The Impact of Wireless LAN Technology on Compliance to the PCI Data Security Standard

339 N. Bernardo Avenue, Suite 200 • Mountain View, CA 94043
www.airtightnetworks.net

THE LEADER IN WIRELESS INTRUSION PREVENTION

Wireless LANs and PCI Compliance

Retailers today use computers and computer networks in three different environments: the office, the store/retail outlet, and the warehouse/distribution center. While the rate of adoption for wireless LAN technology may vary across these environments, WLANs may be present and create security exposures in all three of them.

The Payment Card Industry (PCI) Data Security Standard was created in 2004 to help consumers maintain confidence in the privacy of their personal data and transactions when using credit cards. Compliance is mandatory for all merchants that store, process or transmit credit card data through retail stores, mail order, telephone order and e-commerce.

While there are many qualified third parties that can provide guidance to retailers on their existing security infrastructure and how to achieve PCI compliance, broad knowledge of the security threat from wireless LAN (WLAN) technology may not be well understood by the retail community. However it is understood by organized crime – as they have already funded several attacks on retail networks over wireless links. Unfortunately, this has resulted in several prominent retailers facing losses of customer data, audits and penalties due to wireless LAN security breaches.

Although retailers are extensive users of wireless LAN technology to enable mobility within the store for POS terminals, inventory management and voice, most retail security practices have been focused on securing the authorized wireless LAN, not on protecting against unauthorized WLAN activity. It is this new breed of wireless threats that can compromise a retailer's network that must be understood and defended against. This paper will provide an overview of the wireless threats and suggest strategies to defend against them to ensure PCI compliance is maintained, and more importantly that customer data is secure and customer confidence is maintained.

Network Integrity in the Age of Wireless

Retailers have long been one of the leading users of wireless LAN technology - in retail stores and distribution centers - due to their need to rapidly update inventory positions, regularly reconfigure store layout and POS terminals and provide data and voice connectivity to the large population of mobile employees (store associates, stockers and managers). This usage of wireless technology however also provides opportunities for data loss or theft.

In addition, every office environment today, particularly in major metropolitan areas, is exposed to multiple wireless threats. According to market research firm Current Analysis, over 95% of all laptops purchased in 2006 have built-in WLAN capabilities.

As the vast majority of retailers have mobile office workers – this security exposure cannot be overlooked.

Many retailers have deployed wireless LANs to enable mobility and are aware of the most important security best practice; i.e. using strong encryption and authentication methods such as IEEE 802.11i.

What is less well understood is the danger that unauthorized wireless LAN devices can pose to the integrity of a retailer's network – in stores, distribution centers, and office buildings. Unauthorized WLAN devices can include both access points and clients. Because of the strong consumer demand for wireless LAN technology, WLAN APs and clients are inexpensive and can be purchased by anyone at major computer electronics retailer. Increasingly, wireless clients are standard in notebooks and common in smart phones, printers and even gaming devices.

Because wireless LAN signals travel outside the physical boundaries of buildings, when unauthorized or "rogue" APs are connected to the retailer's Ethernet network (behind the firewall), the retailer's network is compromised. Unfortunately, as unauthorized wireless LAN equipment is typically consumer grade, security is turned off by default. With a few minutes of installation, an insecure wireless signal can create a direct link to your Ethernet network.

Fundamentally, there are two security risks which must be prevented:

- Connections to neighboring wireless LAN networks
- Outsiders connecting to your network via a wireless LAN

Either of these behaviors can result in the loss of customer credit card data, as has already been seen in several large publicized breaches. The next section explains these risks in more detail.

How Wireless Threats Occur

Connections to neighboring wireless LAN networks

The source of this problem is wireless LAN signals from neighboring businesses or homes. Forrester Research reports that over 65% of enterprises in North America have a wireless LAN deployed. And Gartner Group reports that total wireless LAN sales to both enterprises and consumers reached $1.2 billion in 2005 and is expected to grow to $1.6 billion in 2007. With the volume of wireless LAN networks, it's highly likely that multiple neighboring offices, retail stores, or the shopping center has installed open wireless LANs.

