Securing Wireless Technology for Healthcare

Save to myBoK

This practice brief has been updated. See the latest version here. This version is made available for historical purposes only.

With the advent of wireless networking, many organizations are exploring how wireless mobility can change the way they work. Healthcare organizations were among the first to adopt wireless for its obvious advantage of data portability and the ability to integrate voice communication. Many see emerging wireless technology as the next step toward the realization of the electronic health record. However, with this convenience comes a series of risks regarding data confidentiality and reliability.

The Health Insurance Portability and Accountability Act of 1996 mandates that steps be taken to secure electronic protected health information. This practice brief serves as a guideline to help ensure that due diligence has been exercised on the part of healthcare organizations and that risks pertaining to wireless networking are defined and addressed with respect to an organization's bottom line. It focuses on wireless technology from the perspective of mobile client end-user devices and wireless infrastructure devices in a dynamic environment. The workplace is considered a dynamic environment because it changes with the movements of its users. As such, it is conducive to wireless technology. Typically, static environments are those that deploy "fixed" wireless installations—the client end-user device is in a fixed position and does not move.

History

Digital spread spectrum radios, developed in the 1960s and 1970s, fostered the development of today's wireless local area networks (WLANs). Since this technology was in use exclusively by government agencies, there was no limitation on radio frequency (RF) spectrum use, and as a result, available bandwidth was very high. Early adopters of spread spectrum radios, such as the Central Intelligence Agency and the National Security Agency, used the devices mainly for covert communications.

In the 1980s through the early 1990s, based on a partnership between Motorola and IBM, narrow band ultra high frequency (UHF) was utilized, yielding the first commercially available radios for wireless bar-coding and other narrow band UHF-dependent applications that required speeds of 19.8 Kbps. This is also known as cellular digital packet data, familiar to the many who use cell phones.

In the early 1990s the Federal Communications Commission created the industrial scientific medical band by opening to the public the wireless spectrum from 902 MHz to 928 MHz. Speeds of just under 1 Mb (840 Kbps) were attainable.

In 1993 the use of wireless in the healthcare environment made its debut. At this time both frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) existed and were actively competing for market share. Although similar in range, DSSS (2 Mb at this time) had the advantage of speed, while FHSS (1 Mb at this time) had the advantage of frequency agility.

In the mid-1990s, a well-known semiconductor manufacturer named Intersil, which was owned by Harris Corporation, developed a DSSS chipset that allowed as many as 50 companies to develop their own 2.4 GHz WLAN radios. These radios primarily were used for data communications. However, they were not popular due to the absence of standards, poor security, and inadequate performance.

In the late 1990s the Institute of Electrical and Electronics Engineers (IEEE) ratified the important WLAN standard that allowed for over-the-air transmission speeds of up to 11 Mbps (802.11b). The ratification of the WLAN standard was the turning point for wireless device use and for interoperability as we know it today.

With the addition of new speed improvements (802.11a and g) and prominent security standards (802.11i), WLAN has been adopted by many healthcare organizations. WLAN is considered a reliable and practical medium for data, voice, and video, and it is an integral part of most mainstream wireless network deployment considerations.

Basics of Deployment

Configuration options are available when installing a wireless network. These referenced options can be used in part or all simultaneously.

