

## Wireless LAN Security Best Practices and PCI Compliance

This paper describes how best practices for wireless LAN security help businesses meet compliance requirements for the payment card industry (PCI) data security standard.

### Summary

Wireless LANs are a core component of most corporate network infrastructure. With a naturally mobile workforce, industries including retail, hospitality, gaming and restaurants were among the first to realize that a real-time network connection for roaming employees could bring greater efficiency. Wireless LANs have long been used to provide instant visibility into inventory positions, enable easy reconfiguration of point of service (POS) systems, provide information kiosks for customers, and deliver voice services directly to employees or store associates. Any business that handles credit card data must comply with the requirements of the Payment Card Industry (PCI) Data Security Standard.<sup>1</sup> This compliance includes the need to secure the wireless network. However, even if these industries do not have a wireless LAN, factors such as the prevalence of the technology in neighboring homes and businesses, as well as its easy availability and low cost, require them to put in place proper security practices. Proper security practices are essential to ensure that unauthorized wireless LANs are not introduced into the network, potentially causing a violation of the PCI standard or creating a security breach. The good news for IT managers is that when properly deployed—and built upon a foundation of strong wired network security—wireless LANs are as secure as wired networks. While PCI affects any company handling credit card information, this paper focuses on the retail industry given the sheer number of credit card transactions handled. This paper presents best practices for wireless LAN security and the prevention of wireless threats.

### Challenge

While retail IT administrators may already be aware of the proper techniques for securing the wireless LAN using 802.11i, they may be surprised to learn that this alone is not enough to protect the retail network and meet PCI requirements. Whether a retailer has an authorized WLAN or a “no Wi-Fi” policy, it is important to be aware of the vulnerability of the hardwired corporate network to security threats from wireless network sources.

The most common of these security threats is the rogue access point. Eager employees often bring in their own access points—typically consumer-grade and very low-cost devices—to speed wireless connectivity in their department, unaware of the dangers these devices pose. These rogue access points are behind the firewall and cannot be detected by traditional wired network intrusion detection or prevention systems (IDS/IPS). Anyone within range of the signal can attach and access the corporate network. Unfortunately, retailers may also be a target for malicious

---

<sup>1</sup> In 2005, Visa, MasterCard, and other major credit card companies created the Payment Card Industry (PCI) Data Security Standard to protect sensitive cardholder information. The PCI standard sets high data security expectations and compliance requirements for merchants and service providers that process, store, or transmit cardholder data. It includes 12 conditions that retailers, online merchants, data processors, and other businesses that handle credit card data were required to meet by June 1, 2005. The standard sets technology requirements such as the use of data encryption, end-user access control, and activity monitoring and logging. It includes procedural mandates such as the need to implement formal security policies and vulnerability management programs.

hackers. The temptation of consumer credit card information may prompt attacks directed against the retailer with the goal of obtaining this information illegally. Such threats must be considered real and defended against.

A further complication is the new reality of mobile workers requiring access to the corporate network when they are away from the office. Employees regularly conduct business from home, hotels, airports, and other wireless hotspots. These “unmanaged sites” can act as a conduit for events that compromise the corporate network, first because laptops risk contracting viruses, spyware, and malware, and second, because wireless clients can connect to wireless access points or other wireless clients without the user’s knowledge.

### **Solution**

As a component of the Cisco® Intelligent Retail Network, the Cisco Unified Wireless Network provides a comprehensive solution for both protecting the wired network from wireless threats as well as for ensuring secure, private communications over an authorized wireless LAN. Every device in the network—from clients to access points to wireless controllers and the management system—plays a part in securing the wireless network environment through a distributed defense. This extension of Cisco’s Self-Defending Network strategy protects against the new threats to retail networks posed by wireless technologies.

### **Building a Strong Foundation to Meet the PCI Requirements**

The increasingly mobile nature of enterprise communications means that a multilayered approach to enterprise security is required. To mitigate risks from wireless threats, Cisco recommends the following approach to securing the retail wireless and wired network:

- Create an information security policy that includes the wireless LAN.
- Secure the retail wireline (Ethernet) and authorized wireless LAN against wireless threats.
- Defend the cardholder information from theft or tampering.
- Enlist employees in safeguarding the cardholder information.

By following this approach, retailers will meet most if not all the PCI requirements as they relate to wireless LANs and protect both the cardholder information and the retail network from wireless threats.