Another possible source of an open wireless LAN is a city-sponsored municipal Wi-Fi network. Many cities are deploying these outdoor wireless LANs with no security to encourage visitor use, with the unintended consequence that their signals may reach into a retailer's offices or store premises. If any of these neighboring wireless LANs are not secured, i.e. a user name and password is not required, then any wireless LAN client in a notebook, smart phone or gaming device can attach to these networks. This then provides the user with open, unrestricted access to any site on the Internet, including web-based email. Unscrupulous employees could use this avenue for unauthorized leaking of retailer or customer information without any corporate oversight. Even if the connection is unintentional, if the laptop is also plugged into the wired Ethernet infrastructure at the same time, an unintentional bridge has been created with full access to the retailer's network.

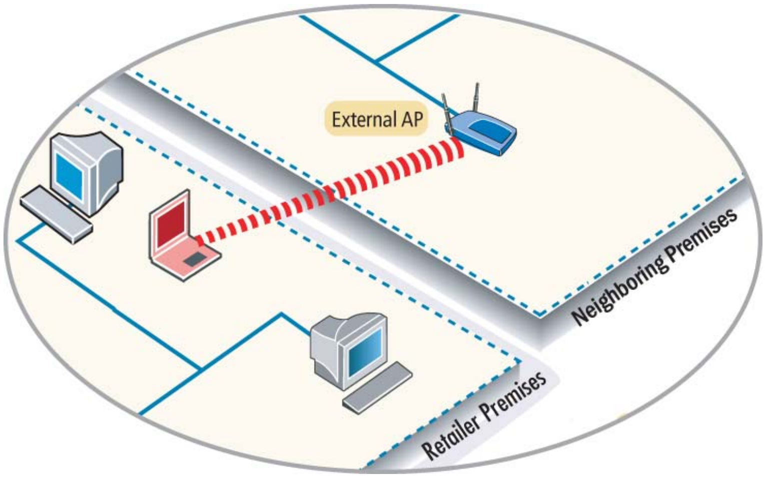

Figure 1: Clients can connect to neighboring wireless LANs and gain unmonitored access to the Internet.

Outsiders connecting to your network via a wireless LAN

Several conditions may exist that allow an outsider access to the wire line network via a wireless LAN. The first occurs if an employee installs their own wireless access point. This is typically done without malice by an employee that wants wireless connectivity in their own work area. Unfortunately, consumer grade access points default to "security off" and thus when connected to the Ethernet network from behind the firewall provide outsiders a direct link in.

Moreover, because of the personal credit card information collected by retailers, they are much more likely to be the target of malicious hacking. One such scenario is the creation of a wireless honeypot. A honeypot is an access point that is configured to be identical to the retailer's wireless LAN. Hacker's can set up the access point in the retailer's parking lot, amplify the signal to attract authorized retail clients to attach to the honeypot access point instead of the authorized retail wireless LAN and collect user name and password information. Once they have successfully gathered this information, the hacker can then log-in (i.e. break in) to the retailer's network as though they were an employee.

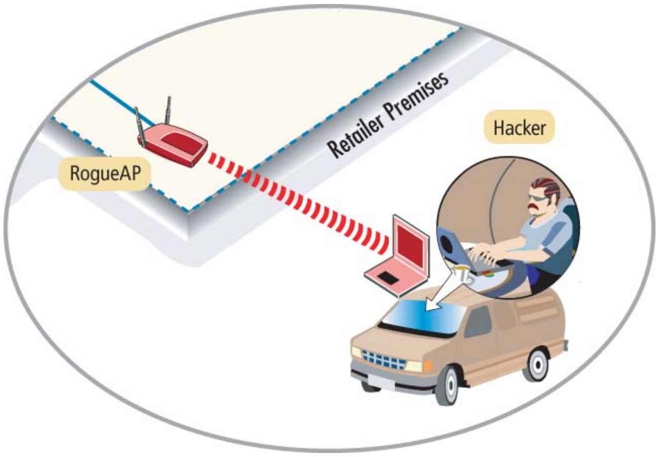

Figure 2: Access points installed without authorization by the IT department can leave a retailer network open to malicious hacking.

