Securing Wireless Technology for Healthcare (2013 update) - Retired

Save to myBoK

Editor's note: This update supplants the May 2004 practice brief "Securing Wireless Technology for Healthcare"

Overview

Wireless local area network (WLAN) environments have evolved from simple, unmanaged stand-alone *access points (APs)* to organizationally managed systems with centralized control and monitoring. These coordinated APs provide healthcare organizations with well-defined configuration, control, monitoring and management features that enable organization-level WLAN installations. One concern that has constrained healthcare organizations in their growth of WLANs is the question of how secure they are and how best to secure them. Fortunately, the evolution of wireless security has reached the point where WLANs can be as secure as a wired network with the proper configuration and implementation.

Healthcare organizations need to manage the basics of securing wireless technology. They need to be able to provide the appropriate level of access to different users including guests. This practice brief serves as a guideline to help ensure that due diligence has been exercised on the part of healthcare organizations and that information risks pertaining to wireless technologies are adequately identified and managed.

Note: Key terms underlined throughout the practice brief are further defined in Appendix A.

Current State of Wireless Technology in Healthcare

Today, WLANs are a standard extension of corporate networks. Healthcare organizations use a variety of wireless technologies. Trends such as Bring Your Own Device (BYOD) for users as well as patients and visitors are commonplace, including the expectation of continuous *Wireless Fidelity (Wi-Fi)* access and availability. Due to these expectations, healthcare organizations are enhancing their wireless network infrastructure and ensuring security is adequately addressed.

Enterasys, a global provider of wireless network infrastructure and security solutions, conducted a study in February 2013 on the current state of wireless networks in healthcare.[1] They surveyed leading healthcare organizations on topics such as how they plan to support biomedical devices and BYOD while keeping their WLANs secure. Some of the survey results revealed:

- 30 percent of hospitals currently do not offer Wi-Fi to patients and guests
- 32 percent of hospitals are not using technology to enforce their BYOD policies
- 63 percent of respondents replied that their Wi-Fi is very important or critical to the success of achieving government regulations such as the "meaningful use" EHR Incentive Program
- 71 percent of hospitals have biomedical devices accessing the clinical Wi-Fi
- 82 percent of hospitals are allowing mobile EHR access on physician-owned devices
- 78 percent of hospitals are allowing some physicians to utilize personally owned devices at the point of care

This survey illustrates the wide-ranging use and prevalence of WLANs in healthcare today. WLANs are being increasingly entrusted with carrying mission-critical applications such as database access, voice over Internet protocol (VoIP), e-mail and Internet access. Securing a WLAN is no easy task given the mobility and diversity of organizational needs and demands in healthcare. Additionally, a variety of threats must be addressed in order to provide the expected availability as well as security for any WLAN.

Common Threats to WLANs

WLANs are an easily intercepted medium that does not require a physical connection to establish a network. Signals can leak outside an organization through walls, floors, and ceilings. A WLAN signal can be intercepted with a low probability of detection from either several miles away or right next door. WLAN exploits or compromises do require physical proximity to the target network. As a result, they are less likely to occur and less susceptible to attack than threats delivered over the Internet. However, WLANs are still vulnerable to several means of attack. Reasons for compromise include continued use of legacy equipment, weak authentication protocols, unencrypted public and private WLANs, configuration errors and personal devices. The following illustrates some of the common threats affecting WLANS in healthcare:

