

Moving From Liability to Viability

Hospitals, health plans and physician practices can outsmart hackers with policy, a comprehensive security infrastructure and wireless monitoring.

By Bill Sims

As wireless LANs are deployed in the healthcare market, their benefits become clear: improved accuracy and efficiency for nursing documentation, dramatic decreases in preventable medication errors, greater customer satisfaction through streamlined admissions and improved information access for physicians.

What isn't as clear are the risks that wireless LANs create from a security standpoint. This leaves healthcare administration and IT staff with a difficult decision: to deploy wireless to decrease errors, improve efficiency and lower costs, or to delay wireless deployment until wireless security improves.

Let's take a closer look at the true extent of the risks created by wireless networks, what exposure they create and what should be done to address those problems.

Rogue Wireless Deployments

The most dangerous issue associated with wireless LANs is that protected health information traveling through a healthcare network is broadcast in the air by a wireless access point (AP) and can be easily intercepted from up to several miles away. Without the proper configuration of authentication and encryption on the AP, anyone—not just a sophisticated hacker—can access the network, intercept all data transmissions, and send and re-

ceive data as if plugged in at a desktop.

How would a wireless network be deployed without proper authentication and encryption? Unfortunately, there are several ways this can happen. The most common and well-known issue is the deployment of unsanctioned "rogue" wireless access points. There are endless examples of rogue wireless deployments in healthcare:

- physicians in the medical office deploying their own wireless networks so they can access their data from a common medical library on another floor;

The threats are real, with a growing number of wireless hackers and more sophisticated wireless hacking tools outpacing attempts to improve wireless security.

- a radiologist who connected two competing hospitals with wireless LANs so he could review films from both hospitals in one office;
- a group of accounting consultants who needed connectivity for several users in a conference room with only one Ethernet jack;

- a mobile cart vendor who left behind an evaluation cart and a wireless AP; or
- a vendor who plugged in an access point to intercept e-mail traffic from purchasing to determine what bids were being offered by competitors.

All of these examples expose the entire network—not just wireless traffic—to outsiders who want to intercept data or compromise the network.

Unintentional Association

In addition to rogue AP deployments, insecure wireless networks can be deployed accidentally through the improper configuration of an access point during installation, after a power failure or as a result of maintenance. Insecure networks can be created by users who configure PCs in peer-to-peer or "Adhoc" mode and connect them to the wired network, effectively creating a rogue access point.

Also, wireless devices themselves are vulnerable to an issue known as "unintentional association." This occurs when a wireless device unwittingly connects to a neighboring network, without the knowledge or intervention of the user. This is a significant issue in urban and densely populated suburban environments, where dozens of wireless networks coexist. Unintentional association also creates a risk from malicious hackers who use hacking tools to make their PCs



look like a legitimate access point, to coax the unsuspecting user to connect to the hacker's PC. If the user has file-sharing enabled, the hacker can easily copy files to or from the user's PC or exploit that PC in other ways. This exploit can be done even if the PC is connected to a secure network.

Because wireless LANs provide an easy target with a low likelihood of a hacker being caught, wireless hacking has become extremely popular, with thousands of hackers using dozens of tools designed specifically for compromising wireless LANs. These tools provide hackers with complete anonymity to avoid being identified and make it easy to find vulnerable wireless LANs, assess their security configuration, exploit the security mechanisms, or attack the wireless or the wired network in order to crash it.

Recently published tools are sophisticated enough to attack more advanced wireless security protocols such as LEAP by sniffing user authentications and quickly cracking weak passwords. There are even "packaged" versions of these tools that allow a PC to boot from a preconfigured CD containing a variant of Linux that contains some of the most popular wireless exploit software to make it easy for beginners to use them.

War Driving

The most innocent and well-known form of wireless hacking is called war driving. Wireless radios, scanning software and GPS receivers are used to locate and map access points across the country. There is even an annual worldwide war drive where thousands of participants find, log and upload access point locations to online databases such as www.wigle.net.

