

PCI's Peripheral Issues

How PCI DSS v1.1. applies to wireless printers and how they can comply




A ZEBRA WHITE PAPER



**Copyrights**

©2008 ZIH Corp. ZebraCare, ZebraLink and all product names and numbers are Zebra trademarks, and Zebra, the Zebra head graphic and ZebraNet are registered trademarks of ZIH Corp. All rights reserved. Wi-Fi is a registered trademark of the Wireless Ethernet Compatibility Alliance, Inc. Motorola is a trademark of Motorola, Inc., registered in the U.S. Patent & Trademark Office. Cisco is a registered trademark of Cisco Systems, Inc. Wavelink Avanzancho is a registered trademark of Wavelink Corporation. All other trademarks are the property of their respective owners.

Unauthorized reproduction of this document or the software in the label printer may result in imprisonment of up to one year



Executive Summary

The challenges of meeting Payment Card Industry (PCI) security standards and the horror stories of not doing so are well known: security breaches at several major retailers have resulted in estimated costs of as high as \$1 billion per retailer; the U.S. Identity Theft Protection Act has established fines of up to \$11,000 per customer record for databases breaches; 14 percent of retailers have suffered a breach and only 28 percent of retailers are fully compliant with PCI requirements, according to the Retail Systems Alert Group 2006-2007 Retail Data Security study; and merchants who do not comply are at risk for fines, higher processing fees and even the loss of card-processing privileges. PCI costs are a major concern for many businesses, even if the cost of non-compliance is potentially so much higher.

Amid these concerns it is easy for retailers to lose site of both the big picture and important details. PCI compliance is a major milestone, but it is only a means to an end of having secure processes, networks, data, devices and peripherals. If a single networked device is non-compliant, the entire network and the retail information systems behind it are all non-compliant. That's why protecting peripherals is an essential, if somewhat overlooked, component of PCI compliance.

This white paper explains how PCI Data Security Standard (DSS) version 1.1 applies to wireless peripherals and presents options for including secure wireless printers in PCI-compliant wireless networks.

Introduction

Many retailers are unwittingly out of compliance with PCI DSS v1.1 because they don't realize its scope, particularly how the standard applies to peripherals. Because of the tougher new wireless security requirements included in PCI DSS v1.1, many wireless computers, printers and other peripherals retailers use every day do not comply.

There is no reason for a printer to be a weak link in wireless network security. Wireless printers can support PCI requirements and other advanced protocols and strategies used to protect mobile computers, POS stations and other wireless devices. Supported security includes 802.11i, 802.1x, LEAP, WPA and WPA2 security protocols. Wireless printers support AES, IPSec, SSL and other advanced encryption and authentication protocols, and can be included in virtual private networks (VPNs).

How PCI Applies to Printers

One of the biggest changes from PCI version 1 to version 1.1 is required support for WPA or WPA2 wireless security standards, or an Internet protocol security (IPsec) based virtual private network (VPN). WPA is the commonly used acronym for Wi-Fi Protected Access, a security protocol that provides data encryption and device authentication for 802.11-standard (Wi-Fi®) wireless networks. The WPA2 standard was developed later and provides even stronger security. Many older wireless devices used in retail today lack the processing power to effectively run WPA2. More legacy devices can run WPA, although not all retailers have installed it. Peripheral support for VPNs is even rarer.

Failure to support WPA or WPA2 is a leading reason many retail wireless networks aren't in PCI compliance, but it is not the only one. There are 12 major requirements that all must be met to comply with PCI DSS v1.1. The most relevant requirements, and tips for meeting them, are presented below.



PCI DSS v1.1 Requirement 2—Do not use vendor-supplied defaults for system passwords and other security parameters.

At one time, it was common to deploy wireless LANs secured with default passwords and security configurations, but this practice has largely been abandoned in favor of more secure methods. To comply, activate security settings during installation (some systems default to security turned off), and create original passwords. Older systems should be reviewed to make sure they are compliant.

Requirement 4—Encrypt transmission of cardholder data across open, public networks.

PCI considers wireless LANs to be public networks. Internet and cellular transmissions are also covered by this requirement, which therefore applies to merchants who wirelessly process payments for delivery, service, home sales and other remote commerce. WPA, WPA2, 802.1x, 802.11i and other standard wireless LAN security protocols provide data encryption, as do wide-area cellular networks.

