Laird TECHNOLOGIES

Innovative **Technology** for a **Connected** World

Wi-Fi® Client Device Security and Compliance with PCI DSS

Originally Published: June 2008

Updated: January 2009, June 2010, October 2012

A White Paper from Laird Technologies

Major payment card companies have joined together and created the Payment Card Industry (PCI) Security Standards Council. It agreed on a number of guidelines, detailing ways retail companies protect payment card information to prevent credit and debit card and fraud and identity theft. Those guidelines are codified as requirements in the PCI Data Security Standard (PCI DSS).

Americas: +1-800-492-2320 Option 3
Europe: +44-1628-858-940
Hong Kong: +852-2268-6567 x026
www.lairdtech.com/wireless

CONTENTS

PROTECTING PAYMENT CARD INFORMATION

It is every retailer's nightmare: An attacker exploits weak network security at a retail store to steal information from customers' payment cards (credit cards and debit cards). The theft affects everyone in the retail supply chain, including the retailer, its customers, banks, and payment card companies. The retailer, however, is the one hammered by bad publicity. In addition to costing the retailer business, the bad publicity sullies the retailer's reputation, forever linking its name to the theft.

In 2004, major payment card companies established the Payment Card Industry (PCI) Security Standards Council to create a common set of guidelines for how retailers must protect payment card information and thereby prevent credit card and debit card fraud and identity theft. Those guidelines are codified as requirements in the PCI Data Security Standard (PCI DSS).

The Council updated PCI DSS in 2006 and 2008. The current set of requirements is known as PCI DSS Version 1.2. The Council will enhance PCI DSS as needed to ensure that the standard mitigates emerging payment security risks while continuing to foster wide-scale adoption.

If a retailer processes, stores, or transmits information for payment cards issued by any of the major payment card companies – Visa Inc. International, MasterCard Worldwide, Discover Financial Services, JCB International, and American Express – then that retailer must comply with the requirements of PCI DSS.

According to www.pcisecuritystandards.org, the PCI Security Standards Council is "an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection." The Council's mission is to "enhance payment account data security by driving education and awareness of the PCI Security Standards."

PCI DSS is "a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures." You can download the PCI DSS specification from the www.pcisecuritystandards.org Web site.

A retailer that fails to comply may risk stiff penalties from the payment card companies and may be denied the ability to accept credit and debit cards from those companies.

Of course, potential penalties for noncompliance pale in comparison to the damage from payment card information being stolen. For example, wireless network breaches at two Miami-area stores of a U.S.-based discount retailer gave hackers undetected access to the retailer's central payment card databases for 18 months, exposing over 45 million credit and debit cards to potential fraud. Fraudulent purchases occurred around the world. The total cost to the retailer – including settlements with U.S. state governments, settled claims with payment card companies, and remediation from the incident – exceeded $320 million. In addition, the retailer's reputation with customers and partners was sullied, and victims of fraud bore a huge burden to recover their identities and change account information.

Compliance with PCI DSS protects a retailer's reputation and, ultimately, its business by ensuring that the retailer has taken proper measures to keep payment card information secure. PCI DSS is a multifaceted security standard, and to comply with the standard a retailer may need to make dozens of changes to network equipment and configurations, client devices and configurations, applications, policies, and procedures.

This white paper focuses on client devices that connect to a network using wireless LAN, or Wi-Fi®, technology. A robust, standards-based approach to Wi-Fi client security aids in PCI DSS compliance by protecting the data that clients transmit and receive and the networks to which they connect.

RETAILERS AND WI-FI

WLANs are prevalent in retail stores and distribution centers. Some retailers have been using WLANs since before the first Wi-Fi standard was ratified by the 802.11 Committee of the IEEE (formerly the Institute of Electrical and Electronics Engineers) in 1997.

