



WHITEPAPER

The Need for Wireless Intrusion Prevention in Retail Networks

The Need for Wireless Intrusion Prevention in Retail Networks

Firewalls and VPNs are well-established perimeter security solutions. The introduction of wireless technologies has created a new category of entry point circumventing traditional security components. Many recently publicized data breaches in the retail industry have exploited wireless vulnerabilities. Attackers have been able to access sensitive applications and databases regardless of security systems such as firewalls and VPNs. Wireless intrusion prevention is required to thwart wireless attacks and provides the least costly method of adhering to the PCI DSS wireless security requirements.

Retailers have used wireless technology to drive business efficiencies for over twenty years. Recently, sophisticated thieves have recognized that these wireless deployments offer the perfect entry point into the network allowing them to access and steal valuable customer information. Many retailers continue to rely only on traditional security systems such as firewalls, VPNs, and/or network segmentation to secure their networks. This paper provides a brief overview of some of the most important threats that wireless presents to retail network security and illustrates how traditional defenses such as firewalls and VPNs are just not enough.

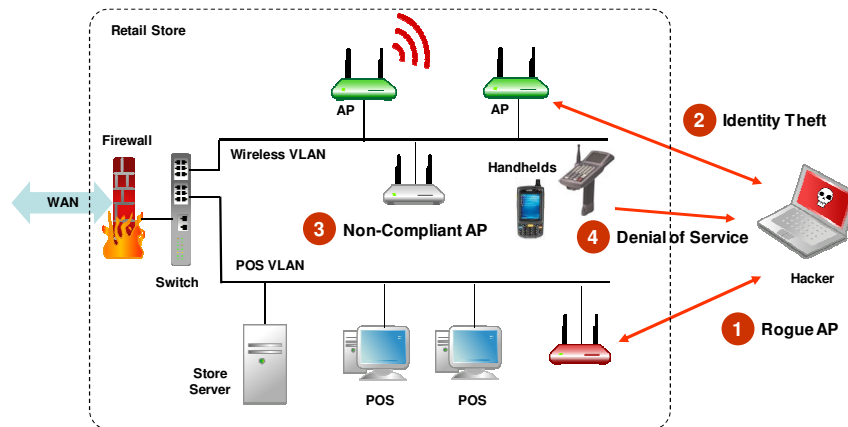


Figure 1: Wireless Security Issues in Retail

1. Rogue Access Points

A rogue access point (AP) is an unauthorized wireless device physically connected to the wired network. A rogue AP can be installed by a careless employee/contractor or a malicious attacker. It is important to realize that rogues can show up on any network segment. Even if POS devices are on a separate network segment, rogue APs can be connected to these networks.

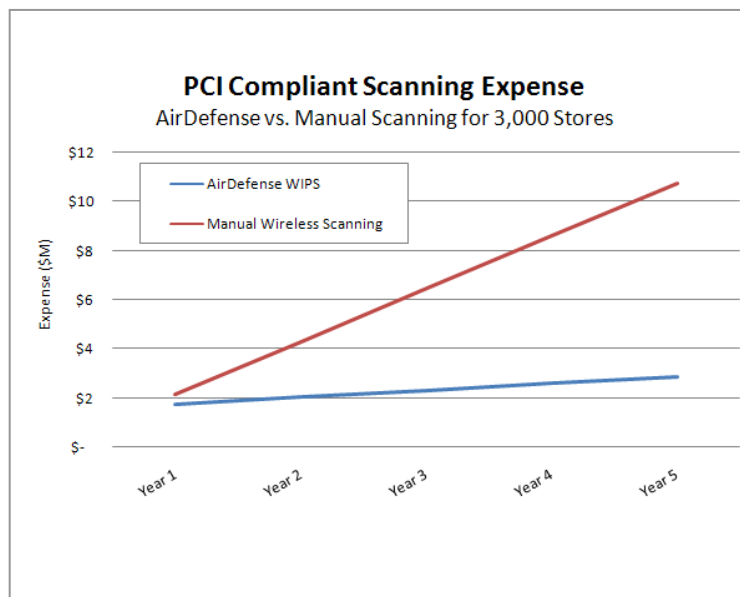
- Rogue APs provide attackers with unrestricted access. They allow the attacker to hack internal servers just as if they were connected to an internal Ethernet port.

- Rogue APs can be installed on any network, including POS networks that have been intentionally segmented from wireless networks
- Rogue APs can be installed in networks that specifically prohibit wireless device
- PCI compliance requires quarterly scanning for rogue devices at the very least. Using laptop based sniffers at each location quickly becomes an expensive and untenable solution for large retailers. This can leave networks vulnerable for months before rogues are detected. (See chart on next page.)

2. Identity Theft

A hacker can masquerade as an authorized wireless device and connect to an authorized AP. Once on the network, all the rogue AP scenarios previously discussed are applicable.