- **Denial of Service (DoS):** Any instance that prevents authorized users from performing their duties may be considered a DoS event. The *802.11* WLAN transmission standards are a shared medium so they are susceptible to DoS attacks. DoS events can occur within any component of the IT infrastructure. WLAN DoS attacks are easy to launch from outside the facility by using freely available tools at the target (i.e., Slowloris, Sockstress, High Orbit Ion Cannon (HOIC) and Low Orbit Ion Cannon (LOIC). For example, a common DoS attack sends many simultaneous requests to a website asking to generate a report. The database server supporting the website queries can reach 100 percent utilization making it inaccessible to user activity and resulting in a DoS.
- **WLAN Scanning and Monitoring:** Attackers use a variety of freely available tools to scan and discover the existence of WLANs and their *service set identifiers (SSIDs)* such as Kismet or NetStumbler (PC-based) and KisMAC or MacStumbler (Mac-based). Once a WLAN is discovered, the attacker can look for rogue APs, connect to ones that will accept an ad hoc connection, eavesdrop on wireless traffic, or try to circumvent authentication procedures. If successful, then the attacker can further probe servers and databases that are connected to the wired network. Data sent over WLANs can be captured by attackers within proximity of the target network.
- **Rogue or Unauthorized APs:** Rogue or unauthorized APs represent a threat to healthcare organizations by creating an open entry point to the network that bypasses existing security measures. This can include laptops, mobile devices, wireless bar code scanners and printers acting as APs. Attackers can use any insecure AP as a path to penetrate the network's security. WLAN APs are inexpensive and easy to install. This may be accomplished by simply plugging an AP into an Ethernet port on the wired network. Unauthorized WLAN APs can be connected to a network unwittingly or with malicious intent without the knowledge of the IT department. Since rogue APs are typically deployed by employees looking for quick wireless access, they are usually installed without standard security controls and can easily be misconfigured. Even healthcare organizations that do not allow the use of WLANs must secure themselves against insertion of rogue APs and the use of ad hoc wireless networking by workstations and other devices.
- **Misconfigured APs:** The latest 802.11 standards offer a variety of relatively complex configuration options and variable client capabilities. Prioritization and segmentation can further complicate the configuration process. APs can be left with factory default settings or improperly configured, which allows attackers easy access to the WLAN. Most APs allow restrictions on which devices can connect to it based on filtering of *media access control (MAC)* addresses of authorized devices. MAC address filtering can provide some control over which devices can connect to your network. Attackers can copy MAC addresses from the WLAN and change the MAC address on their laptop to match the valid MAC address. There are still legacy products that use *Temporal Key Integrity Protocol (TKIP)* and *Wired Equivalent Privacy (WEP)*. TKIP is vulnerable to *message integrity check (MIC)* attacks. The weaknesses of the WEP protocol have been widely documented. Although vendors offer patches to address these vulnerabilities once discovered, driver updates are not typically distributed automatically along with *operating system (OS)* updates.
- **Endpoint Attacks:** Numerous exploits have been published to take advantage of vulnerable Wi-Fi drivers. Automated tools such as Metasploit can be used to launch endpoint attacks with minimal effort. For example, vulnerabilities can result when patches are not applied in a timely manner. Patches are usually issued by vendors once vulnerabilities are discovered. Wi-Fi driver patches are not typically distributed automatically with operating system updates that would require a manual application.
- **WLAN Malware:** The number of mobile malware threats is on the rise and cybercriminals are finding more ways to infect mobile devices. Healthcare organizations are at a higher likelihood to encounter malware infestations on biomedical devices due to outdated operating systems and vendor resistance to upgrade or reconfigure. Most wireless-enabled biomedical devices and supporting systems have inadequate security and are difficult to patch. An August 2012 report was presented to the US Food and Drug Administration (FDA) by the US Government Accountability Office (GAO) entitled "FDA Should Expand Its Consideration of Information Security for Certain Types of Devices."[2] This report highlighted the vulnerabilities in biomedical devices such as heart defibrillators and insulin pumps and how they could be maliciously manipulated.

Wireless Security Recommendations

The best defense against any threat is to be proactive in your security efforts. The following are basic wireless security recommendations for ensuring your WLAN is adequately protected:

- **Implement WLAN Policies and Educate Workforce:** Every healthcare WLAN needs a policy to provide direction on addressing and managing its security. WLAN policies should begin with the basics of forbidding unauthorized APs that can circumvent security as well as the unauthorized reconfiguration or alteration of APs and other WLAN technologies. The policy should also limit WLAN traffic to operate on set channels and connection speeds. By establishing a set channel for each AP, all traffic on the other channels can be more easily identified as suspicious. Workforce education is important and staff should be advised to only connect to provisioned WLANS when conducting business. Also, educate the workforce to use *virtual private network (VPN)* technology such as *Internet Protocol Security (IPSec)* and *Secure Sockets Layer (SSL)* when connecting to a public WLAN to conduct business. Deploying a wireless infrastructure means developing, managing, and executing a scalable wireless security policy with an appropriately educated workforce.
- **Conduct Wireless Security Assessments:** WLANs are just like wired networks in that they need to be assessed to proactively detect weaknesses and vulnerabilities. The same shareware used by attackers (Kismet, NetStumbler and MacStumbler) can be leveraged to assess the airwaves for rogue/unauthorized APs and vulnerabilities. Commercially sold scanners are available for purchase as well. The wireless security assessment typically includes an inventory of wireless technologies, as well as nearby wireless connections. A review of existing wireless policies and an assessment to determine if they are being followed, should also be conducted. Upon completion of the assessment, a comprehensive report should document vulnerabilities and recommend prioritized remedial actions.
- **Implement Configuration Management and Patch Management:** Keep current on patches, configurations and policy enforcement as well as checking to ensure all wireless APs are secure and up-to-date with the latest patches and configurations. This includes following the guidance outlined in this Practice Brief.
- **Restrict All Access Points and Devices:** Ideally, healthcare organizations should limit access to the WLAN based on physical proximity. In a wired network, individual ports may be enabled or disabled to control connectivity to the LAN. With WLANs, the *radio frequency (RF)* signal propagates to areas that might not initially be considered, such as a parking lot or reception area. The ability to manage connectivity by user location can improve security by ensuring that connections outside clearly defined areas are not permitted. Locking down Ethernet ports on the wired network will prevent rogue or unauthorized APs and devices from arbitrarily connecting. Organizations should deploy enterprise-class APs that offer advanced security and management capabilities. Change all default passwords and features. The SSIDs should be changed to names that are meaningless to outsiders. An SSID of "cardiology department" provides additional information for an attacker. Healthcare organizations should also configure APs to disable the broadcast mode where it constantly broadcasts its SSID in search of devices with which to connect. By turning this default feature off, devices must know the SSID in order to connect. If possible, install APs out of sight from visitors, patients, and the general public, such as hiding them on the other side of dropdown ceiling tiles. This conceals the existence of a WLAN from casual inspection and will also make the location of the AP more difficult to determine.
- **Ensure Proper Authentication:** Establishing a user's identity is the first step to controlling access to specific network resources. Authentication methods should be deployed with VPNs and RADIUS servers. VPNs can employ strong authentication and encryption mechanisms between the APs and the network. *RADIUS* servers can be used to manage authentication, accounting, and access to network resources. While VPNs can be a secure solution for WLANs, one-way authentication VPNs are still vulnerable to exploitation. Mutual authentication wireless VPNs offer stronger authentication controls.
- **Deploy Intrusion Detection and Protection Systems (IDS/IPS):** While healthcare organizations may have already deployed intrusion-detection systems for their wired networks, only a WLAN-specific IDS/IPS can protect a wireless network from attacks in the airwaves before the traffic reaches the wired network. The discovery of rogue/unauthorized APs and wireless vulnerabilities can be more effectively accomplished with 24/7 monitoring of the WLAN. This can best be accomplished through IDS/IPS. Continuous monitoring can identify when and where the rogue/unauthorized APs first appeared, who it connected to, how much data was exchanged and the direction of traffic in real time.
- **Enable Strong Encryption:** Healthcare organizations that implement WLANs must ensure that they enable adequate encryption controls to prevent unauthorized access to data. *WPA2* is the most secure encryption method available for

wireless networks. WPA2 support is mandatory in all Wi-Fi certified devices and is widely available. *WEP* was the original wireless encryption protocol but it is unsecure and should never be used. In fact, the use of WEP was prohibited as of June 30, 2010 by the *Payment Card Industry Data Security Standard (PCI DSS)*[3]. WPA replaced WEP with a stronger encryption technology called *Temporal Key Integrity Protocol (TKIP)* with Message Integrity Check (MIC). WPA should not be used either. WPA2 provides the strongest encryption available using the *Advanced Encryption Standard (AES*), dynamic key exchange and strong authentication based on 802.1X. Healthcare organizations should also deploy a VPN using *Internet Protocol security (IPsec)* or *Secure Sockets Layer (SSL)* for users when they conduct business on a public or untrusted network.