Wi-Fi is popular in retail for two reasons. First, many retail workers are mobile, meaning that they do their jobs from different locations or while on the move. An increasing number of these mobile workers rely on client devices such as mobile computers to do their jobs, and those devices rely on network connections using Wi-Fi. Second, Wi-Fi gives retailers flexibility in configuring their stores. For example, devices such as cash registers can be installed and made operational, then moved or removed without any changes to the store's wired (Ethernet) network. Because WLANs improve worker productivity and reduce the costs of configuring and reconfiguring stores, most retailers consider their WLANs to be a critical part of their information infrastructure.

THREATS WHEN WI-FI SECURITY IS WEAK

Wi-Fi involves communication between radios that use a specific type of radio frequency (RF) technology. Wi-Fi radios send data to each other over the air, using radio waves. In a retail store, Wi-Fi radios in computing devices communicate with Wi-Fi radios in infrastructure devices such as access points (APs) that are connected to the store's wired network. The radio waves that travel between the devices can "bleed" through the walls of the store to adjacent stores, parking lots, and other nearby public areas. Those RF signals can be viewed by any computing device in the vicinity of the store, provided that the device is equipped with the following:

- A Wi-Fi radio
- An antenna that provides sufficient gain to enable the radio to "hear" the Wi-Fi packets
- A commonly available software application called a Wi-Fi sniffer, which makes the contents of Wi-Fi packets viewable

Without proper Wi-Fi security in place, a hacker can use intercepted Wi-Fi packets to do one or more of the following: gain access to the WLAN, view sensitive information that is transmitted over the air, or trick users into communicating with him instead of the network.

The first threat of weak Wi-Fi security is **network exposure**. Control packets travel between Wi-Fi clients and a WLAN. When WLAN access is not governed by a strong authentication mechanism, then a hacker can use the control information in sniffed packets to pose as an authorized user and gain access to the WLAN. Once on the WLAN, the hacker may be able to gain access to sensitive information on the network.

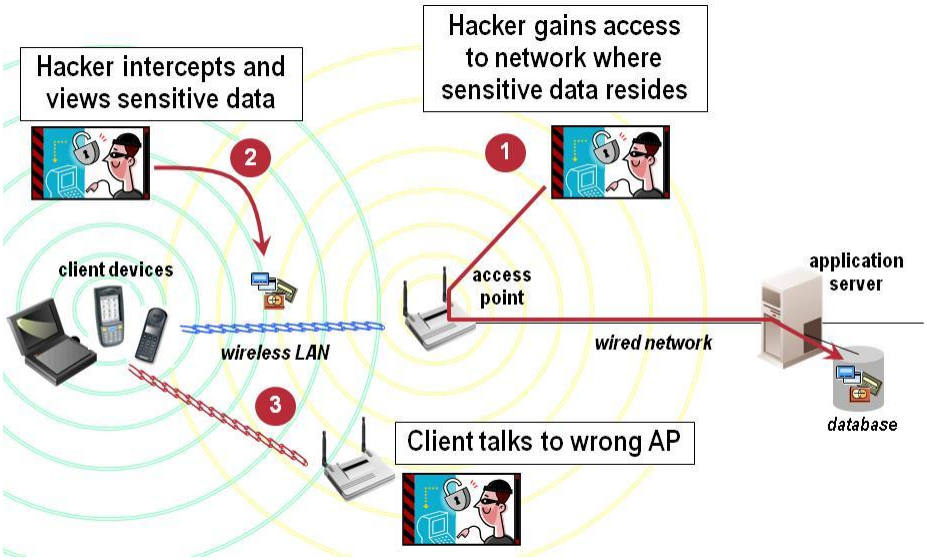

Figure 1: Wi-Fi security threats

The second threat of weak Wi-Fi security is **data exposure**. Some of the data packets that travel between a Wi-Fi client and a WLAN may contain sensitive information. If the packets are not scrambled, or encrypted, so that they cannot be deciphered by a hacker, then the hacker can view sensitive information, such as credit card information, just by sniffing and viewing the packets.

