Standards Council (PCI SSC) was formed in December, 2004 and the associated companies released PCI DSS. PCI DSS evolved from five different programs: The Visa Card Information Security Program, the MasterCard Site Data Protection, American Express Data Security Operating Policy, the Discover Information and Compliance, and the JCB Data Security Program. The reconciliation of and compliance with five different programs posed challenges for many merchants, so the creation of a single, consistent, and comprehensive standard was welcomed by the industry.

The intent of PCI DSS is to prevent credit card fraud, hacking, and identity theft, all of which can arise from underlying security vulnerabilities. It was "developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally." Companies that store, process and/or transmit credit card data are subject to these standards. Unlike the Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA) or the Sarbanes-Oxley Act, PCI DSS is not a state/federal law or regulation for data security; rather it is a standard developed by the major credit card companies. Failure to comply can result in fines and/or the possibility of losing the ability to have credit card transactions processed. Version 1.2 was issued October 1, 2008.

The Data Security Standard (DSS) consists of 6 main objectives and 12 requirements:

PCI Data Security Standard High-Level Overview

Build and Maintain a Secure Network

- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management

- Requirement 5: Use and regularly update anti-virus software
- Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- Requirement 7: Restrict access to cardholder data by business need-to-know
- Requirement 8: Assign a unique ID to each person with computer access
- Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

- Requirement 12: Maintain a policy that addresses information security

Exploring the PCI DSS

The PCI-DSS requirements referenced below are specifically oriented toward Spectralink VoWLAN implementations in the context of PCI DSS compliance. Users of Spectralink solutions should give strong consideration to these requirements, however, only the technologies and procedures which are relevant to DSS and specific to VoWLAN have been referenced in the section below.

Requirement 1

Section 1.2.3

- Install perimeter firewalls between any wireless network and the cardholder data environment. Configure these firewalls to deny or control any traffic from the wireless environment into the cardholder data environment.

Requirement 2

Section 2.1.1

- Change vendor defaults for items such as encryption keys, passwords, and Simple Network Management Protocol (SNMP) community strings.
- Implement strong encryption for authentication and transmission on the wireless Local Area Network (LAN).
- Firmware on wireless Local Area Network (LAN)should support strong encryption for authentication over wireless networks Wi-Fi Protected Access (WPA or WPA2).
- Change encryption keys anytime anyone with knowledge of the keys leaves the company or changes positions.

Section 2.3
- Encrypt all non-console administrative access through the use of technologies such as secure shell (SSH), virtual private network (VPN), secure sockets layer (SSL), transport layer security (TLS). This rule ostensibly applies to administrative systems that are connected to the sensitive cardholder data portion of the virtual LAN (VLAN). If the network is properly segmented (as defined below) through the use of VPNs, then encrypted connections to administrative consoles should not be necessary.

If the network is properly segmented through the use of VPNs, then encrypted connections to administrative consoles should not be necessary.

Requirement 3

Sections 3.5 and 3.6

- Protect/store encryption keys against disclosure and misuse. Restrict access to keys the fewest number of administrators possible. Store the keys securely and in the fewest locations possible. Fully document key management processes and procedures.
- Generate strong cryptographic keys. A key length of 80 bits is generally considered the minimum for strong security with symmetric encryption algorithms. 128-bit keys are commonly used and considered very strong.[1]
- As deemed necessary, rotate the cryptographic keys. PCI recommends at least annually rotating your keys. Retire/replace old keys or keys which may be compromised through revocation and destruction.
- Require key custodians to sign a for[1]m stating that they understand the responsibilities of a key custodian.

Requirement 4

Section 4.1.1

- Ensure wireless networks transmitting card data or connected to cardholder data use industry best practices to implement strong encryption and transmission.
    - Wired Equivalent Privacy (WEP) is prohibited on new wireless LANs after 3/31/2009 and current wireless LANs after 6/30/2010.
    - Use the IEEE standard 802.11i

Requirement 8

Section 8.3, 8.4, and 8.5

- Use technologies such as RADIUS to ensure network authentication
- Render all passwords unreadable during transmission and storage on all system components using strong cryptography.

Requirement 9

Section 9.1.3:

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

Requirement 11

Section 11.1:

- Test for the presence of wireless access points by using a wireless analyzer at least quarterly. Identify all wireless devices in use. Run internal and external network vulnerability scans at least quarterly.