- **Service set identifier (SSID)**—The SSID establishes a "network name" for the wireless network. Users specify this name in their respective client device utility to connect wirelessly to a network. This name will be visible. Therefore, it should be alphanumeric and not promote interest to casual users, in particular to eavesdroppers. Unless you configure it not to, your wireless equipment will broadcast your SSID in an effort to find wireless users. Most wireless infrastructure equipment allows the SSID broadcast to be disabled. This will keep the SSID from being detected by all but the most advanced wireless analysis applications. *Correct example*: 11603; *incorrect example*: Mercy Hospital.
- **Wired equivalent privacy (WEP)**—WEP is a hardware-based encryption standard provided by the access point, the hardware device that acts as a communication hub for wireless network users. WEP is enabled by entering a key in hexadecimal format. (Hexadecimal is a convenient way to express binary numbers in modern computers in which a byte is almost always defined as containing eight binary digits.) WEP is typically available in 40-bit or 128-bit encryption, the 40-bit keys consisting of 10 characters in length and the 128-bit keys consisting of 26 characters in length. Programming a WEP key that does not change produces a "static" WEP key. Several random WEP key generators are freely available on the Internet and are easily found by a Web search. The chosen WEP key will need to be entered both in the access point configuration and the wireless client utility.
- **Media access control (MAC) address filtering**—This is a database of authorized client devices by MAC address, resident on the access point. Only client MAC addresses specified in this access list are allowed to associate, the final operation of the authentication process when a wireless network user attempts to access the wireless network. For large deployments, management of MAC addresses can become tedious because MAC addresses need to be registered on each access point.
- **Range and intended coverage**—Perhaps the most overlooked security risk with wireless networking is simply providing unintentional wireless coverage in areas of high risk. Intentional wireless coverage areas are surveyed in an operation referred to as a site survey to ensure that required data rates and signal strengths are met. It is recommended that areas of risk, such as parking lots, waiting rooms, and public areas, be covered only on an as-needed basis.
- **User authentication**—Wireless users can be authenticated via the proposed Internet engineering task force standard, remote authentication dial-in user service (RADIUS) or a variant. Most server operating systems have a RADIUS compliant user authentication database available by default.
- **Intrusion detection**—Some larger organizations use intrusion detection systems (IDSs) to identify incidents via signatures or fingerprints on an event-by-event basis. Unfortunately, IDS is reactionary; most systems do nothing to stop an attack in progress. (In a reactive system, the IDS responds to the suspicious activity by logging off a user or by reprogramming the firewall to block network traffic from the suspected malicious source. In a passive system, the IDS detects a potential security breach, logs the information, and signals an alert.) Host-based IDS can be helpful in determining if anything was compromised in the attack. Logs and activity auditing can be very useful in troubleshooting and trending. They can also be used as evidentiary information in the case of an attack.
- **Use of higher-level protocols**—The use of higher-level protocols to further secure information traversing the wireless network must be considered. This includes secure socket layer, secure shell, or virtual private networking.

Risks

The risks associated with wireless networking are dynamic based on environment specifics and equipment configuration. The following are known vulnerabilities:

- **Rogue access point**—This is an unauthorized access point on the wired infrastructure. Access points that do not conform to an organization's security policy or are left unsecured can allow unauthorized access to an organization's wired network and pose a significant risk to the confidentiality and integrity of protected health information.
- **Hardware**—Wireless infrastructure devices that are left with factory default settings or are improperly configured can allow a hacker easy access to the wireless network.
- **Sniffing**—Sniffing is passive monitoring that allows an eavesdropper to listen to all the transmissions on a wireless network. The ability to easily "sniff" dictates the need for encryption. In a data packet, the payload or data portion is

encrypted, leaving all of the information in the header in clear text. This can include the systems SSID, source and destination MAC address, and parts of the header that allow the WEP key to be compromised.

- **Identity theft**—All network adapters have an identifying MAC address that differentiates them from all of the other users on a network. Intruders can get the MAC addresses from authorized clients by passive sniffing and then forge or "spoof" the address on their wireless adapter to gain wireless access.
- **Replay attacks**—An attacker records a valid user's authentication transmission sequence and plays it back later to gain access.
- **WEP key vulnerabilities**—Static WEP keys can be compromised through passive monitoring or sniffing of data. Depending on the amount of traffic on the WLAN, the technique used to break the encryption can be very time consuming. Cracking WEP keys typically requires the collection and analysis of more than 1,000,000 transmitted frames. This operation only needs to be performed successfully once with static WEP keys to compromise all WEP-encrypted data until the WEP key is changed.
- **Man-in-the-middle attacks**—An example of such an attack is when a hacker forces a wireless device between a user transmission and an access point. Traffic is routed through the hacker's device and recorded. Wireless clients continually send probe requests to find the access point with the strongest signal. This is a way for a hacker to remove authorized client devices so that the hacker can forge or spoof their MAC addresses on the network. This is also occasionally used as a denial of service (DoS) attack.
- **Jamming**—Since wireless operates in the radio frequency spectrum, transmissions that overlap into the same frequency can cause interference. This intentional type of interference is called jamming. Jamming the wireless channel can force WLAN users to disconnect from access points.
- **MAC flooding**—Flooding the network with MAC addresses or association attempts uses up processing resources on the wireless hardware causing users to disconnect. MAC flooding is used primarily as a DoS attack or as an attempt to force a reboot of the network hardware.