4.1—Use strong cryptography and security protocols such as secure sockets layer (SSL)/transport layer security (TLS) and Internet protocol security (IPsec) to safeguard sensitive cardholder data during transmission over open, public networks.

This requirement applies to wired and wireless, stationary and mobile, and local or Web communications over public networks. Support for SSL, TLS and IPsec is available for wireless printers. Pay careful attention to specifications because there are different varieties of these protocols (e.g., EAP, LEAP, PEAP), so compatibility with the network infrastructure is not assured.

4.1.1—Never rely exclusively on wired equivalent privacy (WEP) to protect confidentiality and access to a wireless LAN.

WEP can be used if WPA, WPA2 or a VPN is also deployed. If WEP is used, do the following: use with a minimum 104-bit encryption key and 24 bit-initialization value; rotate shared WEP keys at least quarterly and whenever there are changes in personnel with key access; and restrict access to MAC addresses. Most of these requirements can effectively be addressed during system configuration.

Other requirements of PCI DSS v1.1 relate to networks, applications and IT infrastructure, so printers and other peripherals must be compatible with enterprise IT policies and standards. Additional PCI components that may impact printers include: Requirement 1—Install and maintain a firewall to protect cardholder data; Requirement 6—Develop and maintain secure systems and applications; Requirement 8—Assign a unique ID to each person with computer access; Requirement 10—Track and monitor all access to network resources and cardholder data; Requirement 11—Regularly test security systems and processes; and Requirement 12—Maintain a policy that addresses information security.

Meeting all these requirements may seem complex and burdensome, but in fact it is quite manageable. Many retailers have complied with PCI DSS v1.1 and use wireless printers for shelf labeling, markdown management, stock keeping, returns processing, assisted shopping, portable POS and other applications every day. None of the PCI DSS v1.1 wireless requirements call for products or technologies that haven't been developed. In fact, securing wireless printers may be one of the easier aspects of PCI compliance because products are already available that support the necessary security protocols. Plus, automated management applications are available to reduce much of the traditional configuration and upgrade time requirements and costs, especially for remote devices. The following sections describe specific security capabilities and management options for wireless printers from Zebra Technologies.

Security Options for Zebra® Wireless Printers

Zebra Technologies provides flexible, standard and current security solutions that can be implemented on mobile, tabletop and cart-mounted printers. Many models support WPA, WPA2 and other PCI requirements and are also fully compatible with LEAP and other security protocols used in 802.11b/g wireless networks from Cisco Systems, Motorola (Symbol Technologies) and other providers.

Different security levels and protocols can be implemented in each type of Zebra printer—mobile, tabletop and cart-mounted. The exact security available depends on the printer model, connection method and radio model used. Support referenced in this white paper applies only to radios tested and approved by Zebra for use with its printers. Security support is frequently updated, so check www.zebra.com or speak with a Zebra representative for the most current information. Mobile models work on wireless networks through integrated radios, while cart-mounted and stationary wireless printers use a print server for access to the wireless network.

Table 1 summarizes the security available for Zebra wireless printers.

Table 1: Quick Reference to Wireless Security Available for Zebra Printers

	QL Plus™, RW™	QL Plus, RW, MZ™, PS4000™	GX™ series, HC100™	XIIIPlus™, 105SL™, PAX4™, S4M™, ZM400™, ZM600™		
WLAN-SECURITY	Motorola® Symbol 11b (LA-4137 CF)	Zebra 802.11b/g	Zebra 802.11b/g	Motorola® Symbol 11b (LA-4137 CF)	Cisco® 802.11b/g (CB21)	Zebra 802.11b/g
WEP	YES	YES	YES	YES	YES	YES
IEEE 802.1X Authentication schemes						
LEAP	YES	YES	YES	YES	YES	YES
EAP-FAST	YES	YES	YES	YES	YES	YES
PEAP	YES	YES	YES	YES	YES	YES
EAP-TLS	YES	YES	YES	YES	YES	YES
EAP-TTLS	YES	YES	YES	YES	YES	YES
(WPA) Wi-Fi protected Access: 802.1X + WPA TKIP						
with LEAP	YES	YES	YES	YES	YES	YES
with EAP-FAST	YES	YES	YES	YES	YES	YES
with PSK (Pre-shared Key)	YES	YES	YES	YES	YES	YES
with PEAP	YES	YES	YES	YES	YES	YES
with EAP-TLS	YES	YES	YES	YES	YES	YES
with EAP-TTLS	YES	YES	YES	YES	YES	YES
IEEE 802.11i =(WPA2):802.1X + AES encryption						
w/PSK, EAP-TLS, EAP-TTLS, LEAP, PEAP, EAP-FAST	NO	YES	YES	NO	YES	YES
Airbeam Safe-VPN	YES	YES	NO	NO	NO	NO



