

ShopVisible™

Protecting the Palace: Cardholder Data Environments, PCI Standards and Wireless Security for Ecommerce Ecosystems

In July the Payment Card Industry Security Standards Council (PCI SSC) published its Information Supplement: PCI DSS Wireless Guidelines version 1.2, addressing security threats and wireless Internet user guidance. For PCI, it is insufficient for Ecommerce companies to secure their software development lifecycle (SDLC) and their servers alone; they must also adhere to a stringent, regulatory manner of wireless security as well to prevent outside breach via what so many Web users employ these days: WiFi access.

Deploying WLAN or wireless local area networks has become increasingly critical for Ecommerce merchants as their efforts at protection and threat avoidance have come under scrutiny from PCI. In recessionary times coupled with an age of hyper-vigilance on the web regarding secure payment transactions, PCI has mandated that wireless monitoring and controversially susceptible APs or access points to the network must be secured with documented supporting policy. Not only does Ecommerce/security solution provider, ShopVisible, function in a realm of PCI compliance, ShopVisible is also excited to share their knowledge with others in Ecommerce to create a safer and more sophisticated payment transaction arena online.



There are two distinct types of PCI wireless requirements: 1. generally applicable requirements that all organizations should have in place to protect their networks from attacks via rogue or unknown wireless access points and clients; and 2. in-scope wireless access requirements stating “that all organizations that transmit payment card information over wireless technology should” be primarily concerned with securing the CDE or Cardholder Data Environment. ShopVisible is mindful that safeguarding the CDE will enforce best practices with regards to online payment. When customers feel safe they are more prone to offer up their wallets and indeed their brand loyalty to online merchants. Finding a PCI compliant provider like ShopVisible can certainly make or break the deal when purchasing from the Web. Don’t let something seemingly trivial and inconsequential to your business practices like wireless activity leave your consumers bereft and your company liable.

For ShopVisible, the essential CDE information is derived from merchant accounts and pertains to customer information, payment data and how such data is stored and transmitted. PCI defines the CDE as the “computer environment wherein cardholder data is transferred, processed, or stored, and any networks or devices directly connected to that environment.” These CDE elements can include Point of Sale terminals in which the cardholder data enters the network’s hubs, switches, and other network devices acting as connectors in the same Ecommerce eco-system; back office servers within the CDE connected by cable networks; firewall demarcation lines as defined by the firewall limitations; and open traffic flowing through the CDE at the end points of encryption and decryption processes. Key encryption and decryption processes are also imperative steps towards PCI compliance; these however are somewhat outside the scope for this document...



ShopVisible™

Access point relevance is often misunderstood in the CDE protection realm. Rogue APs are devices that add unauthorized and unsecured WLAN to the organization's network. Rogue APs often emerge through WLAN card insertion into back office servers, unknown WLAN router connections to the network and other intrusion points. Nowadays, with so many wireless users inputting and storing Ecommerce data via wireless connection, managing and securing the connections has become pivotal in compliance with PCI.

What happens when a user adds a known WLAN to a network residing outside of the CDE? PCI notes that if no traffic at all passes from the WLAN to the CDE, "then that WLAN can be considered out of the scope for the PCI DSS. However, if the WLAN is connected to the firewall on the CDE, or is connected to a network that is connected to the firewall on the CDE, then the firewall's configuration is in scope for both the PCI DSS" and the related PCI documentation on wireless activity, "even though the AP is outside of the scope of both PCI DSS" and the related policy.

In an Ecommerce ecosystem, it is imperative to realize the depth level of WLAN deployment. Companies and organizations utilizing wireless capabilities while also trying to remain PCI compliant must "know the boundaries of the network and [have] an accurate networking inventory and hardware inventory." Recommendations for secure wireless connection can be seen in up-to-date inventory maintenance for all CDE locations. Without said inventory any company would be clueless regarding what authentic devices are and which ones are deemed "rogue" and thereby in breach of PCI requirements.



