Tightening Wireless LAN Security

Author: James L. Bindseil, Global Technical Director for Symantec Security Services

Published: Tuesday, 05 October 2004 13:28 GMT

Here's some news that will grab any information security professional's attention: of 500 firms recently polled by Jupiter Research, less than half had implemented security solutions for their wireless networks. That's a troubling discovery, especially given that wireless networking and mobile computing are two of the fastest growing technologies since the emergence of the Internet.

While wireless networks have ushered in sweeping productivity gains at some enterprises, they have also increased enterprises' exposure to security risks in ways not always understood. This article will look at the principal wireless vulnerabilities encountered today, some recent developments that address them, and finally at wireless security best practices that you should consider implementing.

In 1999, the Institute of Electrical and Electronics Engineers (IEEE) published the 802.11b standard for a group of technologies governing wireless Ethernet connectivity. Because unauthorized users can receive wirelessly transmitted data, the 802.11b standard included Wired Equivalent Privacy (WEP) to encrypt the transmitted packets. Unfortunately, WEP utilized static keys as part of its encryption methodology, which made it relatively easy to intercept enough packets to discern the key and thus crack the coded traffic. Once hackers discovered this flaw, they developed automated cracking programs that soon hit the Internet and gave even inexperienced hackers the tools they needed to crack just about any WEP-based wireless LAN (WLAN). Even worse, it's possible for an attacker to modify the packets, compromising the integrity of the data.

The good news is that the IEEE has a task group working on a standard (802.11i) that is dedicated to providing solid security, although ratification of this standard isn't expected until later this year. In the meantime, the Wi-Fi Alliance, a nonprofit international wireless association, adopted an interim standard for wireless security called Wi-Fi Protected Access (WPA) in the fall of 2002 and began interoperability testing on it in the spring of 2003.

WPA is intended to address all the shortcomings of WEP; it combines user authentication (which WEP did not provide) with a stronger encryption element from the forthcoming 802.11i standard called Temporal Key Integrity Protocol. TKIP includes Message Integrity Check (MIC), which protects against forgeries and so-called replay attacks.

As eWEEK.com has described it, "The transmitter of a packet adds about 30 bits (the MIC) to the packet before encrypting and transmitting it. The recipient decrypts the packet and verifies the MIC (based on a value derived from the MIC function) before accepting the packet. If the MIC doesn't match, the packet is dropped. Having the MIC ensures that modified packets will be dropped and attackers won't be able to forge messages to fool network devices into authenticating them."

Although WPA brings a boost to WLAN security, many view it as a temporary fix because future 802.11 equipment will likely use the Counter Mode with CBC-MAC Protocol (CCMP), which is also a part of the 802.11i draft. CCMP uses Advanced Encryption Standard (AES) to provide even stronger encryption. However, AES is not designed for backward compatibility.

Beware of the backdoor

Ensuring the security of wireless networks isn't just about standards, of course. Information security professionals are justifiably concerned with the many publicized types of attacks that can be launched against WLANs – including traffic interception, "man-in-the-middle" attacks, denial of service, and session hijacking, to name a few. Fortunately, many risks can be mitigated by following basic wireless security practices using enterprise-class and client protection technologies. Let's look at some of the steps involved.

As you know, the boom in wireless networking took many IT departments by surprise, with the result that much wireless equipment was introduced into organizations by individual employees and workgroups, rather than through the IT department or other proper channels. The result of this “backdoor” introduction was that wireless wasn’t put through the normal process of understanding its capabilities and limitations before implementation. Consequently, efforts to secure wireless devices came as an afterthought, or were not sufficiently rigorous.

The first step in creating a secure WLAN is to establish an enterprise-wide strategy for deployment and usage. The strategy should address these areas:

# Determine business needs. (What are the business drivers and needs of your organization? Identify objectives clearly, and make sure that benefits outweigh risks.)

# Integrate wireless policies into existing IT policies. (Remember: wireless solutions are an extension of the wired network.)

# Clearly define WLAN ownership. (This ensures control as well as response when security threats are identified. It also nips backdoor introductions in the bud.)

# Protect the existing infrastructure. (This is critical: do not place wireless devices directly on the internal network. Instead, provide a separate WLAN with highly controlled gateways to the main network.)

# Educate users in wireless policies. (This includes training employees to configure their devices to securely access the network.)

Follow WLAN best practices

To protect a WLAN from attack, enterprises need to be up-to-date with their security best practices. These should include the following:

# Control the broadcast area and lock each access point. Many wireless access points let you adjust the signal strength. Place your access points as far away as possible from exterior walls and windows. Test the signal strength so you can barely get a connection at these locations. Next, make sure to change the default password on all access points. Use a strong password to protect each access point.

# To provide compatibility, purchase hardware from one vendor. While the IEEE standard should provide compatibility between wireless devices from different manufacturers, interpretations of the standards and proprietary extensions can prevent full integration between devices of different manufacturers.

# Use SSID (Service Set Identifier) intelligently. Buy access points that let you disable SSID broadcasting. This prevents access points from broadcasting the network name and associating with clients that aren't configured with your SSID. Also immediately change an access point’s default SSID. (And while you’re at it, change the default username and administrator password, too.)

# Regularly scan for rogue access points. Wireless network interface cards can be configured as access points, and very little effort is required to turn a client computer into a rogue access point. Regularly scan for rogue access points on the network using a wireless scanning tool.

# Implement user authentication. Require access point users to authenticate. Upgrade access points to use implementations of the WPA and 802.11i standards. Also, as you implement user authentication on the access points, reuse any existing servers providing authentication for your other network services. This prevents former employees from using old user accounts to access the network.

# Secure the WLAN with IPsec VPN technology or clientless VPN technology. This is the most secure way to provide user authentication, data integrity, and data confidentiality services on a WLAN. Additional VPN technology is not dependent upon the access point or the wireless LAN card; therefore,

not dependent upon the access point or the wireless LAN card; therefore, additional hardware costs aren't incurred as wireless security standards continue to evolve.

# Use MAC (Media Access Control) address authentication. If you have a manageable number of wireless users and just a few access points, MAC addressing lets you restrict connections to your access points by specifying the unique hardware address of each authorized device in an access control list -- and allowing only those specific devices to connect to the wireless network.

# Turn on the highest level of security your hardware supports. Even if you have older equipment that supports only WEP, be sure to enable it. Whenever possible, use at least 128-bit WEP.

# Deploy personal firewalls and virus protection on all mobile devices. The WiFi Alliance recommends using the corporate network security policy to enforce their continuous use.

# Deploy enterprise-class protection technologies. This includes employing a Layer 7 firewall on the demilitarized zone and client firewalls on each desktop; VPN services that encrypt all traffic to and from wireless devices; intrusion detection systems; antivirus software at the gateway, server, and desktop levels; regular vulnerability assessments of the WLAN; and policy compliance tools.

Conclusion

A recent study by Ipsos-Reid found that the typical mobile worker who accessed wireless e-mail was able to gain an average of 53 work minutes per day. That spells improved productivity and flexibility for workers -- and extra work for IT departments. While creating a secure wireless network is a challenging and ongoing process, a well-designed WLAN, backed by proactive security policies, can provide users with the tremendous benefits of mobile computing -- and even increase the bottom line of today's real-time enterprise.