The third threat of weak Wi-Fi security is **man-in-the-middle attacks.** When Wi-Fi clients are not required to use strong authentication methods, a hacker's laptop posing as an AP may be able to trick clients into associating with it instead of a trusted AP. Once a Wi-Fi client associates to a hacker's laptop, the hacker may be able to steal information from the client, including sensitive information and information required to gain access to the trusted network.

Wi-Fi Security Foundation: WPA2-Enterprise

Fortunately, WLAN security threats can be mitigated through good WLAN security practices. The foundation of any WLAN security approach should be the Enterprise version of Wi-Fi Protected Access® 2, or WPA2®.

In the early 2000s, as Wi-Fi became popular on mainstream client devices such as laptops, it was determined that the original WLAN security mechanism of Wired Equivalent Privacy (WEP) was insufficient for several reasons, including:

- **No access control:** While it defines a means to scramble, or encrypt, transmitted data, WEP provides no means to control access to a WLAN. If you know the WEP encryption key, then you can gain access to the WLAN.
- **Vulnerable keys:** Due to weaknesses in WEP, a hacker can "crack" or decipher a WEP key by collecting WEP-encrypted data packets and running them through a WEP-cracking tool. Today, using sophisticated tools, even a 104-bit WEP key can be cracked in less than an hour.
- **Static keys:** The only way to avoid the use of a WEP key that has been cracked by a hacker is to change all WEP keys regularly, which today means more frequently than every hour. Because the most common way of deploying WEP keys is to define them statically on all devices that used them, changing WEP keys is an administrative nightmare.

The IEEE, which defines the standards for WLANs and how they operate, formed a task group, called the 802.11i task group, to define a standard for stronger WLAN security. The 802.11i task group, like most other IEEE task groups, took several years to define, debate, finalize, and ratify the standard. In the meantime, the market grew increasingly impatient for something better than WEP.

WPA

The Wi-Fi Alliance®, a non-profit industry association of more than 300 member companies, responded to market pressure by teaming with the 802.11i task group to create WPA, which the Alliance termed "a significant near-term enhancement to Wi-Fi security".

According to the Alliance, WPA is "a specification of standards-based, interoperable security enhancements" that ensures data protection through encryption and WLAN access control through authentication. WPA was designed to be supported in software by Wi-Fi CERTIFIED™ products that previously had supported WEP.

There are two versions of WPA: Personal and Enterprise. Each defines a process for mutual authentication between the Wi-Fi client and the WLAN infrastructure. At the end of the authentication process, a key is derived dynamically from the information exchanged between the client and the infrastructure. After the authentication process completes, the derived key is used to encrypt and decrypt all unicast data that travels between the client and the infrastructure.

Personal vs. Enterprise

With WPA-Personal, authentication is done through a four-way handshake using a pre-shared key (PSK) or passphrase. If the PSK on the Wi-Fi client matches the PSK on the AP to which the client is trying to associate, then the authentication succeeds, and an encryption key for that client is derived and stored on the client and the AP.

While WPA-Personal authentication relies on a statically configured pre-shared key or passphrase, WPA-Enterprise authentication relies on IEEE 802.1X, a ratified standard for network access control. 802.1X supports a set of Extensible Authentication Protocol, or EAP, types for mutual authentication of the client device and the network to which it is trying to connect. 802.1X authentication with an EAP type such as PEAP or EAP-TLS is extremely strong. If WPA-Enterprise authentication succeeds, then an encryption key for the client is derived and stored on the client and the AP.

