DUMMIES.COM®

Wireless Security Protocols: WEP, WPA, and WPA2

By **Lawrence C. Miller** from **Home Networking Do-It-Yourself For Dummies**

5 of 8 in Series: The Essentials of Setting Up a Wireless Network

Various wireless security protocols were developed to protect home wireless networks. These wireless security protocols include WEP, WPA, and WPA2, each with their own strengths — and weaknesses. In addition to preventing uninvited guests from connecting to your wireless network, wireless security protocols encrypt your private data as it is being transmitted over the airwaves.

> Wireless networks are inherently insecure. In the early days of wireless networking, manufacturers tried to make it as easy as possible for end users. The out-of-the-box configuration for most wireless networking equipment provided easy (but insecure) access to a wireless network.

Although many of these issues have since been addressed, wireless networks are generally not as secure as wired networks. Wired networks, at their most basic level, send data between two points, A and B, which are connected by a network cable. Wireless networks, on the other hand, broadcast data in every direction to every device that happens to be listening, within a limited range.

Following are descriptions of the WEP, WPA, and WPA2 wireless security protocols:

- **Wired Equivalent Privacy (WEP):** The original encryption protocol developed for wireless networks. As its name implies, WEP was designed to provide the same level of security as wired networks. However, WEP has many well-known security flaws, is difficult to configure, and is easily broken.

- **Wi-Fi Protected Access (WPA):** Introduced as an interim security enhancement over WEP while the 802.11i wireless security standard was being developed. Most current WPA implementations use a preshared key (PSK), commonly referred to as *WPA Personal*, and the Temporal Key Integrity Protocol (TKIP, pronounced *tee-kip*) for encryption. *WPA Enterprise* uses an authentication server to generate keys or certificates.

- **Wi-Fi Protected Access version 2 (WPA2):** Based on the 802.11i wireless security standard, which was finalized in 2004. The most significant enhancement to WPA2 over WPA is the use of the Advanced Encryption Standard (AES) for encryption. The security provided by AES is sufficient (and approved) for use by the U.S. government to encrypt information classified as top secret — it's probably good enough to protect your secrets as well!

f G+ y ▶