Simple Wireless Security Techniques

In many cases, you may only need to employ deterrents to keep the causal snooper from messing with your wireless LAN. The following techniques offer partial security that works for all applications and are generally adequate for home and small office applications:

- **Turn SSID broadcasting "off**." This ensures that the access point doesn't include the SSID (service set identifier) in the beacon frames that are sent multiple times per second. Without the broadcasting of SSIDs, operating systems such as Windows XP will not discover the SSID and automatically configure the user's radio NIC. As a result, an intruder will have to find out the SSID through other, more difficult means. 802.11 association frames always include the SSID, even when SSID broadcasting is off. Thus, someone can use an 802.11 packet analyzer (e.g., AirMagnet or AiroPeek) and sniff the air while a legitimate user boots ups and associates with an access point. This requires enough effort (and expense) to cause most snoopers to go elsewhere. In some cases, though, it may not be practical to turn off SSID broadcasting. For example, you should broadcast SSIDs in public wireless LANs to provide open connectivity.

- **Utilize static IP addresses**. By default, most wireless LANs utilize DHCP (dynamic host configuration protocol) to more efficiently assign IP addresses automatically to user devices. A problem is that DHCP doesn't differentiate a legitimate user from a hacker. With a proper SSID, anyone implementing DHCP will obtain an IP address automatically and become a genuine node on the network. By disabling DHCP and assigning static IP addresses to all wireless users, you can minimize the possibility of the hacker obtaining a valid IP address. This limits their ability to access network services. Of course someone can use an 802.11 packet analyzer to sniff the exchange of frames over the network and learn what IP addresses are in use. This helps the intruder guess what IP address to use that falls within the range of ones in use. Thus, the use of static IP addresses isn't fool proof, but at least it's a deterrent. Also keep in mind that the use of static IP addresses in larger networks is very cumbersome, which may prompt network managers to use DHCP to avoid support issues.

- **Turn WEP "on."** There are certainly problems with WEP (wired equivalent privacy), but it's better than nothing. WEP encrypts the body of each 802.11 data frame, which makes it very difficult for someone with an 802.11 packet analyzer to decipher the actual data. There are methods and tools that hackers can use to untangle the encrypted data into something meaningful, but that generally requires someone with more technical ability than the common, causal snooper. As a result, the use of WEP acts like having a strong lock on the front door of your home. It keeps most people out, but someone with the right skills and motivation can pick the lock. This problem will eventually go away because 802.11 plans to solve the flaws of WEP through more advanced encryption methods.

- **Utilize shared key authentication**. Most wireless LANs on the market today allow the use of this optional 802.11 feature, which helps avoid rogue radio NICs from gaining access to the network. When the authentication process occurs, the access point sends the radio NIC a string of challenge text. The radio NIC must encrypt the challenge text with its WEP key and send the encrypted version to the access point. After decrypting the challenge text with the common WEP key, the access point can determine that the radio NIC has the correct key if the challenge text matches what was sent initially. This forms the basis for allowing the NIC to authenticate with the access point. (Again, this mechanism is only as good as WEP. A determined hacker can still eventually break through.)

- **Install/activate personal firewalls.** This is something that many people overlook. In smaller networks, you generally keep all of your files on a personal computer or laptop. Without personal firewall protection, someone having legitimate or devious access to the wireless LAN can easily copy and open your files. Keep your files in access-protected directories to avoid others from stealing your files. Of course this applies to wired networks as well.

Advanced Security Mechanisms

In addition to the above security techniques, consider the following tips that offer a greater degree of security to satisfy enterprise and vertical application requirements:

- **Utilize a virtual private network (VPN)**. This involves the use of third-party encryption (e.g., triple Data Encryption Standard or 3DES) that affects all data on the WLAN. Generally, the user installs VPN client software on their wireless device, which communicates securely with the VPN network. This can be a relatively expensive and somewhat inflexible solution, but it provides excellent security.

- **Implement mutual authentication mechanisms**. Through the addition of a RADIUS server, 802.1X protocols, and possibly an access controller, you'll have a framework for deploying mutual authentication between users and access points. This reduces man-in-the-middle attacks, such as rogue access points. Many enterprise grade access points support these features. 802.1X provides port-based access control and mutual authentication between clients and access points via an authentication server, such as RADIUS. You'll need to also choose an authentication type, such as EAP-TLS or EAP-TTLS. Be sure to implement encryption of user names and passwords or use digital certificates to strengthen the authentication process. 802.1X also provides a method for distributing encryption keys dynamically to wireless LAN devices, which solves the key reuse problem found in the current version of 802.11 WEP.

- **Place access points outside the enterprise firewall**. To protect intruders from accessing corporate network resources, ensure that the wireless LAN access points remain outside the firewall. You can configure the firewall to enable access

from legitimate users based on MAC addresses, which makes it difficult (but not impossible) for a hacker to mimic. In fact, you can also incorporate MAC address filtering using most enterprise-grade wireless LAN access points.

- **Minimize radio wave propagation in non-user areas**. Try orienting antennas to avoid covering areas outside the physically controlled boundaries of the facility. By steering clear of public areas, such as parking lots, lobbies, and adjacent offices, you'll significantly reduce the ability for an intruder to participate on the wireless LAN. This will also minimize the impact of someone disabling your wireless LAN with jamming techniques.