Laird TECHNOLOGIES

Innovative Technology for a Connected World

Wi-Fi© Client Device Security & HIPAA Compliance

Originally Published: September 2010

Updated: October 2012

A White Paper from Laird Technologies

Connecting medical devices to a hospital's Wi-Fi network improves workflow on both the clinical path and the financial path. With networked devices, a hospital delivers better care to more patients while billing those patients, and their insurance companies, quickly and accurately. Networking medical devices also enables technicians to monitor and manage those devices from a central point of control.

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

Contents

EXECUTIVE SUMMARY

Wi-Fi in Hospitals

According to ABI Research, the use of wireless local area networking (WLAN) technology in healthcare grew 60% globally in 2009. Worldwide sales of WLAN, or Wi-Fi®, technology into the healthcare market are expected to reach $4.9 billion in 2014. More than 500,000 Wi-Fi infrastructure endpoints, or access points (APs), are expected to be implemented in U.S. healthcare facilities in 2010, representing a 50% increase from 2009.

Even though Wi-Fi offers many potential benefits, a hospital will not rely on Wi-Fi unless the hospital has confidence that its Wi-Fi networks and devices will protect sensitive information, including electronic medical records (EMRs), which are transmitted over Wi-Fi or stored on networks that can be accessed through Wi-Fi. This white paper provides Wi-Fi client security best practices that protect the data that Wi-Fi clients transmit and receive and the networks to which those clients connect.

HIPAA: PROTECTING HEALTH INFORMATION

According to the Web site for the U.S. Department of Health and Human Services (HHS), the Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the HHS Secretary to develop regulations protecting the privacy and security of certain health information. To fulfill this requirement, HHS published two documents:

1. The HIPAA Privacy Rule, which establishes national standards for health information protection
2. The HIPAA Security Rule, which establishes a national set of security standards for organizations that handle protected health information that is held or transferred in electronic form.

The Security Rule seeks to protect the privacy of individuals' health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care. The Security Rule is found in the Code of Federal Regulations (CFR) Title 45, Part 164, Subpart C, entitled "Security Standards for the Protection of Electronic Protected Health Information". The sections of Subpart C are shown at the right.

For Wi-Fi client devices and networks, the key part of Subpart C is section 164.312, which lists technical safeguards. The section includes five standards and, for three of the standards, a set of implementation specifications or guidelines. Each guideline is either required (R) or addressable (A).

Subpart C—Security Standards for the Protection of Electronic Protected Health Information

§ 164.302 Applicability
§ 164.304 Definitions
§ 164.306 Security standards: General rules
§ 164.308 Administrative safeguards
(a)(1) Security Management Process
(a)(2) Assigned Security Responsibility
(a)(3) Workforce Security
(a)(4) Information Access Management
(a)(5) Security Awareness and Training
(a)(6) Security Incident Procedures
(a)(7) Contingency Plan
(a)(8) Evaluation
(b)(1) Business Associate Contracts
§ 164.310 Physical safeguards
(a)(1) Facility Access Controls
(b) Workstation Use
(c) Workstation Security
(d)(1) Device and Media Controls
§ 164.312 Technical safeguards
(a)(1) Access Control
(b) Audit Controls (R)
(c)(1) Integrity
(d) Person or Entity Authentication (R)
(e)(1) Transmission Security
§ 164.314 Organizational requirements
§ 164.316 Policies, procedures, documentation
§ 164.318 Compliance dates

(R) required (A) addressable

Error! Reference source not found. provides details on §164.312.

Table 1: §164.312 of HIPAA Security Rule

(a) **Access control:** Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).

Implementation guidelines:
(i) **Unique user identification (R):** Assign a unique name and/or number for identifying and tracking user identity.
(ii) **Emergency access procedure (R):** Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
(iii) **Automatic logoff (A):** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
(iv) **Encryption and decryption (A):** Implement a mechanism to encrypt and decrypt electronic protected health information.

(b) **Audit controls.** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

(c) **Integrity.** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Implementation guidelines:
Mechanism to authenticate electronic protected health information (A): Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

(d) **Person or entity authentication.** Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

(e) **Transmission security:** Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

Implementation guidelines:
(i) **Integrity controls (A):** Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.
(ii) **Encryption (A):** Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

To satisfy the requirements of HIPAA, a hospital Wi-Fi system needs:

- Strong, mutual authentication between every authorized client device and a trusted hospital network to ensure that:
  - Only trusted Wi-Fi clients can gain network access
  - Trusted Wi-Fi clients are not tricked into connecting to an untrusted network
- Strong encryption of all data, especially protected health information, that is transmitted between a Wi-Fi client and the hospital network
- Before looking at the type of Wi-Fi security that satisfies HIPAA requirements, let's consider the threats to sensitive information when Wi-Fi security is not as strong as it should be.

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 hospital, Wi-Fi radios in computing devices communicate with Wi-Fi radios in infrastructure devices such as access points (APs) that are connected to the hospital's wired network. The radio waves that travel between the devices can reach waiting rooms and other public areas and even "bleed" through the walls of the hospital to parking lots and other nearby areas. Those RF signals can be viewed by a computing device that is hundreds of meters from the sending and receiving stations, provided that the computing 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 the hacker 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.