### **Create an Information Security Policy that includes the Wireless LAN**

The PCI standard incorporates security policy and documentation throughout. Retailers need a wireless security policy document that covers authorized use and security measures. Many templates already exist for the specific sections that should be covered in the written security policy. Typically, security policy documents include the following sections:

- Purpose
- Scope
- Policy
- Responsibilities
- Enforcement
- Definitions
- Revision History

If a company does not deploy wireless technology, it is still wise to include wireless in the information security policy. Stating that wireless is not deployed and what the enforcement action will be if wireless devices are detected on the network is strongly recommended. PCI Requirement 11 mandates that companies must scan for wireless devices, whether or not wireless technology is deployed.

### **Secure the Retail Wireline and Authorized Wireless LAN Against Wireless Threats**

#### **Secure the Authorized Retail Wireless LAN**

Several areas in the PCI standard address securing wireless, such as PCI requirements 2, 4, and 11. Confidential communications is one of the characteristics of the Cisco Self-Defending Network strategy. Applying this to a wireless LAN is not hard—industry advances in technology and the Cisco Unified Wireless Network make this easier than ever, as the following sections explain.

#### **Confidential Communications**

Requirement 2 says: “Do not use vendor-supplied defaults for system passwords and other security parameters”. Requirement 4 says: “Encrypt transmission of cardholder and sensitive information across public networks.” These requirements are directly addressed by implementing WPA for the authorized wireless LAN. This standard enables accurate identification of authorized clients and infrastructure through the 802.11i standard. IEEE 802.11i ensures that users accessing the network have a unique username and password, thus supporting PCI Requirement 8, which requires unique user ids. Ensuring that the network can be used only by those who have proper credentials is the first important step towards restricting access. Requirement 4 is also addressed through the use of WPA. The Cisco Unified Wireless Network supports WPA which uses Advanced Encryption Standard (AES) encryption, the highest level available.

#### **Segmenting Users to Appropriate Resources**

Wireless LANs are multi-use, with many different types of users requiring access to the wireless LAN. As an example, warehouse personnel require access to the order entry and shipping systems, while store managers may require access to sales performance data. To ensure appropriate controls are in place to restrict data to business need-to-know, the Cisco Unified Wireless Network also provides the ability to restrict users' access to network resources based on their identity, using the virtual LAN (VLAN) capability. Although all users are on the same wireless LAN infrastructure, specific resources can be assigned to a VLAN such that warehouse personnel can access only e-mail and enterprise resource planning (ERP) systems, while store managers have additional privileges to view store sales data.

Many corporations may use bar code scanners for inventory tracking in shipping and receiving or mobile printers on manufacturing floors. And as voice over wireless LAN gains popularity, Wi-Fi phones are becoming more prevalent. These types of devices often do not support the IEEE 802.11i or Wi-Fi Protected Access (WPA) security standards, supporting instead the less secure Wired Equivalent Privacy (WEP) encryption standard.

#### **Using Security Strategies for Business-Specific Clients**

Cisco understands that most retail environments require the use of business-specific clients such as bar code scanners or mobile printers that may not yet support 802.11i. In this situation, using WPA or a VPN for these devices is the next best option, and is also required by the PCI standard. This approach, combined with network segmentation using VLANs, provides a very robust solution for networks with varied clients, and is also inline with the PCI requirements.

If none of these methods are possible, it is advisable to configure WEP. Per PCI requirement 4, WEP alone cannot be used as an encryption method for the transmission of sensitive cardholder data and Cisco does not recommend this security method for any application that transmits cardholder data over a wireless LAN. The methodology will render the network as PCI NON-compliant. However, these devices are common in retail environments for non-cardholder data transmission, such as inventory management applications, and they should be secured to mitigate security risks. These devices can be segregated on a specific VLAN, which allows access only to the specific database or application they are associated with. This, along with frequent encryption key changes and MAC address control lists, mitigates potential security risks.

