Overview

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.

Enhanced Data Encryption through TKIP

To improve data encryption, Wi-Fi Protected Access utilizes its Temporal Key Integrity Protocol (TKIP). TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named *Michael*, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. Through these enhancements, TKIP addresses all WEP's known vulnerabilities.

Enterprise-level User Authentication via 802.1x and EAP

WEP has almost no user authentication mechanism. To strengthen user authentication, Wi-Fi Protected Access implements 802.1x and the Extensible Authentication Protocol (EAP). Together, these implementations provide a framework for strong user authentication. This framework utilizes a central authentication server, such as RADIUS, to authenticate each user on the network before they join it, and also employs "mutual authentication" so that the wireless user doesn't accidentally join a rogue network that might steal its network credentials.

Wi-Fi Protected Access and IEEE 802.11i Comparison

Wi-Fi Protected Access will be forward-compatible with the IEEE 802.11i security specification currently under development by the IEEE. Wi-Fi Protected Access is a subset of the current 802.11i draft, taking certain pieces of the 802.11i draft that are ready to bring to market today, such as its implementation of 802.1x and TKIP. These features can also be enabled on most existing Wi-Fi CERTIFIED products as a software upgrade. The main pieces of the 802.11i draft that are not included in Wi-Fi Protected Access are secure IBSS, secure fast handoff, secure de-authentication and disassociation, as well as enhanced encryption protocols such as AES-CCMP. These features are either not yet ready for market or will require hardware upgrades to implement. The IEEE 802.11i specification is expected to be published at the end of 2003.

Wi-Fi Protected Access for the Enterprise

Wi-Fi Protected Access effectively addresses the WLAN security requirements for the enterprise and provides a strong encryption and authentication solution prior to the ratification of the IEEE 802.11i standard. In an enterprise with IT resources, Wi-Fi Protected Access should be used in conjunction with an authentication server such as RADIUS to provide centralized access control and management. With this implementation in place, the need for add-on solutions such as VPNs may be eliminated, at least for the express purpose of securing the wireless link in a network.

Wi-Fi Protected Access for Home/SOHO

In a home or Small Office/ Home Office (SOHO) environment, where there are no central authentication servers or EAP framework, Wi-Fi Protected Access runs in a special home mode. This mode, also called Pre-Shared Key (PSK), allows the use of manually-entered keys or passwords and is designed to be easy to set up for the home user. All the home user needs to do is enter a password (also called a master key) in their access point or home wireless gateway and each PC that is on the Wi-Fi wireless network. Wi-Fi Protected Access takes over automatically from that point. First, the password allows only devices with a matching password to join the network, which keeps out eavesdroppers and other unauthorized users. Second, the password automatically kicks off the TKIP encryption process, described above.

Wi-Fi Protected Access for Public Access

The intrinsic encryption and authentication schemes defined in Wi-Fi Protected Access may also prove useful for Wireless Internet Service Providers (WISPs) offering Wi-Fi public access in “hot spots” where secure transmission and authentication is particularly important to users unknown to each other. The authentication capability defined in the specification enables a secure access control mechanism for the service providers and for mobile users not utilizing VPN connections.

Wi-Fi Protected Access in “Mixed Mode” Deployment

In a large network with many clients, a likely scenario is that access points will be upgraded before all the Wi-Fi clients. Some access points may operate in a “mixed mode”, which supports both clients running Wi-Fi Protected Access and clients running original WEP security. While useful for transition, the net effect of supporting both types of client devices is that security will operate at the less secure level (WEP), common to all the devices. Therefore, organizations will benefit by accelerating the move to Wi-Fi Protected Access for all Wi-Fi clients and access points.

Press and analyst contact:
C. Brian Grimm
Wi-Fi Alliance
910.686.0870
briang@wavecoms.com

rev. 10/31/2002