Wi-Fi Protected Access

Overview

Over the past year, many Wi-Fi Alliance members and their customers have become increasingly concerned about the vulnerabilities of Wired Equivalent Privacy (WEP), the basic mechanism to date for interoperable security in Wi-Fi CERTIFIED products. In response, the Wi-Fi Alliance in conjunction with the IEEE, has driven an effort to bring strongly enhanced, interoperable Wi-Fi security to market in the first quarter of 2003. The result of this effort is Wi-Fi Protected Access (WPA).

Wi-Fi Protected Access is a specification of standards-based, interoperable security enhancements that strongly increase the level of data protection and access control for existing and future wireless LAN systems. Designed to run on existing hardware as a software upgrade, Wi-Fi Protected Access is derived from and will be forward- compatible with the upcoming IEEE 802.11i standard. When properly installed, it will provide wireless LAN users with a high level of assurance that their data will remain protected and that only authorized network users can access the network. The Wi-Fi Alliance plans to begin interoperability certification testing on Wi-Fi Protected Access products starting in February 2003.

WEP Vulnerabilities

Not long after its development, WEP's cryptographic weaknesses began to be exposed. A series of independent studies from various academic and commercial institutions found that even with WEP enabled, third parties can breach WLAN security. A hacker with the proper equipment and tools can collect and analyze enough data to recover the shared encryption key. Although such security breaches might take days on a home or small business WLAN where traffic is light, it can be accomplished in a matter of hours on a busy corporate network.

Despite its flaws, WEP provides some margin of security compared with no security at all and remains useful for the casual home user for purposes of deflecting would-be eavesdroppers. For large enterprise users, WEP native security can be strengthened by deploying it in conjunction with other security technologies such as Virtual Private Networks or 802.1x authentication with dynamic WEP keys. Nevertheless, Wi-Fi users demanded a strong, interoperable, and immediate security enhancement native to Wi-Fi. The result of this demand is Wi-Fi Protected Access.

Wi-Fi Protected Access

Wi-Fi Protected Access had several design goals, i.e.,: be a strong, interoperable, security replacement for WEP, be software upgradeable to existing Wi-Fi CERTIFIED products, be applicable for both home and large enterprise users, and be available immediately.

To meet these goals, two primary security enhancements needed to be made. Wi-Fi Protected Access was constructed to provide an improved data encryption, which was weak in WEP, and to provide user authentication, which was largely missing in WEP.