PCI requirement 11 is one of the most difficult to secure. The payment standard, 11.1, exists to "ensure that an unauthorized or rogue wireless device introduced into an organization's network does not allow unmanaged and unsecured WLAN access to the CDE." In a nutshell, this functions to prevent rogue hackers using wireless devices to intercept cardholder data. It is essential for any location holding cardholder data to be updated and checked regularly. Using a wireless analyzer or preventive measures like IDS and IPS or intrusion detection and intrusion protection systems is critical. Potentially, rogue devices can emerge anywhere where storage, transmission and processing of data occur. In other words, any CDE location is susceptible. In order to be complaint with PCI, companies may not select a sample of servers or sites to test and perform security measures in an effort to support WLAN protection; "organizations must ensure that they scan all sites quarterly to comply with the standard." Sample testing will be done only at the direction of the PCI assessor and not the company or organization being assessed.

Wireless analyzers and scanning tools in the forms of an IDS/IPS are needed to comply with PCI requirement 11.1. Wired side scanning tools can identify threats but often have high false positive rates says PCI. They often "miss cleverly hidden and disguised rogue wireless devices or devices that are connected to isolated network segments." To combat the constantly blossoming spectrum of rogue threats for intrusion of the CDE, a variety of tools exists, ranging from free PC tools to commercial scanners and 3rd party services intent on fully securing the network. Rogue wireless clients are deemed any unauthorized device with a wireless interface that should not be present in the ecosystem. Upon detection of a rogue device or intrusion companies must immediately remediate the problem and then



ShopVisible™

rescan for new threats. This will then result in compliance with both PCI 11.1 and 12.9. For best practices, large companies or those with high revenue clients and burgeoning implementations should automate wireless scanning through wireless IDS or IPS systems.

PCI recommendations:

- use an IDS or IPS to recognize rogue intrusion devices affecting the CDE; quarterly scans are a minimum but to ensure best practices, these can be conducted weekly
- utilize automatic alerts and containment mechanisms on a wireless IPS to secure the CDE
- formulate an incident response plan as part of you ISP or information security policy that will show the path for rogue device physical destruction upon immediate detection in the CDE; this will be in line with PCI requirement 12.9.5

For PCI compliance, wireless networks that do not store, process or transmit cardholder data should be

PCI DATA SECURITY STANDARD

PRINCIPLES AND REQUIREMENTS
Build and Maintain a Secure Network <ol style="list-style-type: none"> 1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data <ol style="list-style-type: none"> 3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program <ol style="list-style-type: none"> 5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures <ol style="list-style-type: none"> 7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks <ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy <ol style="list-style-type: none"> 12. Maintain a policy that addresses information security

isolated from the CDE using a secure firewall. This makes it so unauthorized users cannot access the CDE via wireless deployment. The wireless firewall must perform the following functions to be PCI compliant: isolate traffic from entering the CDE by filtering wireless packets based on the 802.11 protocol; perform stateful inspections of the connections; and monitor and log the traffic (permitted or denied) by the firewall in scope with PCI requirement 10.

To be in line with the PCI requirements regarding firewall usage and maintenance, all firewall rules must be audited and reviewed at a minimum of every 6 months. The PCI wireless document notes that “organizations should consider using outbound traffic filtering as a technique for further securing their networks and reducing the likelihood of internally based attacks.” Relying on VLAN or virtual

LAN based segmentation alone will be inadequate for rendering a secure CDE. In general, with PCI rules, any protocol and traffic acting as a non-imperative in the CDE security controls should be blocked if not needed for performing credit card transactions.