- **Implement Network Segmentation:** The addition of guest access and employee-owned devices is driving healthcare organizations to use multiple SSIDs to segment WLAN traffic. As with guest access, segregating BYOD traffic is one technique used to protect the organizational infrastructure. Segmenting the network also provides flexibility in content filtering and traffic monitoring to detect inappropriate access or malware, selective policy enforcement by device class, and selective endpoint monitoring. Offering guest access enables an Internet connection while isolating the visitor from the organization's sensitive information. The WLAN implementation should support multiple SSIDs to allow traffic segregation. At the minimum, there should be two SSIDs: one for traffic from organization-managed devices and one for unmanaged guest devices. Additional SSIDs could be added to support employee-owned or physician-owned devices. Biomedical devices should also be on a separate WLAN. Contractors could be treated as employees and allowed access to the organization-owned network, placed in the employee-owned equipment network, or given a separate SSID for their own use.
- **Deploy Network Access Control (NAC):** NAC is a proactive, end-user networking solution for wired and WLAN connections that identifies potential security gaps or problems on a device before it accesses the network. NAC enforces security policies on the WLAN so that only authorized and safe users and devices are allowed access to appropriate resources. With BYOD challenges, NAC can profile personally owned devices and apply controls that are consistent with existing policy. NAC's ability to detect what type of device is connecting to the network and apply limited access capability when required is a core component of managing risk.
- **Protect Wireless Medical Devices:** In August 2013, the FDA published a guide on the use of wireless devices in healthcare settings. The document, *"Radio Frequency Wireless Technology in Medical Devices—Guidance for Industry and Food and Drug Administration Staff,"*[4] contains recommendations aimed at wireless biomedical devices. As malicious intent or unintentional interferences become more prevalent and publicized with biomedical devices, manufacturers are being challenged to respond and take action. Unfortunately, the majority of biomedical device manufacturers do not typically have the internal skill necessary to address existing or emerging security issues. As a result, they struggle to build security into their hardware, software, and firmware platforms. Biomedical device manufacturers should review the GAO and FDA reports and become involved with workgroups developing security guidelines. They should also leverage existing or acquire security knowledge necessary to develop and adapt more robust security protections. Healthcare organizations should work with these biomedical device manufacturers' product development, risk, regulatory, and validation teams on existing security issues to determine viable options.

Summary

The state of securing wireless technologies has significantly improved over the years. Healthcare WLANs can be effectively hardened against intrusion and misuse. However, end-to-end security still cannot be assumed. Simply enabling encryption will not make applications running over WLANs "secure." Technologies, products and threats will continue to emerge and evolve. Healthcare organizations will need to keep abreast of new threats, analyze their risk, and take appropriate action.

The best approach to take towards wireless security is to be constantly vigilant. Ensure the security used on a WLAN stays current as the standards, technologies, and threat environment changes. Whatever approach is chosen, it should be scalable, dynamic, and address the organization's specific business and environmental needs. Aspects of organizational mission, operations, service level, budget allotment, as well as risk tolerance are all part of the balance in effectively securing wireless technology.

Appendix A: Securing Wireless Technology for Healthcare Glossary

Definitions

802.11 Standard: an evolving family of specifications for wireless LANs, developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). 802.11 standards use the Ethernet protocol and carrier sense multiple access with collision avoidance (CSMA/CA) for path sharing.

802.1X Standard: designed to enhance the security of wireless local area networks (WLANs) that follow the 802.11 standard. 802.1X provides an authentication framework for WLANs allowing a user to be authenticated by a central authority.

Access Point (AP): a station that transmits and receives data (sometimes referred to as a transceiver). An access point connects users to other users within the network and also can serve as the point of interconnection between the WLAN and a fixed wire network. The number of access points a WLAN needs is determined by the number of users and the size of the network.

Internet Protocol Security (IPSec): a set of protocols for securing Internet communications and is commonly used in conjunction with virtual private networks (VPNs).

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.

Message Integrity Check (MIC): method that ensures the contents of a message has not been inappropriately altered.

Radio Frequency (RF): alternating current (AC) having characteristics such that, if the current is input to an antenna, an electromagnetic (EM) field is generated suitable for wireless broadcasting and/or communications.

RADIUS: Short for Remote Authentication Dial-In User Service, an authentication and accounting system.