Managing Security on Zebra Printers

Wireless security is dynamic, with new standards and protocols being developed and gaining support from leading equipment manufacturers. Wireless infrastructures—including printers and their management tools—must be flexible enough to facilitate change so users can easily implement the latest upgrades and options to optimize their network security.

Zebra offers powerful management options that make it simple to deploy, monitor, configure and upgrade security protocols on Zebra printers, such as ZebraNet™ Bridge Enterprise. Select Zebra mobile printers can also be managed with Motorola's Mobility Services Platform (MSP) and Wavelink Corp.'s Avalanche software—both provide a complete management environment for multiple types of wireless devices from different manufacturers.

Using ZebraNet Bridge Enterprise, Motorola MSP or Wavelink Avalanche® network management utilities, system administrators can remotely implement software updates and security upgrades, configure devices and modify settings. With these tools and Zebra wireless printers, IT administrators can maintain complete visibility and control over the devices from a single, remote console—without ever having to physically touch the printers. The ability to effectively manage and secure all types of mobile devices from a single point significantly reduces the support costs across an enterprise's wireless network.

Conclusion

In the major effort to bring data centers and enterprise systems into PCI compliance, it's easy to overlook a legacy stock keeping or shelf labeling application at a distant store. But it only takes one oversight to put your entire system, your customers' data, and your merchant status at risk. Protecting wireless printers is necessary for PCI compliance, but it isn't necessarily difficult because of the advanced security and support available.

Zebra has numerous wireless printers, networking tools and management resources to help retailers meet their security and business needs. Retailers around the world rely on Zebra printers as part of efficient and innovative customer service, transaction processing, shelf management, inventory control, markdown and other operations. Visit www.zebra.com/retail to learn more and to download additional white papers and case studies on retail, wireless and security topics.

Zebra Technologies Corporation (NASDAQ: ZBRA) helps companies identify, track and manage assets, transactions and people with on-demand specialty digital printing and automatic identification solutions. In more than 100 countries around the world, more than 90 percent of Fortune 500 companies use innovative and reliable Zebra printers, supplies, RFID products and software to increase productivity, improve quality, lower costs and deliver better customer service. Information about Zebra and Zebra-brand products can be found at <http://www.zebra.com>.



Notes



GLOBAL/AMERICAS

HEADQUARTERS

Zebra Technologies Corporation
333 Corporate Woods Parkway
Vernon Hills, IL 60061-3109 U.S.A.

T: +1 847 793 2600 or
+1 800 423 0442
F: +1 847 913 8766

EMEA HEADQUARTERS

Zebra Technologies Europe Limited
Zebra House, Unit 14,
The Valley Centre
Gordon Road, High Wycombe
Buckinghamshire HP13 6EQ, UK

T: +44 (0)1494 472872
F: +44 (0)1494 768251

ASIA-PACIFIC HEADQUARTERS

Zebra Technologies Asia Pacific, LLC
120 Robinson Road
#06-01 Parakou Building
Singapore 068913

T: +65 6858 0722
F: +65 6885 0838

OTHER LOCATIONS

USA

California, Georgia, Rhode Island,
Texas, Wisconsin

EUROPE

France, Germany, Italy, Netherlands,
Poland, Spain, Sweden

ASIA-PACIFIC

Australia, China, Japan, South Korea

LATIN AMERICA

Florida (USA), Mexico

AFRICA/MIDDLE EAST

India, Russia, South Africa,
United Arab Emirates