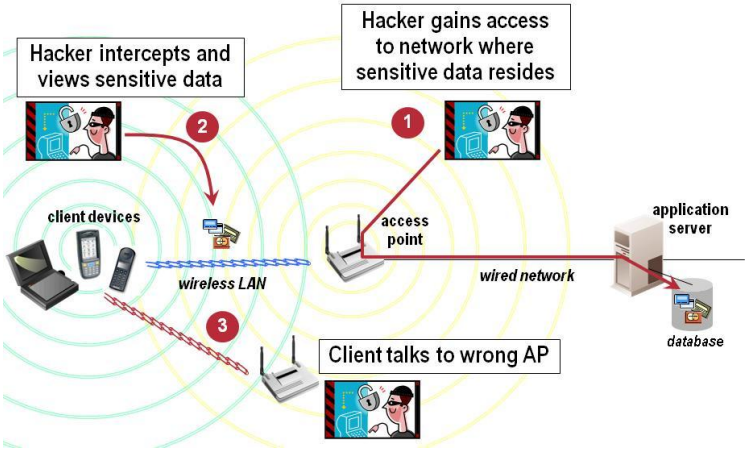

Figure 1: Wi-Fi security threats

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 PSK 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 2 compares popular EAP types that are used with 802.1X authentication:

Table 2: 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 successful, then the hacker has determined the PSK and 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 is 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 the message integrity check (MIC) key and the plain text of the packet from an encrypted ARP packet. The execution time of this attack is 12-15 minutes.
- The attack by the Japanese scientists can obtain the same information from an encrypted ARP packet 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. Earlier this year, the Wi-Fi Alliance announced that it is 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, which 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.

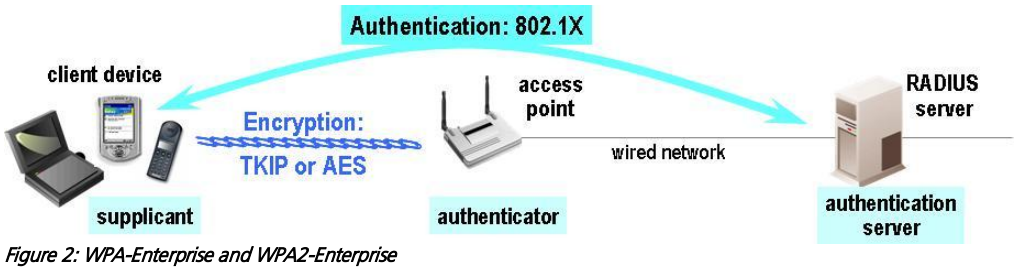

Figure 2: WPA-Enterprise and WPA2-Enterprise

As shown in Figure 2 above, 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 earlier 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.

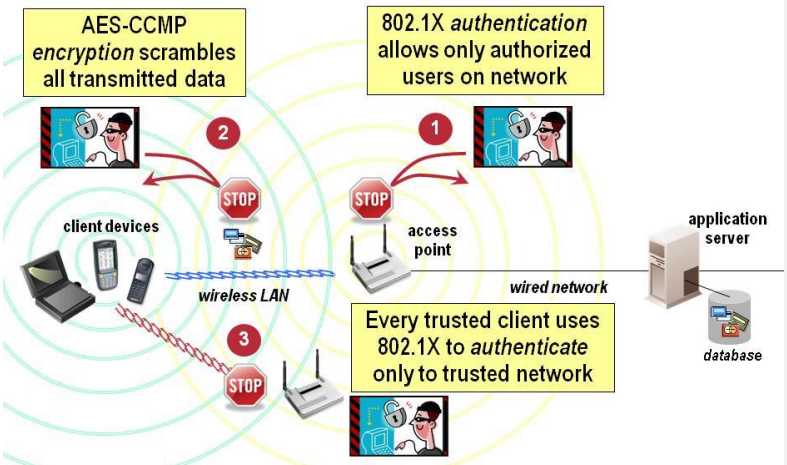

Figure 3: WPA2-Enterprise and Wi-Fi security threats

- **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.)

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.

Connect Only to Trusted APs

By default, WLAN devices are "open", meaning that they have no security configured. To ensure that a client device uses WPA2-Enterprise, you must change that device's default configuration.

On devices that run a version of Microsoft Windows, such as Windows Mobile or Windows 7, you can use a native WLAN configuration facility called Windows Zero Config (WZC). WZC supports the configuration of only two EAP types, PEAP with EAP-MSCHAPv2 as the inner method (PEAP-MSCHAP) and EAP-TLS. Many organizations rely on other EAP types – such as EAP-TTLS, EAP-FAST, and PEAP-GTC – because those types provide a better "fit" with infrastructure and security requirements.

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. Supplicants are available for and are even bundled with devices that run Windows 7 or Windows XP. For devices that run another operating system, 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.

Protect Authentication Credentials

Many hospitals try to prevent unauthorized users from having physical access to certain devices that can connect to the hospital network. Physical device security is rarely 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 will not typically 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 HIPAA compliance:

- 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.