- MAC address based filters are useless since wireless MAC addresses are broadcast and hackers can easily change the MAC address of their device to match that of an authorized device.
- WEP encryption can be cracked in a few minutes. Once hackers have the WEP key they have unrestricted access to the network allowing them to attack internal servers and applications.
- WPA Pre-Shared Key is easy to implement and does not have the vulnerabilities of WEP; however, one common key is used between many devices. Hackers have been known to steal portable data terminals or use social engineering to obtain the pre-shared key. Once the key is stolen, the entire network is vulnerable until administrators manually change the key at every AP and every portable data terminal.
- Some retailers have considered requiring the use of a VPN on every wireless device. This method is not scalable and is difficult to manage. Existing portable data terminals rarely have VPN client software installed; VPN client software is not even available for many of the most popular portable data terminals. Most wireless deployments are moving away from VPN technology due to these limitations.
- Firewalls cannot prevent an attacker that has gained access to the wireless network from attacking internal servers. Firewalls require that ports be opened to allow applications to operate in the store. An attacker that gains access to the wireless LAN can use any of the hundreds of available methods to break into the applications provided on your internal network. Visa recently identified the top five security threats to retailers; four of them rely on application vulnerabilities that are not thwarted by firewalls.



3. Non-Compliant Access Points

Wireless APs are frequently misconfigured. According to Gartner, a majority of all wireless security incidents will happen as a result of misconfigured devices. Misconfigurations happen for a variety of reasons including human error and bugs in AP management software.

- A misconfigured AP in a store or distribution center can be detected and exploited by a hacker to gain access to the network allowing them to attack internal servers and applications.
- It is important to constantly audit your wireless network against established policy. Firewalls provide no visibility into the configuration of wireless devices. As an example, if an authorized AP is inadvertently or maliciously reset to default settings, firewalls cannot detect the vulnerability.
- WLAN APs and infrastructure contain well-known vulnerabilities that can result in information disclosure, privilege escalation, and unauthorized access through fixed authentication credentials.

4. Denial of Service

Hackers can easily perform wireless denial of service (DoS) attacks preventing devices from operating properly and stopping critical business operations.

- Wireless DoS attacks can cripple a distribution center or store despite the best security standards like WPA2. Firewalls and VPNs cannot detect wireless DoS attacks.
- Hackers can insert malicious multicast or broadcast frames via wireless APs that can wreak havoc on the internal network. These are Layer 2 attacks which cannot be detected by Layer 3 based firewall and VPNs.

Conclusion

Wireless introduces vulnerabilities in retail networks that traditional firewalls and VPN based solutions cannot address. Rogue APs allow attackers unfettered access to the internal network. The quarterly scans required by PCI DSS are too costly to implement without a wireless IPS. A wireless IPS can eliminate rogue APs, detect and prevent identity theft, monitor for AP misconfigurations, and mitigate wireless denial of service attacks. Wireless IPS provides protection against sophisticated wireless attackers, costs less to implement than quarterly scanning, and mitigates wireless vulnerabilities where firewalls and VPNs cannot.

AirDefense, the market leader in anywhere, anytime wireless security and monitoring, is trusted by more Fortune 500 companies, healthcare organizations and high-security government agencies for enterprise wireless protection than any other wireless security provider. Ranked among *Red Herring's* Top 100 Private Companies in North America, AirDefense products provide the most advanced solutions for rogue wireless detection, policy enforcement and intrusion prevention, both inside and outside an organization's physical locations and wired networks. Common Criteria-certified, AirDefense enterprise-class products scale to support single offices as well as organizations with hundreds of locations around the globe.

AirDefense Enterprise, the flagship product, is a wireless intrusion prevention system that monitors the airwaves 24x7 and provides the most advanced solution for rogue detection and mitigation, intrusion detection, policy monitoring and compliance, automated protection, forensic and incident analysis and remote troubleshooting. As a key layer of security, AirDefense Enterprise complements wireless VPNs, encryption and authentication. Using a monitoring architecture of distributed smart sensors and a secure server appliance, the AirDefense Enterprise system provides the most comprehensive detection of all threats and intrusions. Unlike any other solution on the market, AirDefense Enterprise analyzes existing and day zero threats in real time against historical data to more accurately detect threats and anomalous behavior originating inside or outside the organization. The system automatically responds to threats according to appropriate business process and compliance requirements on both wireless and wired networks, making AirDefense Enterprise the industry's most secure and cost-effective wireless intrusion prevention and troubleshooting solution.

AirDefense Personal, the industry's first end-point security solution, provides uninterrupted protection for all mobile employees and their enterprise wireless assets, regardless of location – at work, home, airports or other wireless hotspots. Policy profiles are defined centrally on AirDefense Enterprise and automatically downloaded to each mobile user. If threats are discovered, AirDefense Personal notifies the user and sends the alerts to AirDefense Enterprise for central reporting and notification. This unique solution allows the network administrator to enforce corporate policies and provide complete protection for the mobile workforce, regardless of location.

The **AirDefense InSite Suite** is a collection of powerful tools available today for network architects to design, install, maintain and troubleshoot wireless networks. Tools included in the suite are: **AirDefense Mobile**, complementary to AirDefense Enterprise allows administrators to perform wireless assessments, security audits, locate and manage rogues. **AirDefense Architect** provides complete design and 3D RF simulation of wireless LANs based on building-specific environments. **AirDefense Survey** provides real-time, in-the-field measurements of Wi-Fi RF environments for site-specific surveys.

For more information or feedback on this white paper, please contact info@airdefense.net or call us at 770.663.8115. **All trademarks are the property of their respective owners.**