

General Information

March 27, 2009 • Vol.31 Issue 11

Page(s) 34 in print issue

Wireless Encryption & Security

Top Issues & Technologies To Consider

Key Points

- WEP should not be deployed. It's too insecure, and its vulnerabilities are well-known and broadly exploited.
- WPA2 with Enterprise extensions offers the tightest protection currently available. Combine with a VPN for even stronger protection.
- Remember human factors. Technology can only go so far. Train end users and enforce secure wireless behaviors.

Deploying wireless networks can free employees from the creativity-crushing sameness of a hard-wired desktop computer in a hard-wired cubicle. But cutting the cord opens up a range of security issues that network administrators can't afford to ignore.

"Attackers love wireless networks," says Forrester Research Senior Analyst John Kindervag. "They're easier to break into, and they tend to have fewer controls."

■ A Risk Not Worth Taking

Kindervag says the TJX data breach in 2007, widely viewed as one of the most significant security violations ever, was executed via wireless infrastructure.

"In that case, people weren't looking. Generally, people don't understand how flawed wireless can be," he says. "It is clearly one of the greatest hack vectors, but for whatever reason, there's a lot of complacency around it." This complacency can create significant risk for organizations.

"Security is especially important in Wi-Fi networks because they can extend outside the physical boundaries of a secure building and can potentially open a window into your business systems," says Andy Logan, product marketing manager for Aruba Networks (www.arubanetworks.com).

Understanding that risk is essential in today's networked economy. Tiller Beauchamp, principal security consultant with IOActive (www.ioactive.com), says small enterprises are especially vulnerable.

"Running an unsecured wireless network is like leaving your car unlocked and running while you go to the movies—you are inviting abuse," says Beauchamp. "Using WEP is equivalent to putting a fence around your yard. It will discourage some people, but anyone with enough curiosity will simply hop the fence."

■ Encryption Is Just Part Of The Story

Wireless security planning often centers around the importance of encryption, or the manner in which traffic is protected from eavesdropping as it moves between wireless components. A number of encryption standards have evolved since wireless networking was first popularized:

- **WEP** (Wired Equivalent Privacy) was the first widely available encryption standard and is also the weakest. It contains a number of inherent weaknesses, all of which have been thoroughly

exploited by hackers, prompting it to fall into relative disfavor.

- **WPA** (Wi-Fi Protected Access) replaced WEP and pointed the industry toward the eventual IEEE wireless security standard, 802.11i. WPA, however, still contains a number of weaknesses and is not fully compliant with 802.11i.
- **WPA2** added AES (Advanced Encryption Standard, also known as Rijndael) encryption and includes all of the 802.11i mandatory requirements.

While there's no disputing encryption's importance, Avi Deitcher, CEO at operations consulting company Atomic (www.atomicinc.com), says it's only part of any final solution. Authentication (determining that users actually are who they say they are), authorizing (determining that they are allowed to do what they want to do), and accounting (keeping track of who did what for the purposes of future auditing) are other critical features. Even then, encryption and AAA (authentication, authorizing, and accounting) still aren't the last word on wireless security features and thinking.

"WPA and WPA2 have enterprise extensions that allow for user-by-user authentication and authorization, usually using an external server managed by the organization," says Deitcher. "This allows for much finer-grained control and auditing."

With all of these options to consider, organizations often turn to hybrid solutions. "The most secure organizations that I have seen do both WPA2-Enterprise and require a VPN to connect," says Deitcher. "Essentially, they treat access from the wireless network as insecure as access from the Internet. For many, this may be overkill, but for very sensitive networks, this may make sense."

■ Why It Matters

Deitcher says organizations must get serious about protecting wireless infrastructure to reduce vulnerability to three primary attack methods:

Data theft. "If you don't protect your wireless network, other parties may gain access to sensitive corporate data," Deitcher says, adding organizations covered by privacy regulations such as HIPAA for health records or PCI DSS for credit card data may face fines or other sanctions if they fail to act.

Denial of service. Deitcher says even if hackers don't succeed in stealing data, they can compromise an organization's ability to operate by denying access to its own networks.

Hijacking. Attackers use your WLAN as a so-called staging area to launch malicious assaults against other networks. "These assaults may be traced back to you," Deitcher says, "and you may be found liable."

Protection begins at the planning stage. Aruba's Logan recommends taking a system-level view of the issue. "Interdependencies between features can affect security and performance and need to be taken into account during system design," he says. "For example, authentication affects key generation and management, which, if not handled correctly, could enable the type of security breach that authentication is intended to prevent."

Although many organizations have outright banned wireless implementations as a means of protecting themselves, Logan says this is insufficient. "Simply declaring a 'no-wireless' policy is insufficient to protect a company unless an active scanning and enforcement regime is in place," Logan says. "The low cost of commodity Wi-Fi devices makes it simple for an employee to plug an unsecure wireless router into a wired network, bypassing all of the wired network security and creating an unauthorized entrée into the network."

Human factors often trump technological ones in ensuring secure wireless infrastructure.

"The strongest encryption in the world is useless if it's not configured correctly or if the secret keys (or passwords) are stolen," says Joe Levy, CTO of Solera Networks (www.soleranetworks.com). "Presuming the presence of effective antimalware controls such as a unified threat-management solution, the focus shifts to human rather than technology issues. The systems and their controls must be easy enough for people to use or they will be misused or disused."

Forrester's Kindervag says companies deploying wireless networks need to change their thinking. "Many companies don't understand that wireless is not Ethernet," he says. "They treat it like Ethernet, but it's a different protocol. This creates problems because it ends up being poorly deployed in many instances." ■

by Carmi Levy

Know Your Wireless Best Practices

Jeff Kalwerisky, chief security evangelist at Alpha Software (www.alphasoftware.com), recommends the following wireless best practices:

- Enforce standards around passwords. "Always use a long, complex password—i.e., at least 12 characters comprising lowercase, uppercase, and numeric characters," says Kalwerisky. "Change the password regularly or after change of any sensitive roles such as network administrator."
- Consider deploying two-factor authentication over a VPN for wireless access to corporate networks
- Monitor and record all wireless access to the system for forensic analysis in case of a break-in
- Do not broadcast the wireless network's SSID (service set identifier)