### **Secure the Wired Retail Network Against Wireless Threats**

Becoming PCI-compliant in the age of wireless networks must include a strategy to protect against unauthorized wireless usage. Because wireless LAN technology is so ubiquitous—found in almost all new notebook computers and available at low cost from all major electronics retailers—it can be easily acquired and used by employees or hackers. Improperly used, wireless technology creates the following threats that can place the business in violation of the PCI requirements:

- **Rogue access points and clients**—An access point installed without the authorization of the IT department. Typically done without malice by employees eager for wireless access, it can provide a direct link to the retail network as it is already behind the firewall. It is also typically not configured to use security. This threat can affect a retailer's compliance with PCI in several areas.
- **Ad hoc networks**—A network that is formed directly between two client devices without going through security checks performed by the infrastructure. Ad hoc networks are dangerous because they can be created without the employee's knowledge while the employee is simultaneously connected to the wired network, allowing potential hackers direct access to the retail network. This threat can also affect a retailer's compliance with PCI Requirement 1 because the client may be behind the firewall.
- **Client misassociation**—An authorized retail wireless client that attaches to a neighboring network. This may occur through an employee intentionally avoiding IT security controls to surf the Internet or use Webmail, or unintentionally if Windows automatically attaches to a wireless network. When client misassociation occurs because Windows automatically attaches to a wireless network, it can create a bridge to the wired retail network if the device is simultaneously connected to the Ethernet network. Like rogue clients and ad hoc networks, client misassociation can affect a retailer's PCI compliance.

The first step in enabling accurate wireless threat detection and prevention is to ensure that authorized wireless infrastructure and users are properly identified to the network. This is done through use of IEEE 802.11i. Without this step, any wireless IDS/IPS will be of little value because administrators will spend much of their time resolving false positives. Once authorized users and infrastructure are identified, the Cisco Unified Wireless Network is able to protect the retailer against common wireless threats.

The Cisco Unified Wireless Network incorporates radio resource management (RRM) to continuously monitor the surrounding air space. Because the Cisco Unified Wireless Network uses a centralized architecture, all managed access points are known. This knowledge, combined with detection of all over-the-air wireless activity, enables the Cisco Unified Wireless Network to immediately identify and prevent rogue access points and ad hoc networks, which supports PCI Requirement 11. Deployment of Cisco Security Agent on wireless endpoints ensures that simultaneous connections to the enterprise wired network and wireless interface is prevented, so that client misassociations do not occur.

#### Protecting Retail Sites That Do Not Have Wireless LAN Coverage

Some retail sites may not have wireless LAN coverage. In some respects, these areas are even more vulnerable to wireless threats as employees may bring in their own access points to gain wireless connectivity. To protect these areas, Cisco Unified Wireless Network lightweight access points can be deployed as dedicated air monitors. Air monitors do not service client traffic, but are solely responsible for monitoring the airwaves. All channels can be scanned and intrusion prevention techniques initiated as necessary to protect the enterprise. PCI Requirement 11 mandates that a company scan for wireless devices at least quarterly.

An advantage of deploying the Cisco Unified Wireless Network versus an overlay wireless IDS system for this situation is that when the retailer is ready to deploy a wireless LAN in these areas, the air monitors can be converted to service wireless clients, or additional access points can be managed by the same controller if the retailer wants to keep a dedicated sensor network for wireless threats. In either case, only one system needs to be deployed, learned, and maintained over time.

#### Defend the Cardholder Information from Theft or Tampering

Like any other enterprise, retail networks are amorphous: no single perimeter exists. Mobile device and broadband access have given rise to mobile workers connecting to the retail network from homes, hotels, airports, and many other places. The retail network must be protected from security threats, such as viruses, worms, and spyware, while these mobile devices are away from the site. Requirement 5, "Use and regularly update anti-virus software or programs," relates directly the need for protection against threats that can be acquired while taking advantage of wireless connectivity. Cisco offers Network Admission Control (NAC) and the Cisco Security Agent to help meet requirement 5.

#### Enlist Employees in Safeguarding the Cardholder Information

Social engineering is often the most effective tool in helping to secure the retail network and in turn, cardholder information. Informational posters and training about security best practices (such as password selection and privacy) can go a long way toward protecting the network—most employees are simply not aware of the risks without education. As an example, the majority of employees would not realize that the simple act of plugging an access point into an Ethernet jack endangers corporate network security.

Table 1 summarizes the PCI requirements, the associated wireless connectivity security risks, and ways to deal with the risks and meet each requirement.