Ad hoc wireless networks may also create a security breach. An ad hoc wireless network is formed when two laptop computers form a direct wireless connection to each other. This is very easy to do, as this is a built in functionality in Windows and is turned on by default. If one of the computers is also plugged into the wired Ethernet infrastructure at the same time, the other wireless client has full access to the retailer's network.

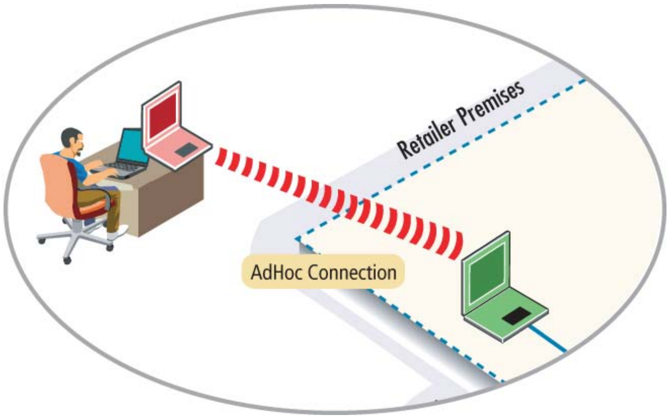

Figure 3: Unintentional ad hoc connections can create a bridge to the retailer network without the employee's knowledge.

So, as an example, someone external to the retailer's premise can set up an ad-hoc connection to an employee's laptop that is connected to the Ethernet network, and see everything on the retailer's network that the employee can see. This may expose confidential information on the employee's computer and on the network or allow malicious behavior.

Lastly, improperly configured authorized access points could also pose a danger. If the access point is reset to defaults or otherwise loses its security settings and becomes 'open', it too becomes a gateway to the Ethernet network.

The potential consequences of any of these security breaches are multiple, but essentially they boil down to two primary threats:

- employees can try to profit (e.g. be paid by organized crime) by feeding data out over unsecured wireless links and then selling or using it
- Hackers can directly try to steal customer or retailer data

Wireless links are an easy attack vector for the determined criminal.

Wireless Intrusion Prevention Defends The Retailer Network

To secure the retailer against unmonitored Internet access and other wireless threats, AirTight Networks offers a wireless intrusion prevention and performance management solution. Traditional computer security products, such as firewalls and VPNs, only monitor wired traffic and have no visibility into the wireless traffic that is flowing in the air.

SpectraGuard Enterprise provides a complete wireless intrusion prevention solution which continuously scans the airwaves and provides automatic protection against any unauthorized wireless activities. SpectraGuard Enterprise can prevent wireless connections to external, neighboring APs while allowing use of the authorized retail wireless network. Or, the retailer can institute a complete "no wireless" policy preventing all wireless LAN activity. In either case, SpectraGuard Enterprise eliminates the risk of data loss over an insecure wireless connection while doing no harm to authorized internal WLANs or neighboring WLANs. SpectraGuard Enterprise also provides protection against many other wireless threats including ad hoc networks and clients connecting to external neighboring wireless LANs. Above all SpectraGuard Enterprise provides peace of mind that the brand image and reputation of the retailer will not be damaged through a wireless security breach.

