
Wireless Security - Why it matters!

Once you connected your new wireless access point or integrated cable/DSL modem access point to your broadband connection, it just seemed simpler to bypass setting up any type of security/encryption on the network. After all, you're just sending the data around your house and between your systems anyway. However, employing wireless security IS important! Here's why.

The Neighbor Kid - and Worse!

Want to get just a bit nervous? Just do this simple experiment (Windows XP example). Go to the Network Connections area of the Windows Control Panel. Click on Wireless Connections and just see how many networks - other than your own - are displayed. I just did the experiment on my system and saw two networks - obviously those of my neighbors. Now, if I can see their network, it's pretty clear that they can see mine. And if your network is unsecured, and Tommy the neighbor kid is curious..... Well, you get the picture.

Even scarier however, are the folks that wander through neighborhoods looking for "open" wireless networks to "hack". Believe it or not, this IS a problem. And, if you've got credit card or other personal information available to them, they'll be very happy to take it from you and use it for their personal gain.

Wireless Security - Your Options

Most wireless equipment targeted for home use incorporates three, basic security features - and we strongly suggest that you implement them. They are:

- *SSID or Service Set Identifiers:* SSID is the common network name for devices on a wireless LAN and is used to segment the wireless LAN. SSID prevents access from any device that does not have or "know" the wireless LAN SSID. However, by default, access points broadcast their SSID so anyone can determine the wireless LAN SSID if they "listen". The broadcast can be turned off, but intruders can still find the SSID through "sniffing" tactics (turn your beacon off anyway!).
- *WEP or Wireless Encryption Protocol:* WEP employs a scheme to make gaining access to your wireless LAN a bit more difficult. Use WEP the access point sends the wireless client a challenge-text packet that the client must encrypt with the correct WEP key and send back to the access point. WEP keys can be 40 or 128 bits and are the same for all devices on the network. We consider employment of WEP encryption the baseline. Everyone should use it. However, if your laptop or other wireless device is lost or stolen, others could access your network if they know where you live.
- *MAC Address Authentication:* Some vendors use the physical or MAC address of devices to support authentication. In this scenario, the access point allows access only to clients whose MAC address has been entered into an authentication table in the access

point. In other words, you have to configure the MAC table in the access point's software. Again, if your wireless device is stolen, intrusion is possible.

- *WPA - or Wi-Fi Protected Access:* WPA Pre-Shared Key (PSK) verifies the user's password or identifying code on both the client and the access point. The client gains network access if the password they send matches the access point's password. The password is also used by TKIP (Temporal Key Integrity Protocol) to generate an encryption key for every packet of data transmitted. In other words, all of the transmissions on the network are encrypted as well.

We strongly recommend that you employ either WEP or WPA on your wireless network to ensure that it has the basic protections you need to keep your information safe.

Stronger Security

Higher end wireless equipment employs even stronger security capabilities. Based on industry standards from the IEEE, 802.1X authentication provides dynamic, per user, per session encryption keys instead of the static keys used in WEP or WPA. These dynamic solutions however, most often require implementation of a security server such as Remote Authentication Dial-In User Service (RADIUS) or Authentication, Authorization and Accounting (AAA) servers. If you have a small business outside of the home, implementation of these services, based on the Extensible Authentication Protocol (EAP) for communication between client and access point, may be required. You'll have to do some further research as well if you do decide on an EAP-based solution as EAP comes in a variety of "flavors" - Cisco LEAP, EAP-Transport Layer Security (EAP-TLS), protocols that work over EAP-TLS such as Protected Extensible Authentication Protocol (PEAP), EAP-Tunneled TLS (EAP-TTLS) and EAP Subscriber Identity Module (EAP-SIM).

Don't Just Sit There...

So, don't just sit there, protect your wireless LAN - and business and personal information - right now. Open up the web interface to your access point/router and enable WEP. Then reconfigure your client devices with the correct password. You'll sleep better at night knowing that "Tommy" can't get at your corporate AMEX number.