Security Standards

- **Protected extensible authentication protocol (PEAP)**—PEAP was the first security standard to be adopted by Microsoft. Support was later included in Windows XP. Unfortunately, PEAP requires server-side security certificates involving additional administrative overhead. It is still vendor proprietary at this point, and few other third-party vendors have released support for it.
- **Wi-Fi Protected Access (WPA)**—Introduced by the Wireless Fidelity (Wi-Fi) Alliance, WPA is the only new wireless security standard based on open standards. Based on the IEEE 802.11i wireless security protocol, WPA addresses all of the current WEP and "replay attack-based" vulnerabilities. WPA requires 802.1X authentication, as well as temporal key integrity protocol and message integrity check (see below).
  Most new off-the-shelf wireless equipment is WPA ready although existing access points and client devices may have firmware upgraded to support WPA.
  WPA secures all versions of 802.11 devices, both multiband and multimode. It is forward- and backward-compatible and runs on existing Wi-Fi devices as a software download. WPA devices should work well with forthcoming 802.11i devices (also known as WPA2), according to the Wi-Fi Alliance.
- **Temporal key integrity protocol (TKIP)**—TKIP dynamically generates four WEP keys based on each wireless user's session key. The WEP keys are then rotated every 10,000 packets. This prevents WEP key attacks simply by changing the WEP key often enough that even if a single key could be compromised, the hacker's window of opportunity would be ineffective. Since a new session key is created every time a user associates to an access point, the compromised key would be invalid for any other session.
- **Message integrity check (MIC)**—To prevent replay attacks, MIC uses a frame counter to establish if frames are arriving at the access point out of sequence. If this happens, the frames are simply dropped or ignored.

Authentication

Security is either provided by an authentication server including extensible authentication protocol (EAP) transport, EAP transport layer security (EAP-TLS), EAP-tunneled transport layer security (EAP-TTLS), or protected extensible authentication protocol. In smaller deployments, preshared key (PSK) authentication from the client device can facilitate first-time user authentication. This gives the user the advantage of dynamic WEP keys and MIC without a full-blown RADIUS deployment.

Steps to Deploying WPA

The WPA firmware upgrade is available from most hardware manufacturers' Web sites. Not all manufacturers have released a WPA update. However, most should have posted a tentative release date. Download the update and apply it to the access point. There will be a choice to specify an authentication server or to use PSK security. If the PSK is chosen, a password is entered on the WPA-enabled access point. When the client device is WPA-enabled, the user is prompted for the preshared key. When the user associates, the PSK is verified, and the client device is authenticated.

Technology

Presently there is no shortage of wireless vendors offering equipment to establish wireless coverage in healthcare facilities. Finding the ideal equipment to suit security and bandwidth needs requires careful consideration. Guidelines in this practice brief can be used as best practice options for measuring the value of equipment selection.

Return on Investment

Quantifying the return on investment of a WLAN can present a difficult challenge. Through analysis of both tangible and intangible benefits, the true return can be realized as a blended value proposition to most organizations. As Cisco Systems suggests, WLAN intangible benefits "impact the users' working lives." This theme is clearly repeated with comparison of studies performed by several leading manufacturers of wireless infrastructure and client components.

The studies indicate that an average of 11 extra minutes of productivity per week can pay for a WLAN. Reduced cabling costs, easier setup, and overall reduction of networking costs are cited as the major IT and MIS motivators. Customer and patient care gains in productivity are clear as well for input error control as the data collection device moves with the user. Other factors not as easily measured monetarily can include user satisfaction and faster decision making.