Table 1 compares popular EAP types that are used with 802.1X authentication:

Table 1: Comparison of popular EAP types

Type	Credential(s)	Database(s)	Pros and Cons
LEAP	Microsoft password	Active Directory (AD)	No certificates Strong password required
PEAP with EAP-MSCHAP	Microsoft password	AD	Native support in Windows, CE CA certificate on every client device
PEAP with EAP-GTC	Password, one-time password, token	AD, NDS, LDAP, OTP database	Broad range of credentials CA certificate on every client device
EAP-TTLS	Wide variety	Wide variety	Broad range of credentials Not widely supported
EAP-FAST	Microsoft password, others	AD, others	No certificates Complex provisioning process
EAP-TLS	Client certificate	Certificate authority (CA)	Very strong authentication Native support in Windows, CE CA, user certificates on every client device

While PSKs are easy to implement on small networks, a hacker can "guess" a short PSK using a dictionary attack. In such an attack, the hacker captures packets that were created using the PSK and then, using a dictionary of potential PSKs and the published algorithm for WPA, tries to recreate the capture packets. If he is successful, then he has determined the PSK, and he can use it to gain access to the WLAN. An online service runs a 20-minute attack using a dictionary of 135 million words for a cost of $17.

To avoid vulnerability to a dictionary attack, your PSK or passphrase must be a random string of at least 20 characters, including characters other than letters and digits. Of course, such a random string is difficult, if not impossible, to remember, so it must be configured statically on every client device and every infrastructure device in one sitting. Configuring a few devices in a home or small office is feasible; configuring scores or hundreds of devices in a larger organization can be a huge challenge.

For nearly every organization, the Enterprise version is superior to the Personal version.

TKIP: Vulnerable?

With WPA-Personal and WPA-Enterprise, encryption and decryption of all unicast data is done using Temporal Key Integrity Protocol, or TKIP. Like WEP, TKIP uses RC4 encryption, but TKIP is designed to address vulnerabilities of WEP by providing these enhancements:

- Longer initialization vector, which minimizes the chance that a key will be reused during a session
- Key hashing, which results in a different key for each data packet
- Message integrity check, which ensures that the message is not altered in transit between sender and receiver

In late 2008, two German researchers reported that a vulnerability in TKIP could enable an attacker to decrypt individual packets that are encrypted with TKIP. In mid-2009, two Japanese researchers reported that they had expanded on the German researchers' work and devised a way to mount a successful attack on TKIP. The latter report received a lot of media attention, with some articles claiming that TKIP can be cracked in less than one minute.

Summit has analyzed the paper published by the Japanese researchers and noted these highlights:

- The paper heavily leverages a paper written by German students in the fall of 2008. The new attack is simply a refined and practical version of a theoretical attack proposed by the German students.
- The attack described by the German students works only when the Wi-Fi router supports 802.11e. The approach by the Japanese scientists uses a man-in-the-middle (MITM) attack to overcome that limitation.
- Both attacks work with both the Personal and Enterprise versions of WPA because the attacks focus on encrypted packets and are oblivious to the authentication scheme that generates the encryption key used for TKIP.
- The attack by German students can obtain from an encrypted ARP packet the message integrity check (MIC) key and the plain text of the packet. The execution time of this attack is 12-15 minutes.
- The attack by the Japanese scientists can obtain from an encrypted ARP packet the same information but in less time (reportedly as little as one minute) and without the restriction of 802.11e support on the router.
- Neither attack can decipher the TKIP encryption key.

While the contents of an ordinary data packet are relatively unpredictable, all bytes of an ARP packet are fixed or known values except the last byte of the source and destination IP addresses. In other words, only two bytes of an ARP packet are unknown. The attack "cracks" those two bytes. It also "cracks" the eight bytes of the MIC and four bytes of the checksum by using an attack called chopchop 12 times.

In summary, the Japanese researchers improved an existing attack that enables a tool to decrypt the unknown two bytes of an ARP packet as well as the MIC and checksum used in conjunction with TKIP. The researchers provided no evidence that a practical tool for cracking an actual TKIP key or deciphering TKIP-encrypted data packets is imminent.

The reports, however, were enough to sound the death toll for TKIP and WPA. In May 2010, the Wi-Fi Alliance announced to its members that it was phasing out TKIP, first on infrastructure devices and then on client devices. In fact, beginning the first day of 2011, TKIP is not optional but **prohibited** in APs except as a component of WPA2 with mixed mode. TKIP (and WEP) will be prohibited in any Wi-Fi CERTIFIED device beginning in 2014.

