

Deploying Secure, Reliable Wireless LANs in the Healthcare Environment

By Bill Sims

For many healthcare institutions, wireless LANs (WLANs) have become a key component of the IT infrastructure. WLANs have moved into mainstream use by providing greater efficiency and accuracy to users of such mission-critical applications as bedside medication administration, emergency registration, order entry, physician rounding and clinical documentation.

As the paper chart gives way to computer-based patient records, mobile devices are becoming the primary point of clinical communications. As the user base grows and mobile applications become increasingly mission-critical, the need for effective security and management of these networks becomes a top priority.

Yet for all of their benefits, wireless networks introduce significant risks and challenges to IT management.

Challenge #1: Rogue Wireless Deployments

Unauthorized rogue access points are the most daunting challenge created by WLAN technology. A rogue access point provides easy access to the entire network infrastructure—and not just for a serious hacker, but for anyone with a wireless network adapter and an antenna within several miles of the rogue access point.

Rogues may be introduced by well-intentioned employees, physicians, consultants or contractors who install their own access points without regard to proper se-

curity configuration requirements. Rogues also can be created accidentally during deployment or maintenance of the wireless network by failing to properly configure an access point. Users also can create rogues by using the “ad hoc” wireless configuration feature that allows a PC to act as an access point.

HIPAA will require a means of ensuring that encryption integrity is maintained not only at deployment, but also during maintenance and upgrades.

PCs can create a rogue situation by connecting unknowingly to neighboring networks, a process known as “accidental association.” The problem of rogues is so common that several websites, such as www.WIGLE.net, actually catalog thousands of open wireless networks. Stopping rogue deployment is a must for healthcare organizations.

Challenge #2: Malicious Hackers

Wireless networks provide anonymity and ease of access to the enterprise network. Unlike Internet hacking, the anonymous nature of WLAN hacking means that it is nearly impossible to track down a hacker’s origin. This has made WLANs a

popular entry point for stealing intellectual property or obtaining demographic and credit card information for identity theft or credit card fraud. Wireless hacking also provides a wealth of unwitting sources for e-mail spamming or malicious hacking into others networks.

WLAN technology uses a notoriously weak encryption scheme inappropriately called Wired Equivalent Privacy (WEP). On a busy network, WEP can be cracked in a matter of hours. Wireless vendors have responded with more advanced solutions such as Microsoft’s 802.1x/EAP and Cisco’s Lightweight Extensible Authentication Protocol (LEAP). Many new products are available that protect the WLAN through the use of virtual private network (VPN) solutions. Although these technologies are a crucial part of any secure wireless deployment, they provide only part of the required security infrastructure.

Even when using WEP, LEAP or VPN technologies, all traffic at OSI layers 1 and 2 are available to the hacker along with crucial management frames. There is no authentication involved at layers 1 and 2, so any hacker can pretend to be an access point or any legitimate network user. This has made it easy to create software to perform wireless Denial of Service attacks.

Because the hacker can see both sides of any conversation, “man-in-the-middle” attacks—which are difficult to execute on the Internet—are an easy task in the wireless realm. This is true even when

For more information about wireless LAN security solutions from AirDefense, www.airdefense.net

VPNs are being used. (Refer to the draft RFC at www.ietf.org/internet-drafts/draft-puthenkulam-eap-binding-01.txt for an assessment of man-in-the-middle attacks against wireless VPNs.)

All wireless stations are at risk to the malicious hacker. Any PC with a wireless radio in it can be easily coaxed into associating with a hacker's PC, making any files on the PC readily available, regardless of any enterprise encryption or authentication scheme. A hacker can take advantage of this vulnerability to browse through the contents of a PC in a hospital—or on board an airliner. Although the likelihood of a malicious hack may be low, the risks are high because of the difficulty in detecting and thwarting an attack.

Challenge #3: Meeting HIPAA Security Requirements

Obviously, the recently published HIPAA security rule will have an impact on an organization's view of its wireless risks. The rule requires that data traveling over a public network be encrypted. (One can assume that a wireless LAN is by definition a public network.) WEP or any more advanced encryption scheme may be considered sufficient to meet this requirement, but the challenge will be ensuring that encryption is turned on throughout the enterprise.