War driving helps to document the location of public hot spots and, by itself, is not malicious. However, anyone wanting to know if a hospital is vulnerable need only supply the latitude and longitude of the facility to wigle.net to find if the hospital has open access points that can be attacked.

War driving is only the beginning, however. Once a wireless network is detected, the hacker can scan the network for vulnerabilities, sniff unencrypted data out of the air, hijack user sessions, attack wireless stations, shut down the wireless network, attack the wired network, plant worms or simply steal Internet bandwidth. The press is full of examples of wireless attacks: Major

Wireless devices ... are vulnerable to an issue known as "unintentional association." This occurs when a wireless device unwittingly connects to a neighboring network, without the knowledge or intervention of the user.

retailers have had credit card transactions stolen, businesses have had spam transmitted from their network without their knowledge, and consultants and press have exposed companies with open wireless networks to generate publicity.

Most recently, a physician practice received great notoriety when its wireless LAN was compromised and the data the hacker obtained were sent to the practice's insurance company—and worse, to the patients themselves. This hacker became the first person to be convicted of a wireless cybercrime, only be-

cause he exposed his activity by contacting the individuals affected by his actions. There are hundreds of similar stories that have not made the press.

What can be done to avoid these risks? For many institutions, wireless presents a risk they are not willing to take, so they have delayed wireless deployment. However, this may actually *increase* the risk by inviting the deployment of highly vulnerable rogue wireless networks. The answer lies in three steps:

- creating, communicating and enforcing a wireless policy;
- building a comprehensive wireless security infrastructure; and
- using wireless monitoring to monitor, enforce and document policy adherence.

Importance of Policy

The first step is critical: to create a wireless policy that is distributed from senior management to all employees, physicians, subcontractors and business partners. The policy should document clearly what risks wireless poses to the organization, who has authority over wireless deployments and what the repercussions are for not following policy.

This policy should be part of any chain-of-trust agreements with third parties.

However, policies are often ignored, forgotten or mistakenly broken, so detection of violations and enforcement are critical. With all of the possible ways that insecure wireless LANs can be created, how can policy be enforced, especially in a large institution with limited resources? Periodic vulnerability assessments are prone to human error, create a significant recurring expense and don't provide continuous protection.

To effectively enforce policy requires a multilayered security in-

frastructure that consists of wireless device protection, access point configuration management, wireless VPN deployment and enterprise wireless monitoring. Wireless device protection can be provided by personal firewalls or vendor-provided tools that ensure that stations are protected from unintentional association with neighboring networks or malicious attacks by hackers posing as legitimate access points.

Access point configuration management tools provide simplicity of configuration for large wireless deployments to improve the consistency of wireless configurations with minimal resources and effort. A wireless VPN treats the wireless network as a “dirty” network like the Internet, and provides a more robust means of authentication and encryption to improve access control and the privacy of information.

The final layer—wireless monitoring—ensures that all of the other layers are configured and operating according to policy. A monitoring solution ensures that there are no rogue stations by detecting the presence of potential hackers or devices that have not been securely configured by the IT staff. Monitoring verifies “out-of-band” that the access points have been properly configured and that they maintain the proper security configuration.

Monitoring also verifies that authentication and encryption are being used according to policy by detecting rogue access points, Adhoc station configurations, unintentional associations with neighboring networks, or malicious attempts to disable or circumvent the VPN firewall. Most importantly, a monitoring solution provides the capability to document adherence to policy over time—along with alarms for policy violations and resolution—providing management with a concise and reliable means of ensuring HIPAA compliance.

Wireless LANs pose a serious security risk to the healthcare enterprise, even for organizations with no sanctioned wireless deployment. The threats are real, with a growing number of wireless hackers and more sophisticated wireless hacking tools outpacing attempts to improve wireless security.



Bill Sims is the director of healthcare solutions for AirDefense, a provider of wireless LAN security solutions in Alpharetta, Ga. Contact him at bsims@airdefense.net and www.airdefense.net/healthcare/

HMT