Secure Sockets Layer (SSL): a security protocol to enable websites to securely communicate sensitive information in an encrypted format.

Service Set Identifier (SSID): is the network name that identifies a particular Wi-Fi access point or router.

Temporal Key Integrity Protocol (TKIP): is a security protocol for WPA. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism.

Virtual Private Network (VPN): 1) an encrypted tunnel throughout the Internet that enables secure transmission of data[1]; 2) a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A VPN ensures privacy through security procedures and tunneling protocols. Data is encrypted at the sending end and decrypted at the receiving end.

Voice Over Internet Protocol (VoIP): a protocol for transmitting voice communications over the Internet.

Wired Equivalent Privacy (WEP): A form of encryption used to authenticate the sender and receiver of messages over networks, particularly when the Internet is involved in the data transmission; should provide authentication (both sender and recipient are known to each other), data security (safe from interception), and data nonrepudiation (data that were sent have arrived unchanged)[2]

Wireless Fidelity (Wi-Fi): a term for certain types of WLANs. Wi-Fi can apply to products that use any 802.11 standard. Wi-Fi has gained acceptance in many businesses, agencies, schools, and homes as an alternative to a wired network. Many airports, hotels, and fast-food facilities offer public access to Wi-Fi networks.

Wireless Local Area Network (WLAN): 1) a wireless local area network that uses radio waves as the carrier[3]; 2) a local area network (LAN) that users access through a wireless connection. 802.11 standards specify WLAN technologies.

Wi-Fi Protected Access (WPA): a security protocol designed to improve the authentication and encryption features of Wired Equivalent Privacy (WEP). WPA provides stronger encryption than WEP through the use of Temporal Key Integrity Protocol (TKIP).

Notes

1. AHIMA. Pocket Glossary of Health Information Management and Technology, third edition. Chicago, IL: AHIMA 2012, 356.
2. AHIMA. Pocket Glossary of Health Information Management and Technology, third edition. Chicago, IL: AHIMA 2012, 359.
3. AHIMA. Pocket Glossary of Health Information Management and Technology, third edition. Chicago, IL: AHIMA 2012, 359.

Notes

1. Rousseau-Vesta, Tamera. "The State of Wireless Networking in Healthcare." Enterasys Secure Networks. February 28, 2013. http://blogs.enterasys.com/the-state-of-wireless-networking-in-healthcare-a-global-healthcare-study/
2. US Government Accountability Office. "Medical Devices. FDA Should Expand Its Consideration of Information Security for Certain Types of Devices." August 2012. http://www.gao.gov/assets/650/647767.pdf
3. PCI Security Standards Council. "Information Supplement: PCI DSS Wireless Guidelines." August 2011. https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_Wireless_Guidelines.pdf
4. US Food and Drug Administration. "Radio Frequency Wireless Technology in Medical Devices—Guidance for Industry and Food and Drug Administration Staff." August 13, 2013. http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077210.htm
5. National Institute of Standards and Technology. "Guidelines for Securing Wireless Local Area Networks (WLANs)." http://csrc.nist.gov/publications/nistpubs/800-153/sp800-153.pdf

Prepared by (2013)

Brian Evans, CISSP, CISM, CISA, CGEIT

Assisted by (2013)

William Miaoulis, CISA, CISM
Tom Walsh, CISSP

Acknowledgments (2013)

Becky Buegel, RHIA, CHP, CHC
Marlisa Coloso, RHIA, CCS
Jane DeSpiegelaere-Wegner, MBA, RHIA, CCS, FAHIMA
Kathy Downing, MA, RHIA, CHPS, PMP
Elisa R. Gorton, RHIA, CHPS, MAHSM
Lesley Kadlec, MA, RHIA
Kelly McLendon, RHIA, CHPS
Diane Reed, RHIT, CCS-P
Angela Dinh Rose, MHA, RHIA, CHPS, FAHIMA

Prepared by (Original)

John Retterer
Brian W. Casto, BSEE, CET

Acknowledgments (Original)

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, CHPS

Article citation:
AHIMA Practice Brief. "Securing Wireless Technology for Healthcare (2013 update) - Retired" (Updated November 2013)