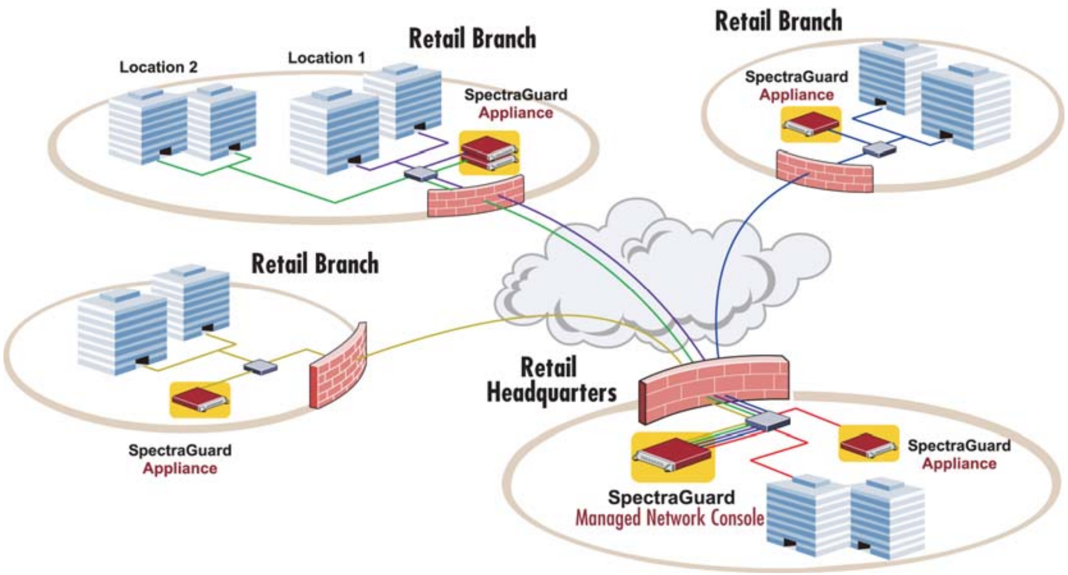

Figure 4: Retailers can manage multiple SpectraGuard Enterprise deployments from a single centralized SpectraGuard Managed Network Console (MNC)

SpectraGuard Enterprise automatically identifies unauthorized wireless behavior and takes immediate action to prevent it. This means that retailers do not need a local IT manager to initiate prevention; SpectraGuard Enterprise allows administrators to set policies that take effect automatically. As retailers typically have centralized IT resources, SpectraGuard Managed Network Console allows global management of all SpectraGuard Enterprise deployments, no matter where they are. Different policies can be defined for office, store, and warehouse facilities. Centralized policies can be pushed to each retail branch, and each site can be independently monitored, down to each individual Wi-Fi client.

How a WIPS Solution Maintains Network Integrity and Relevant PCI Requirements

The PCI standard has several requirements which are directly impacted by wireless security threats. According to the PCI security assessment guidelines, the scope of compliance validation includes:

> "**All external connections** into the merchant network (e.g.; employee remote access, payment card company, third party access for processing, and maintenance)..." [emphasis added]

Given that wireless LANs can and do provide external connectivity into the merchant network – in office, store, and warehouse facilities – WLANs must be secured in all of these environments.

Requirement 1: *Install and maintain a firewall configuration to protect data.*

While wired firewalls are a required and necessary first step in protecting customer data, wired firewalls are not effective in preventing wireless attacks as they have no means to monitor and analyze wireless traffic. This means that rogue access points behind the firewall will not be protected by traditional wireline security methods. Ad hoc networks and wireless clients that connect to neighboring wireless LANs from behind the firewall will also escape monitoring.

SpectraGuard Enterprise provides immediate protection against these threats through 24 x 7 continuous monitoring of the air space. All wireless LAN activity is immediately identified and classified according to policies set up by the IT administrator. Any rogue access point, ad hoc network or connection to a neighboring wireless LAN can be immediately quarantined, preventing all data transmission until the unauthorized device is physically removed or disabled.

This requirement is also intended for employee laptops taken offsite and used to access the retailer network. PCI recommends use of a personal firewall. However, personal firewalls have the same challenge in not monitoring wireless connections or the air space. SpectraGuard SAFE is a wireless connectivity management software for laptops that protects against wireless threats while away from the office. It can be remotely configured and managed by SpectraGuard Enterprise and provide reports of unsafe wireless activity while away from the office.

Requirement 2: *Do not use vendor-supplied defaults for system passwords and security parameters*

Section 2.1.1 of the PCI Data Security Standard - added in September 2006 – clearly calls out the requirement for changing the default settings on any and all wireless access points in the environment. This is a minimal security best practice that should be followed in all wireless installations.