Recommendations

- **Conduct a comprehensive site survey** of the intended coverage area when your healthcare organization has made its decision to deploy a WLAN. The site survey should be conducted in three dimensions. Access points adjacent to, above, and below your location can affect performance and stability for WLAN users later.
- Take appropriate time in **researching the type of equipment** that best suits your organization's budget and bandwidth requirements. You will need at least one access point based on your equipment selection and a client adapter best representing the average adapter in use by your wireless users.
- Conduct the site survey by **temporarily placing an access point** in an area where coverage is most needed or where electricity and data cable exists or can be easily provided. The placement of the survey access point should be as close as possible to the intended final placement location. Slowly survey the area to be covered by connecting to the access point with a wireless client device and walking through rooms paying close attention to changes in connection speed and signal strength. It is not necessary to have a wired Ethernet connection to the access point during this phase.
- **Use directional antennae** to further isolate the area of intended RF coverage, much like the beam of a flashlight. This directional approach is generally more desirable when designing coverage areas than omni-directional antennae that radiate signals outward in all directions, similar to a light bulb.
- Pay special attention to the transmission power of your access points and client devices. To achieve a good wireless footprint in your environment, it is important that the RF cells overlap slightly. This helps wireless users on the move to roam from cell to cell with little or no interruption to their service. In general, low-power wireless networks are more secure and typically perform better in many environments.
- Use careful channel selection to overcome transmission collisions. Current wireless network equipment is half-duplex, meaning only one wireless device associated to a single access point can send or receive data at one time. If multiple devices attempt to transmit data at the same time, a collision can occur. This obstacle is overcome mainly by channel selection. Of the 11 channels available to 802.11b users, only three channels do not overlap. Using a logical channel design, large numbers of access points can be deployed in a relatively small area using only the nonoverlapping channels.

The techniques required to perform a comprehensive WLAN site survey and design are well beyond the scope of this practice brief. Typically a junior radio frequency engineer will spend considerable time in the field with senior level staff members in order to be competent performing this type of analysis. Although performing a WLAN deployment looks simplistic and attractive from the average IT/MIS staff person's perspective, a WLAN deployment is not recommended for deployments beyond several access points without the involvement of experienced team members entrenched in the design process.

Common pitfalls such as multipath fades, client contention, high numbers of "retries" regarding hidden node effects, and numerous security implications can be avoided by applying careful consideration and in involving experienced team members.

Summary

Wireless networking can be a very complex science, requiring an understanding of physics and the electromagnetic spectrum. While the radio theory behind the technology can be challenging, a basic understanding of wireless networking can be sufficient for small-scale deployment.

Numerous security mechanisms are available to wireless technologies, making it practical, scalable, and affordable for healthcare organizations. The decision on the selected security model should take into account the needs for additional server hardware and administrative costs. Where wide area network connections exist between cooperative organizations, deployment of a distributed security model can be considered to reduce administrative overhead.

The wireless approach chosen should be dynamic and concentrate on the organization's specific environmental needs. Aspects of organizational mission, operations, service level, and budget allotment as well as an organization's risk tolerance are all part of the balance in the decision to deploy wireless technology.

Prepared by

John Retterer
Brian W. Casto, BSEE, CET

Acknowledgments

Ian Alexander, MD
Beth Hjort, RHIA, CHP
Deborah Kohn, MPH, RHIA, CHE, CPHIMS
Michael Mathews, PhD, CCIE, CISM, CISSP, MCSE2K, RHCE, SCNA/SCSA
Dale Miller, CISSP, CHP
Don Mon, PhD
Harry Rhodes, MBA, RHIA, CHP

References

Alexander, I.J. "Securing Your Wireless Network." *AAOS Bulletin* 51, no. 2 (2003).

Cisco Systems. "2003 Wireless LAN Benefits Study." Available online at www.cisco.com/application/pdf/en/us/guest/products/ps4570/c1031/cdccont_0900aecd800cf91f.pdf.

Intel. "Wireless LANs—Linking Productivity Gains to Return on Investment." White paper available online at www.intel.com/business/bss/infrastructure/wireless/roi/productivity_gains.pdf.

John Retterer *is director of engineering and Brian Casto (bcasto@icinetworks.net) is president and CEO at ICI Networks.*

Article citation:
Retterer, John. "Securing Wireless Technology for Healthcare." (AHIMA Practice Brief)

Journal of AHIMA 75, no.5 (May 2004): 56A-D.