> Generate strong cryptographic keys. A key length of 80 bits is generally considered the minimum for strong security with symmetric encryption algorithms.

---

1   1 http://en.wikipedia.org/wiki/Cryptographic_key

- Perform penetration testing at least once a year and after any significant infrastructure or application upgrade. Include a network-layer penetration test and an application layer penetration test.
  - The test(s) should be performed by a qualified internal resource or external third party.
  - Use intrusion detection/prevention systems to monitor all traffic and alert personnel to potential compromises.
  - Keep intrusion detection engines up-todate.
- Ensure that responses to alerts are covered in an Incident Response Plan.

Minimizing Scope and Complexity of DSS Implementation

Scope and Segmentation

PCI DSS security requirements apply to all "*system components*." In this context, system components are defined as "any network component, server, or application that is included in or connected to the cardholder data environment."

"The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data."

"Network components include but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Server types include, but are not limited to the following: Web, application, database, authentication, mail, proxy, network time protocol (NTP), and domain name server (DNS). Applications include all purchased and custom applications, including internal and external (Internet) applications."

According to DSS, "network segmentation of, or isolating (segmenting), the cardholder data environment from the remainder of the corporate network is not a PCI DSS requirement. However, it is recommended as a method that may reduce:

- The scope of the PCI DSS assessment
- The cost of the PCI DSS assessment
- The cost and difficulty of implementing and maintaining PCI DSS controls
- The risk to an organization (reduced by consolidating cardholder data into fewer, more
- controlled locations)"

The PCI authors of DSS are providing latitude here to reduce the scope, cost, and resulting complexity of the implementation of the standard for their constituents.

The DSS goes further to state that:

"Without adequate network segmentation (sometimes called a "flat network") the entire network is in scope of the PCI DSS assessment."

With this statement, the authors for PCI SSC are giving their constituents ways to architect the network so that the entire network is not subject to the requirements of DSS. In fact, the authors of the DSS additional definitive statements on network configuration:

Perform penetration testing at least once a year and after any significant infrastructure or application upgrade. Include a network-layer penetration test and an application layer penetration test.

"Network segmentation can be achieved through internal network firewalls, routers with strong access control lists or other technology that restricts access to a particular segment of a network."

"If wireless technology is used to store, process, or transmit cardholder data (for example, point-ofsale 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…."

The conclusion to draw from these preceding statements is that through the use of firewalls, subnets, and VPNs with strong authentication and access control, a network can be segmented so that the entire network is not subject to DSS.

Through the use of firewalls, subnets, and VPNs with strong authentication and access control, a network can be segmented so that the entire network is not subject to DSS.
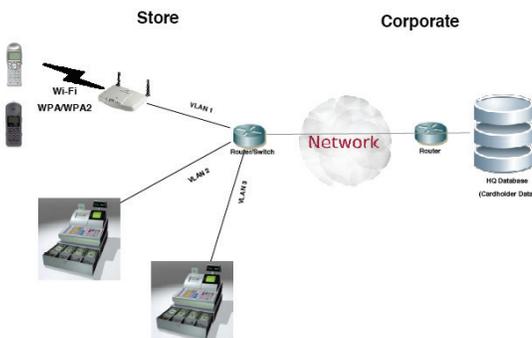
As a current or potential user of a VoWLAN and a site considering PCI-DSS compliance, the basic assessment questions you should ask are:

- *Is my wireless LAN being used to transmit cardholder data?*
- *Do I use my wireless telephones to communicate cardholder data?*
- *Is my wireless LAN connected to the cardholder data environment (that is, not segmented)?*

If the answers to these questions are all "no," then it is likely that the entire scope of PCI DSS does not apply to your VoWLAN traffic. In particular, your VoWLAN end-points should be compliant provided that you have implemented WPA/WPA2. You will want to ensure that you have made the security modifications (specified below in Section 5) to your Spectralink infrastructure.

If your answer to either the first or third question is "yes," then the deployment of a firewall, subnet, or VLAN separating the VoWLAN traffic from the cardholder data environment is recommended as the most practical way to reduce the scope of PCI compliance.

If you answered "yes" to the second question above, then Spectralink recommends that you use strong encryption and authentication (WPA/WPA2) on the access point and that you properly segment your network in order to achieve PCI DSS compliance.

Deploying Spectralink Technologies for PCI DSS Compliance

Current and prospective users of Spectralink VoWLAN should be aware of the following features native to the Spectralink Wi-Fi handsets and corresponding infrastructure. These technologies should be considered and enabled for DSS compliance, when applicable.