**Table 1.** PCI Requirements and How to Meet Them

PCI Requirement	The Security Risk from Wireless Connectivity	Meeting the Requirement
Requirement 1: Install and maintain a firewall configuration to protect data.	Rogue access points, ad hoc networks and client misassociation can occur behind the firewall, potentially opening up the network and invalidating wired network security protection measures.	Cisco Unified Wireless Network security services prevent wireless threats such as rogue access points and ad hoc networks. In combination with Cisco Security Agent, all of this works to prevent client misassociation.
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	Default WEP keys, SSID, password and community strings can open up easy holes for credit card theft.	The Cisco Unified Wireless Network supports WPA and WPA2 for strong wireless authentication and encryption.
Requirement 4: Encrypt transmission of cardholder and sensitive information across public networks.	Improperly configured access points, rogue access points, ad hoc networks, or client misassociation can leave confidential information at risk of compromise while in transit.	Cisco Unified Wireless Network deployments centralize access point configuration, so local misconfiguration is not possible. Cisco Unified Wireless Network security services prevent wireless threats such as rogue access points and ad hoc networks. In combination with Cisco Security Agent, all of this works to prevent client misassociation.
Requirement 5: Use and regularly update anti-virus software or programs	Mobile devices such as laptops may introduce viruses or other malware into the retail network.	Cisco Security Agent deployed on the client can help prevent introduction of malware or other viruses. Cisco Network Admission Control can enforce security policies when the mobile device returns to the retail network.
Requirement 8: Assign a unique ID to each person with computer access.	Supporting multiple user groups on the same wireless network, wireless kiosk or wireless POS device may put cardholder information at risk.	The Cisco Unified Wireless Network supports multiple VLANs, which logically separate users so that when they use the wireless network, they can access only the resources for which they have permission.
Requirement 11: Regularly test security systems and processes.	Rogue access points, ad hoc networks, and client misassociation create opportunities for unmonitored access to network resources and cardholder data.	Cisco Unified Wireless Network security services prevent wireless threats such as rogue access points and ad hoc networks. It works collaboratively with Cisco IPS systems for dynamic, proactive threat mitigation.

## Summary

Wireless LANs are a core part of most retail network infrastructure. When developing a plan to meet PCI requirements, it is important to take into consideration the unique challenges that wireless connectivity brings. Implementing best practice wireless security techniques brings retailers much closer to meeting PCI requirements. Starting with a wireless LAN policy to explicitly detail the use of wireless is the first step. The next step is using a combination of IEEE 802.11i security along with Cisco Unified Wireless Network security services to defend and prevent against wireless threats. It's also important to ensure that security tools such as firewalls, VPNs and anti-virus software are in place on mobile devices to help prevent threats through wireless connections. Cisco Network Admission Control can monitor compliance with security policies when those devices return to the network, so that security policies can be enforced. Finally, educating employees about the dangers of wireless threats such as rogue access points should help prevent these threats from entering the retail site.



**Americas Headquarters**  
 Cisco Systems, Inc.  
 170 West Taftman Drive  
 San Jose, CA 95134-1706  
 USA  
[www.cisco.com](http://www.cisco.com)  
 Tel: 408 520-4000  
 800 653-1715 (toll free)  
 Fax: 408 527-0689

**Asia Pacific Headquarters**  
 Cisco Systems, Inc.  
 155 Robinson Road  
 #28-01 Capital Tower  
 Singapore 068912  
[www.cisco.com](http://www.cisco.com)  
 Tel: +65 6317 7777  
 Fax: +65 6317 7799

**Europe Headquarters**  
 Cisco Systems International BV  
 Heerlenbergweg 13-19  
 1101 CH Amsterdam  
 The Netherlands  
[www.europe.cisco.com](http://www.europe.cisco.com)  
 Tel: +31 20 620 0791  
 Fax: +31 20 657 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Ring logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access, Register, Abroad, EPC, Catalyst, CSDA, CCIP, CCIE, CCIP/CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Diagnose/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IQS, iPhone, IPTV, IQ Director, the IQ logo, IQ Net, Roadshow, Scorecard, iQuick Study, iStream, iLinksys, iMeeting Place, iMGX, iNetworking Academy, iNetwork Register, iPacket, iPK, iProConnect, iRabbit, iUX, iScriptShare, iVoiceCast, iVARTool, iBackWire, iThe Router, iWay to Increase Your Internet Quotient, and iThreatPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (07012)