PCI recommendations:

- use firewall to block wireless traffic from the entering the CDE and reconfigure the firewall as needed by using a wireless IDS or IPS
- do not use VLAN based segmentation with MAC address filters to segment networks
- monitor the firewall logs daily and verify firewall rules every 6 months

Applicable requirements for in-scope wireless networks are contingent on physical security measures. At a datacenter for instance, all APs must be caged or chained down to the physical device if accessible



ShopVisible™

to the public. Camera monitoring should be in place as should extensive badge access security and visitor and site logging of who is touching the hardware and when. In the case of ShopVisible's PCI level I audit, extensive coordination with the data center was wrought by a team of security specialists, both internal and external, to ensure company policy documentation matched up with data center physical security protocols. If utilizing a hardened data center, it is best to ascertain their physical security packet facets before and after a QSA initiated site visit. The 3rd party auditor along with an internal representative should verify sound physical security practices as mentioned above in the data center.

PCI defines obvious risks to physical security aside from theft as "the ability of an unauthorized person to reset the AP factory defaults. Here it is valuable to note that any organizational ISP or security policy must include PW identification and derivation practices. The reset function poses a particular problem because it allows an individual to negate any security settings that administrators have configured in the AP." If malicious intent is present in any user intrusion, the person can exploit this reset function and access the console thereby diverting the PCI security firewall already in place. PSKs or pre shared keys are not recommended nor are printed or default passwords. PCI summarizes the measures needed here by stating that APs should be mounted on the ceiling or anyplace not susceptible to breach or physical tampering; use APs with chassis and mounting options to prevent port access and resetting; secure handheld devices with unique passwords and always encrypt PSKs if cached locally; utilize wireless monitoring systems to track and locate device placement and unauthorized device presence in the network.

Wireless intrusion prevention and user access logging are two pivotal aspects of PCI as far as wireless connections go. PCI defines intrusion detection as "the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incident, which are violations or imminent threats of violation of computer security polices, acceptable use policies, or standard security practices."

IDS are software bundles that automate intrusion detection processes; IPS function with IDS capabilities but also can prevent breaches and threats at various APs. Wireless systems performing these functions are grouped by PCI into 3 categories: those detecting rogue wireless device containment; those detecting unsafe activity and network configurations; and those detecting denial of service attacks and other wireless intrusion efforts.

Milestone	Goals
1	Remove sensitive authentication data and limit data retention. This milestone targets a key area of risk for entities that have been compromised. Remember – if sensitive authentication data and other cardholder data are not stored, the effects of a compromise will be greatly reduced. If you don't need it, don't store it.
2	Protect the perimeter, internal, and wireless networks. This milestone targets controls for points of access to most compromises – the network or a wireless access point.
3	Secure payment card applications. This milestone targets controls for applications, application processes, and application servers. Weaknesses in these areas offer easy prey for compromising systems and obtaining access to cardholder data.
4	Monitor and control access to your systems. Controls for this milestone allow you to detect the who, what, when, and how concerning who is accessing your network and cardholder data environment.
5	Protect stored cardholder data. For those organizations that have analyzed their business processes and determined that they must store Primary Account Numbers, Milestone Five targets key protections mechanisms for that stored data.
6	Finalize remaining compliance efforts, and ensure all controls are in place. The intent of Milestone Six is to complete PCI DSS requirements and finalize all remaining related policies, procedures, and processes needed to protect the cardholder data environment.

PCI recommendations:

-use a centrally controlled wireless IDS/IPS to monitor unauthorized access and detect rogue devices
-enable historical data logging to verify access to wireless networks; provide "granular wireless device information and



ShopVisible™

store event logs and stats for no less than 90 days”

-enable an IPS that will automatically disable rogue elements upon detection if connected to the CDE

-ensure that the IPS signature set is regularly and vigilantly monitored/updated as new threats emerge

-coordinate logging events with other network monitoring processes

-address policy to function immediately after an IDS/IPS discovers a rogue element

-keep an informed topology of physical locales and APs

*****All facts, figures and quotations presented here are derived from the Information Supplement: PCI DSS Wireless Guideline, July 2009, version 1.2; authored by the PCI SSC Wireless Special Interest Group (SIG) Implementation Team**

****Summary article authored by ShopVisible Marketing Manager, Vijay Mahoney;
vijaym@shopvisible.com; (404) 496-6914**