HIPAA will require a means of ensuring that encryption integrity is maintained not only at deployment, but also during maintenance and upgrades. The rule will require a means of verifying, testing and documenting the proper security configuration, and that there is a mechanism in place for detecting and responding to attacks.

The WLAN challenge is significant: How will institutions be able to document that they have encrypted wireless traffic considering the likelihood of rogue and improperly configured access points,

accidental association with neighboring networks, and ad hoc wireless PC configurations?

Challenge #4: Performance Management and Troubleshooting

Wireless networks can be challenging to manage. Overall wireless performance is very limited when compared to wired LANs, and user performance varies based on environmental conditions such as distance, user load and interference.

Interference can come from other access points on the same channel, either part of the same network or from neighboring networks. It can also come from outside sources: microwave ovens, telemetry systems, cordless phones and imaging systems. Any occurrence of users being disconnected or experiencing poor performance can be caused by poor coverage, improper channel configuration, outside interference, access point or radio degradation, or network utilization, among other factors.

The challenge is gathering enough useful information to determine where performance issues are coming from and rapidly responding. As applications become more mission-critical, not only are patient safety and clinical productivity at risk, but so is the adoption of the entire software investment.

Addressing the Challenges

Much has been written on the basics of securing the wireless environment. Fundamental requirements include using 128-bit WEP, turning off broadcast of the Service Set Identifier (SSID), and using SSIDs and WEP encryption keys that are not easily guessed. If your WLAN includes many access points, configuration management tools are available from WLAN vendors to help simplify and organize access point deployment.

To further secure the network from attacks against WEP's weak-

nesses, most security experts recommend a wireless VPN, either provided by the wireless vendor or one of many third-party solutions. However, VPN deployment must be considered carefully, since they present their own challenges. They can be expensive to deploy and labor-intensive to manage. Users may object to having another login requirement to access the network. Most importantly, the client software component can cause interoperability issues with other products, especially with handheld products or notebook PCs that have non-vendor compatible wireless radios built in.

Manage the Airwaves

To completely secure and effectively manage a WLAN infrastructure, you must manage the airwaves. Inspection of the airwaves provides the only trustworthy means of detecting all forms of rogues—unauthorized access points, ad hoc PC configurations or accidental association. Products that monitor the airwaves can provide detection, alarm and, with some products, even prevention against malicious attacks. Looking at the airwaves is the only effective means of quickly finding performance bottlenecks and sources of interference.

To manage the airwaves, there are two general product categories: stateful solutions and stateless solutions. Stateless solutions are inexpensive to acquire and typically run on a handheld computer or notebook PC. These products require that the device be present in the area when a problem occurs and that expertise be applied to determine the source and cause of the problem. This is much like having a security guard walk through a facility to check doors and look for intruders. Although easy on the capital budget, stateless solutions require greater expertise and manpower.

A stateful system requires a

greater degree of capital investment, using distributed sensors that provide information about the wireless environment back to a central monitoring server. It is similar to deploying a monitored alarm system and security cameras. Although stateful solutions cost more, they provide the most comprehensive solution, because the entire facility is monitored for policy exceptions on a 24/7 basis. Adherence to policy can be easily documented for management reporting purposes, and stateful solutions require minimal labor and expertise.

The IT staff benefits from having the only definitive means of

determining whether the WLAN environment is secure and performing properly. When problems arise, these products act like wireless sniffers to quickly isolate and resolve problems.

In conclusion, wireless networks play an increasingly important role in the delivery of healthcare, but they bring new challenges to IT management. Meeting these challenges requires clear configuration requirements combined with security solutions that strengthen the inherently weak capabilities of today's WLAN standards. The most effective way to ensure the security, performance and reliability of

a wireless LAN infrastructure is to effectively monitor the airwaves with stateful solutions. While they are more expensive, they provide continuous verification of the security and operational integrity of the entire network. HMT



Bill Sims is director of healthcare solutions for AirDefense, a provider of wireless LAN security solutions, in Alpharetta, GA. Contact him at

bsims@airdefense.net.

For more information on AirDefense and Wireless LAN Security contact:
info@AirDefense.net or visit www.airdefense.net