Wi-Fi Handset

WEP with 40 bit and 128 bit key lengths. WEP is intended to provide the same level of security over a wireless LAN as on a wired Ethernet LAN. Please note that WEP is prohibited by the PCI on new wireless LANs after March 31, 2009 and current wireless LANs after June 30, 2010.

WPA/WPA2 – The implementation of WPA/WPA2 on the access point prevents hacking into and exposure of the entire network. The Spectralink phones use 802.11i and Temporal Key Integrity Protocol (TKIP) for dynamic key encryption and mutual authentication with WPA. When WPA2 is enabled, the phones use Advanced Encryption Standard (AES) for encryption of the voice conversation. The deployment of either WPA or WPA2 requires phone to authenticate using one of the following methods:

- Pre-Shared Key (PSK) for "personal mode"
- Enterprise mode: 802.1X for radius authentication onto the wireless LAN
- The Supplicant (EAP) types used in conjunction with Radius authentication are:
    - EAP-Fast with OKC
    - PEAP v0 with OKC
    - PEAP v0 with CCKM

Handset Administration Tool (HAT)

HAT is the administrative application used to manage the phone. When making any modification to the phone, such as changing the WPA/WPA2 PSK on a handset from HAT, a USB connection is required, thus there is no danger in exposing the Pre-shared Key (PSK) in clear text over a TCP/IP network. Access to this management application is restricted through the use of a user name and password. The password is stored in an encrypted format using a proprietary stream cipher. It uses this same encryption scheme for the transmission of the password to the handset. Spectralink recommends that the factory default user name(s) and password(s) are changed.

Spectralink Infrastructure

Spectralink infrastructure (including Spectralink Voice Priority (SVP) server, gateways, and Open Application Interface (OAI) server) occasionally require administrative access for periodic management in which user name and password is used in a Telnet session. The password is stored in an encrypted format using an MD5 hash. Spectralink recommends that the factory default user name(s) and password(s) are changed. If the wireless LAN is properly segmented as described above, then encrypted connections to Spectralink Infrastructure via technology such as SSH to administrative consoles should not be necessary for PCI DSS compliance since there is no sensitive data accessible within that VLAN. Even if Spectralink customers cannot segment their network, there is no root level access to the infrastructure devices so a perpetrator could not perform any malicious acts with access to one of these infrastructure devices. Also note that the Spectralink infrastructure devices do not store IP packets, so assuming VoWLAN is used for transmission of credit card data, so there is no sensitive data stored on an SVP, OAI, or a gateway.

> Spectralink infrastructure devices do not store IP packets, so assuming VoWLAN is used for transmission of credit card data, so there is no sensitive data stored on an SVP, OAI, or a gateway.

Trivial File Transfer Protocol (TFTP) Server

A TFTP server is used for over-the-air firmware updates to the various handsets. The TFTP application should ideally be placed on a server with SSH access for secure management. Spectralink customers should minimize the amount of time the new TFTP image is on the gateway. Ideally, this new firmware image would be resident on the TFTP server for less than one day. It is recommended that Spectralink customers remove the code at the end of the transition process at each store.

Conclusion

The intent of the PCI DSS is to prevent credit card fraud, hacking, and identity theft which can arise from underlying security vulnerabilities. DSS does provide the flexibility to its constituents to segment their networks through the use firewalls, subnets, and Virtual Private Networks (VPNs) so that the entire network is not subject to its requirements. This segmentation can reduce the cost, scope, and difficulty of implementing DSS. Through the proper configuration and design of the Spectralink Voice over wireless LAN solution, it is possible to comply with the Payment Card Industry Data Security Standard (PCI DSS).

Note: Please seek full legal advice on PCI-DSS compliance as well as the security aspects of the safe transmission and retention of sensitive cardholder data. This white paper does not constitute legal advice nor is it intended to be a comprehensive review of the DSS. The PCI has not reviewed nor does it endorse this document.

About Spectralink

Spectralink, a global leader in wireless solutions, solves the everyday problems of mobile workers through technology, innovation and integration that enable them to do their jobs better. By constantly listening to how customers move through their workdays, Spectralink is able to develop reliable, enterprise-grade voice and data solutions and deliver them through a powerful, durable device.

Spectralink
2560 55th Street
Boulder, CO 80301
Tel: +1 800 775 5330
info@spectralink.com
spectralink.com