With WPA's encryption method of TKIP rapidly moving from recommended to prohibited, organizations must adopt a stronger encryption method.

WPA2

In July 2004, the IEEE approved the full 802.11i specification. Soon after that, the Wi-Fi Alliance introduced a new interoperability testing certification, called WPA2, that incorporates the key elements of 802.11i. WPA2 is essentially the same as WPA, with TKIP replaced by a stronger encryption method based on the Advanced Encryption Standard (AES) cipher. In March 2006, WPA2 certification became mandatory for all new equipment certified by the Wi-Fi Alliance.

As with WPA, there are two versions of WPA2: Personal and Enterprise. With Personal, the process for authentication and dynamic key derivation relies on a PSK or passphrase; with Enterprise, the process relies on 802.1X. For the reasons discussed in the section on WPA, WPA2-Personal is insufficient for an organization with sensitive information such as cardholder data on its networks.

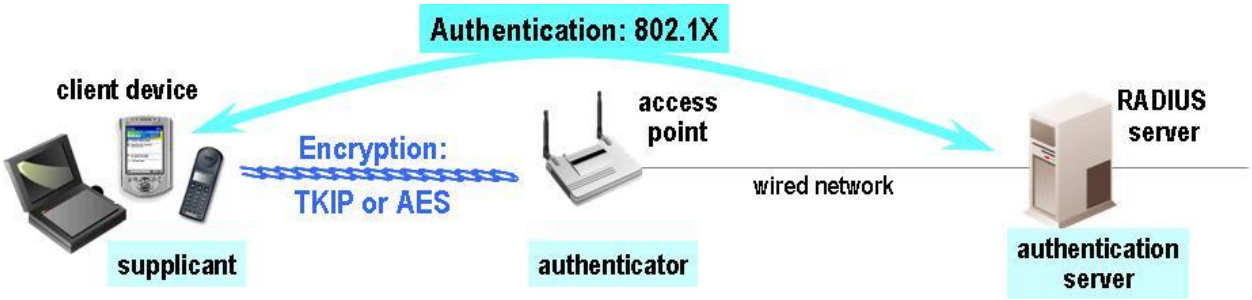

Figure 2: WPA-Enterprise and WPA2-Enterprise

As shown in Figure 2, the only difference between WPA-Enterprise and WPA2-Enterprise is the method of encryption. AES-CCMP, the encryption algorithm used with WPA2, does not have the vulnerabilities of TKIP.

In fact, AES-CCMP is strong enough to satisfy the U.S. federal government encryption standard of FIPS 140-2.

By combining 802.1X and AES-CCMP, WPA2-Enterprise addresses the security threats mentioned early in this section:

- **Network exposure:** When every Wi-Fi client uses WPA2- Enterprise and its 802.1X authentication, a hacker cannot glean from sniffed packets any information on how to gain access to the network.
- **Data exposure:** To prevent the data in Wi-Fi packets from being viewed by a hacker, the sender of those packets must encrypt the data in such a way that only the intended recipient can decrypt the packets and view the data in its unscrambled, clear-text form. WPA2-Enterprise provides proven mechanisms for ensuring that all transmitted data is protected from being viewed by a hacker.
- **Man-in-the-middle attacks:** When every Wi-Fi client is configured to use a strong EAP type for mutual authentication to the trusted WLAN, no client will associate inadvertently to a hacker's laptop that is posing as an AP. (See the discussion of requirement 2.1.1 for details on configuring clients.)

