

February 2006

## Wireless security

By Greg Goth

When it comes to the immediate future for wireless network security, it's still a "good news, bad news" scenario.

The good news is that 802.11i, the comprehensive security protocol ratified by the Institute of Electrical and Electronics Engineers (IEEE), Piscataway, N.J., is now fully supported by the computer industry. The linchpin piece of the puzzle, inherent support for the protocol in Microsoft's Windows XP operating system, was finalized in the second quarter of 2005.

Frank Hanzlik, managing director of the Austin, Texas-based Wi-Fi Alliance, the industry organization representing manufacturers of 802.11 equipment, says that in order to obtain the organization's seal of approval, equipment must feature the latest protocol, dubbed WPA2 (Wi-Fi Protected Access 2), by March 1.

The bad news, however, is that the incredibly fast deployment curve of 802.11 wireless LANs (WLANs) over the past several years has left users with plenty of equipment built for the vulnerable and now-obsolete Wired Equivalence Privacy (WEP) security scheme. What's worse, this equipment, which various industry sources estimate accounts for a third of all WLANs, can't be upgraded to become compatible with the new protocol. Therefore, WLAN security will remain a patchwork of virtual private networks, dynamic monitoring, and best practices until it's time for wholesale network upgrades.

But since some smaller vendors haven't made the protocol leap yet, even hospitals that have decided to upgrade their wireless security are encountering compatibility issues between their network and end-user devices.

"Some vendors are not supporting new security technologies in remote devices that attach to things like IV pumps, or medication pumps," says Bo Mendenhall, principal information security analyst at the University of Utah Health Sciences Center, Salt Lake City. "Those devices just don't have the processing power to support anything other than WEP—and WEP is 'sometimes,' if we're lucky."

The Wi-Fi Alliance's Hanzlik says he understands that industry-wide adoption of the new technology will take time.

“We just want to make sure that everybody who is going to be in the market for Wi-Fi solutions will have the specifications very well understood in terms of what they should be looking for,” Hanzlik says. “We think WPA2 will be very well received and is important.”

### Networking WLAN security

Bill Sims, a member of the healthcare advisory board for AirDefense Inc., an Atlanta-based wireless security provider, has been working with wireless networks for many years. The growth of 802.11 networks happened so quickly it’s easy to forget that the first wireless deployments were not really conceived as critical extensions to enterprise networks in which security concerns were paramount, he notes.

“When wireless networks were first designed, pre-802.11 and even before some of the early proprietary networks, the most exciting part of this was to use it in public settings,” Sims says. “It wasn’t to use it as infrastructure high-speed backbone to support voice and image data transfers in a secure manner in a mission critical environment. No one ever thought of that.”

The technology quickly attracted enterprise users, however. The first industry standard Wi-Fi equipment used WEP as its security mechanism, originally featuring 40-bit encryption based on the RC4 cipher and a shared static key between network components. But by 2001, numerous researchers had discovered WEP was very vulnerable to eavesdropping attacks via its weak key scheme and relatively limited initialization vector capabilities.

By late 2003, the Wi-Fi Alliance certification mandated the use of Wi-Fi Protected Access (WPA) instead. WPA, a subset of the 802.11i specification, replaced WEP’s static key with a dynamic 128-bit key scheme called Temporal Key Integrity Protocol and also introduced mutual authentication between client devices and access points via the Extensible Authentication Protocol (EAP). The IEEE 802.11i working group ratified the full specification in June 2004. The full protocol also mandates the 128-bit Advanced Encryption Standard (AES), whose algorithm is considered to be much stronger than the RC4 cipher.

With the latest wireless networking equipment, large enterprise customers are encouraged to use WPA2 with authentication servers that automate the authentication process. Smaller network setups may use a pre-shared key, in which access points are issued authentication key-generating pass phrases manually. The latter method is impractical for large-scale deployments, but it is far cheaper than buying an authentication server for a limited number of users.

### Real-world problems

While researchers exposed the weaknesses in the now-obsolete WEP protocol by trying concerted cracking attacks, IT executives discovered that malicious break-ins were relatively rare. Far more common were careless deployments of unapproved “rogue” access points, “accidental association” connections in which open access points interacted with clients from another nearby network, and unclear client access policies.

Sims recalled the story of a radiologist who connected his offices in two competing hospitals with a WLAN so he could do all his reading in one office. When he plugged his laptop into one hospital’s wired network one day, he unwittingly unleashed a virus into the network.

AirDefense monitors enabled the hospital's IT staff to trace the virus back to the laptop and to expose the unauthorized wireless use.

He also spoke of a hospital IT network executive who discovered that recently installed access points in a nearby building were hopping over to stronger signals on the hospital's WLAN. He had to reconfigure not only his network to isolate specific channels from the offending side of the building, but also had to reconfigure his wireless clients to communicate only with the hospital's Service Set IDs and access points.

Such accidental and careless deployments seem likely to continue as organizations tighten up their network policies.

At the University of Utah Health Sciences Center, Mendenhall's staff has identified 30 to 40 rogues on the network in the past year, all installed in various settings and for various reasons. As the center codifies its wireless policy, he says education, not punishment, is the preferred avenue of remediation.

"We came across one rogue they set up because they didn't want to pay for having a new cable to the office, and sometimes they needed two people to work. Our policy for that is still fairly new, and so I think we're more in the education phase. I would prefer to go in and say, 'We don't care that you have wireless here, but let us provide it for you.'"

So far, Sims says, regulations under the Health Insurance Portability and Accountability Act (HIPAA) have not been strictly enforced in assuring wireless security. But even facilities that are still running WEP-based equipment can benefit from dynamic monitoring of their WLANs, he adds. Such monitoring can isolate equipment that is lacking an approved medium access control (MAC) address, equipment the hospital didn't purchase, and equipment that is using a suspiciously high amount of bandwidth. It also provides an audit trail in case catastrophe strikes.

At this point, even rudimentary WEP deployment meets HIPAA's mandate to take reasonable precautions with commercially viable equipment, Sims says; so IT executives who make sure to institute best practices while waiting for the next wholesale upgrade of their networks would be going a long way in doing the right thing. Not knowing your network contains a rogue access point may not be an actionable offense, but Sims says breaches that could be prevented should be considered unacceptable for ethical reasons if not legal ones.

"Suppose you have an open AP you do know about? Where does responsibility begin and end?"

*Greg Goth is a freelance writer in Oakville, Conn.*