SpectraGuard Enterprise provides a monitoring and enforcement mechanism for this requirement – ensuring that any all wireless access points on the network are properly encrypted and have the proper SSID – and disabling any that violate this policy. And, as we'll point out in Requirement 11, SpectraGuard provides for on-going monitoring and enforcement of this requirement – even as the network grows and expands.

Requirement 3: *Protect stored cardholder data.*
and
Requirement 4*:* *Encrypt transmission of cardholder and sensitive information across open, public networks.*

Both of these requirements are intended to protect card holder data wherever it is stored and whenever it is transmitted. And since all wireless communication are effectively in the open, anytime wireless is used, it must be protected. SpectraGuard Enterprise can ensure this requirement is met by:

- preventing authorized wireless LAN access points from becoming mis-configured and accidentally allowing transmission of sensitive data in the clear
- preventing rogue access points from being installed and used to access stored customer data or install mal-ware to capture and export cardholder information.

An authorized wireless LAN access point that becomes mis-configured will create an immediate alarm for the IT administrator. Policies can be applied to prevent traffic from moving through the access point until it is properly reconfigured. As with Requirement 1, SpectraGuard Enterprise can immediately identify and prevent rogue access point communication.

Requirement 10: *Track and monitor all access to network resources and cardholder data.*

Unscrupulous individuals might use a neighboring wireless LAN as an avenue to leak confidential information through personal webmail which would go unmonitored. SpectraGuard Enterprise can immediately prevent authorized wireless clients from associating with any wireless network other than the retailer's authorized wireless LAN. This ensures that existing security protocols for corporate email cannot be avoided.

SpectraGuard Enterprise also ensures that mis-configured access points are immediately identified and all traffic prevented. An authorized access point that is misconfigured to be open will not require a username and password. SpectraGuard Enterprise will prevent any authorized client from accessing the network via this method, ensuring a proper audit trail is maintained at all times.

Requirement 11: *Regularly test security systems and processes.*

This requirement ensures that security vulnerabilities are regularly assessed. It specifically calls out the use of a wireless analyzer to periodically (at least quarterly) identify all wireless devices in use. The challenge with this approach is that it is periodic and only valid for that very brief point in time. It also does not address the large problem of many individual small sites that do not have local IT support. SpectraGuard Enterprise provides continuous 24 x 7 monitoring of the retailer's air space ensuring that wireless activity is precisely known at all times. The solution is architected such that it can be deployed at all sites but centrally configured and managed. This eliminates the steep costs associated with IT personnel having to travel to each individual site – reducing costs while providing better security.

Requirement 12: *Maintain a policy that addresses information security for employees and contractors.*

With SpectraGuard Enterprise, specific wireless security policies form the heart of the system. This ensures that the retailer has a documented, in force wireless security policy at all times. SpectraGuard Enterprise also can maintain a list of all authorized wireless clients and immediately flag the administrator of any new wireless devices (such as those embedded in new notebooks) which may need appropriate configuration before accessing the wireless network. In the interim, all traffic from those wireless clients can be automatically prohibited to prevent security breaches.

Conclusion

Wireless LANs are and will continue to be a critical component of many retailers' network infrastructure. However, along with the productivity gains from this technology also come new security threats. These wireless threats can compromise the corporate infrastructure integrity and security, whether or not the retailer has their own wireless LAN network. The two primary attack types are

- outside hackers trying to steal customer credit card/account data via a wireless link
- employees trying to steal/transmit/sell/use data – over a wireless link

These threats combined with the need for PCI compliance require new solutions to protect the network integrity and security. A wireless intrusion prevention system (WIPS) can provide 24 x 7 monitoring and prevention for all categories of wireless threats. Using a WIPS solution can ensure that proper authentication and access controls for the wireless LAN infrastructure remain in place. It will prevent unauthorized access points. And it will prevent clients from connecting to neighboring wireless LANs.

Retailers should invest in a WIPS to prevent potentially compromising cardholder information and the retailer's brand image and reputation.