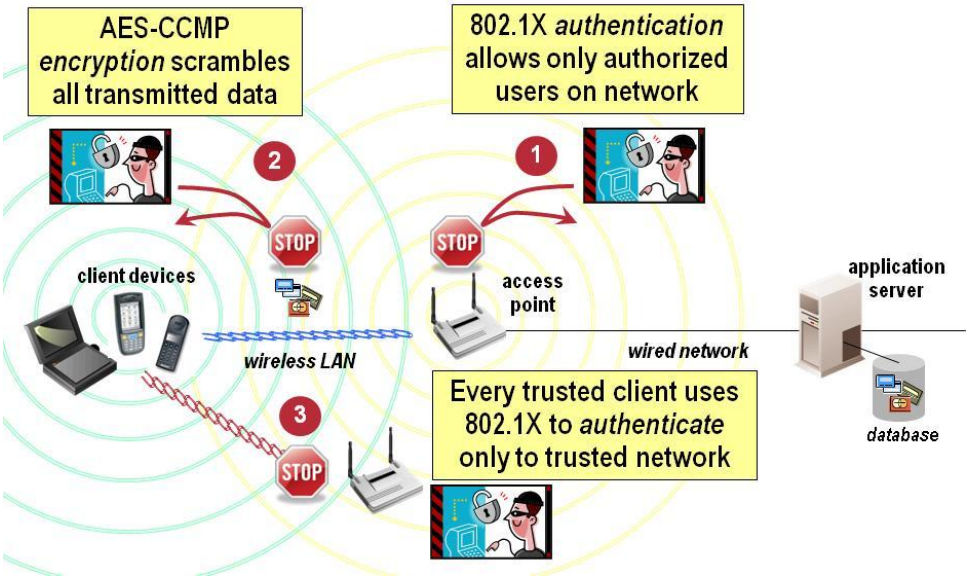

Figure 3: WPA2-Enterprise and Wi-Fi security threats

The use of WPA2-Enterprise protects all sensitive data, including credit card information, and the networks that house that data. Reliance on WPA2-Enterprise is a best practice for strong Wi-Fi security.

Best practice: Ensure that a Wi-Fi client device can gain access to your WLANs only using WPA2-Enterprise with a strong EAP type.

As is explained below, WPA2-Enterprise is required for PCI DSS compliance.

PCI DSS Requirements that Apply to Wi-Fi Clients

Any organization that stores, processes, or transmits cardholder data must comply with PCI DSS. The following is a list of the 12 high-level requirements of PCI DSS:

Build and Maintain a Secure Network
Requirement 1: Install and maintain a firewall configuration to protect cardholder data.
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Protect Cardholder Data

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

Maintain a Vulnerability Management Program
Requirement 5: Use and regularly update anti-virus software.
Requirement 6: Develop and maintain secure systems and applications.

Implement Strong Access Control Measures
Requirement 7: Restrict access to cardholder data by business need-to-know.
Requirement 8: Assign a unique ID to each person with computer access.
Requirement 9: Restrict physical access to cardholder data.

Regularly Monitor and Test Networks
Requirement 10: Track and monitor all access to network resources and cardholder data.
Requirement 11: Regularly test security systems and processes.

Maintain an Information Security Policy
Requirement 12: Maintain a policy that addresses information security

To achieve each of these 12 high-level requirements, you must satisfy up to several dozen more specific requirements. Organizations that use WLANs have struggled to determine which of those specific requirements apply to their WLANs and the trusted Wi-Fi clients that interact with those WLANs.

In July 2009, the PCI SSC Wireless Special Interest Group (SIG) Implementation Team published a supplement entitled "PCI DSS Wireless Guideline". This supplement helps an organization ensure that its WLANs are compliant with PCI DSS v1.2 by explaining how PCI DSS applies to WLANs in organizations that handle cardholder information.

PCI DSS requirement 1.2.3 stipulates that you must install a firewall between every WLAN and the cardholder data environment. The firewall is to prevent Wi-Fi devices from gaining access to the cardholder data environment, unless applications that run on Wi-Fi devices require access to that environment, in which case the firewall is to "control" traffic. It is extremely difficult for a firewall to control traffic unless the firewall knows which devices are authorized to have access and which are not.

Recognizing that, in many organizations, WLANs have access to cardholder data, the supplement categorizes such WLANs as "in-scope" WLANs. As you may expect, requirements for in-scope WLANs are more rigorous than requirements for WLANs that are not in scope.

The best feature of the supplement is a flow chart, shown in Figure 3 at the right. The flow chart provides a handy summary of all PCI DSS requirements for a WLAN. An in-scope WLAN must meet these requirements:

- Change defaults on every AP, controller, and Wi-Fi client device
- Use 802.11i (WPA2-Enterprise) security
- Restrict physical access to WLAN devices
- Log all WLAN access centrally
- Detect and alert staff to WLAN intrusion attempts
- Develop usage policies for WLAN access

The key requirement is 4.1.1. To comply with PCI DSS, every WLAN and every Wi-Fi client device must use WPA2-Enterprise. This is the Wi-Fi security best practice that was discussed earlier in this paper.

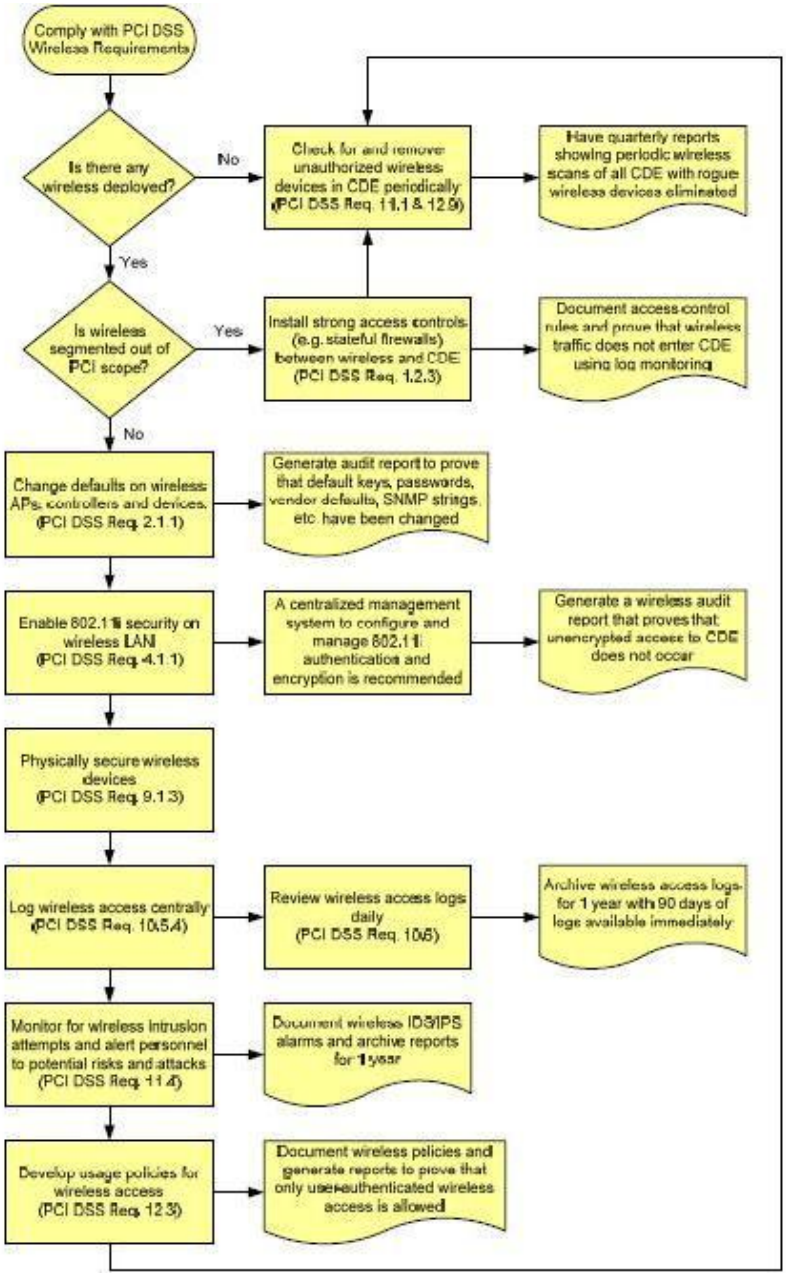

Figure 4: PCI DSS requirements for WLANs

Let's look a brief look at two other PCI DSS requirements that affect Wi-Fi client devices.

Change WLAN Defaults

By default, WLAN devices are "open", meaning that they have no security configured. To comply with PCI DSS, WLAN devices must be configured for WPA2-Enterprise. As a result, default configuration settings must be changed.

In environments where compliance with PCI DSS is a goal, most Wi-Fi client devices run a version of Microsoft Windows, such as Windows Mobile or Windows XP. All Windows versions include a WLAN configuration facility called Windows Zero Config (WZC), which enables a user or administrator to configure the device to associate to an AP, provided that the AP uses one of the authentication methods supported by WZC. WZC supports the configuration of two EAP types, PEAP with EAP-MSCHAPv2 as the inner method (PEAP-MSCHAP) and EAP-TLS. Many organizations, however, rely on other EAP types – such as EAP-TTLS, EAP-FAST, and PEAP-GTC – because those types provides a better "fit" with infrastructure and security requirements.

Build and Maintain a Secure Network

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

2.1 Always change vendor-supplied defaults before installing a system on the network…

2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.

To use an EAP type that is not supported natively by the Windows operating systems, a client device must include a software application called an 802.1X supplicant that supports that EAP type. Commercial supplicants are available for Windows XP but not for Windows CE or Windows Mobile. For the latter two operating systems, the Wi-Fi radio in the client device must include the supplicant.

To simplify administration of Wi-Fi client devices, you should choose devices with software that supports a wide range of EAP types and ensures that the devices are configured to connect only to your trusted WLAN using your chosen EAP type. Ideally, this software will support a means to distribute the same configuration to many devices with minimal intervention.

Best practice: Configure every trusted Wi-Fi client device to connect only to trusted APs.

Restrict Access to Wi-Fi Client Devices

Requirement 9 and its sub-requirements are designed to prevent physical access to data or systems that house cardholder data, because anyone with physical access has the ability to remove or make copies of data. WLANs, of course, enable client devices to gain access to data and systems even when the users of those devices have no physical access to the data or systems.

Restrict Physical Access to Cardholder Data

9.1: Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.

9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices.

Requirement 9.1.3 extends the restriction of physical access to "handheld devices" or, by extension, any client devices with Wi-Fi access to an in-scope WLAN. In other words, if a client device provides access to an in-scope WLAN and, through it, cardholder data, then you prevent unauthorized users from having (physical) access to that client device.

In reality, physical device security rarely is foolproof, and Wi-Fi client devices sometimes fall into the wrong hands. Because a stolen device probably runs a limited set of applications, a thief typically will not use a stolen device to break into the WLAN and the resources behind it. Instead, the thief will copy WLAN configuration information from the stolen device to a specially configured laptop that can be used to hack into the in-scope WLAN and steal cardholder information.

To limit threats from stolen Wi-Fi client devices, an organization should not store authentication credentials, such as a username and password, on a device. Instead, the organization should require a trusted user to enter a valid username and password at device startup. When authentication credentials are not stored on a stolen device, a thief cannot transfer those credentials to a hacking device.

Best practice: Do not store WPA2 (EAP) authentication credentials on client devices.

Summary: Security Best Practices for Wi-Fi Client Devices

The following best practices for Wi-Fi client device security and administration help to ensure compliance with PCI DSS:

- Ensure that a Wi-Fi client device can gain access to your WLANs only using WPA2-Enterprise with a strong EAP type.
- Configure every trusted Wi-Fi client device to connect only to trusted APs.
- Do not store EAP authentication credentials on client devices.