



WIRELESS STANDARDS UPDATE Issue 11/2002

A new wireless mechanism has been defined to meet the vulnerabilities of WEP. This mechanism called WPA includes most of the functionalities that will be embedded in the 802.11i security standard when finalised. Hot-spots are hot, the Wi-Fi alliance is looking into roaming between hot-spots which is key for the deployment of the hot-spot concept.

CONTENT

<u>Page</u>	<u>Title</u>
1	WPA : Wi-Fi protected access
3	<i>Blueprint ready for WLAN hot-spot roaming.</i>

✓ Wi-Fi Protected Access : WPA

Over the past year, wireless vendors and users have become increasingly concerned about the vulnerabilities of the Wired Equivalent Privacy (WEP), the basic mechanism to date for interoperable security in Wi-Fi certified products. In response the Wi-Fi alliance (formerly the WECA – Wireless Ethernet Compatibility Alliance) in conjunction with the IEEE, has driven an effort to bring strongly enhanced, interoperable wireless security to market. The result of this effort is Wi-Fi Protected Access (WPA)

Beginning Q4 2002 the consortium will refuse to issue its 'Wi-Fi' certified seal of approval to 802.11 based products that do not support this enhanced WPA security scheme.

Starting in February, 802.11 products must pass WPA conformance and interoperability testing to be granted the Wi-Fi seal. The alliance says it expects WPA-certified products to be available on the market as early as March. Existing products require a software upgrade to become WPA compliant.

As of February, WPA will serve as a replacement for the Wired Equivalent Privacy (WEP) in the 802.11 products. WPA consists of a subset of the 802.11i security suite. The 802.11i standard is still in development at the IEEE, and ratification is not expected until late 2003. But many wireless LAN vendors, as well as third party companies that offer software products and gateways as wireless LAN complements, offer some 'pre-standard' parts of 802.11i anyway.



What is in WPA ?

As mentioned, the Wi-Fi Protected Access security suite that will be required for Wi-Fi certification of wireless LAN products next year contains many of the components of the formal security standards nearing ratification by the IEEE 802.11 Task Group I.

Upgrading to the WPA suite requires software changes to access points and clients, which will likely be made available for a nominal fee by most vendors. A mixed network can run with WPA and its predecessor, Wired Equivalent Privacy (WEP), both installed. However, security in these networks will default to WEP, which offers less protection.

WPA contains the pieces of 802.11i that are closest to final approval, so few, if any, software changes should be required when 802.11i becomes "real."

One 802.11i component not required in WPA is Advanced Encryption Standard (AES) support. AES will replace 802.11i's RC4-based encryption under 802.11i specifications.

Migrating to AES encryption, though, will require hardware changes, so this has been deferred by the Wi-Fi Alliance until the formal standard is in place to give vendors and customers some breathing room. But 802.11i will require hardware changes regardless of whether WPA gets deployed over the next year or not.

So do you want to protect your networks now or wait to better secure them until 802.11i products emerge in the second quarter of 2004? You can also use third-party proprietary products in the interim, which we'll discuss here at a later date.

Here are the components included in WPA and 802.11i:

- * 802.1x authentication framework.
- * AP-to-client communications security.
- * Key hierarchy.
- * Key management.
- * Cipher and authentication negotiation.
- * Temporal Key Integrity Protocol, which rotates encryption keys on a per-packet basis and provides other important functions.

Here's what will still be left to add when 802.11i is commercially deployed:

- * AES.
- * Pre-authentication (a strength when voice quality of service is required).
- * Peer-to-peer communications security.



Products supporting WPA will be labelled "Wi-Fi WPA-certified. When 802.11i is a standard, products will be labelled as "Wi-Fi WPA2-certified." In the future, we'll likely see WPA3, WPA4...

✓ ***Blueprint ready for WLAN hot-spot roaming.***

A plan that would let Wireless LAN users roam among service provider networks is in the final stage of preparation by the Wi-Fi Alliance.

The Blueprint is a set of best practices for the wireless LAN service providers and vendors, as well as carriers. Wireless LAN sites that adhere to these practices will be identified by a new Wi-Fi Alliance symbol – Wi-Fi Zone- created for this project. Next year (starting in the US) wireless users should be able to log on at any public access point, or wireless LAN hotspot, that shows the symbol. Such users will be authenticated through a network of Remote Authentication Dial-In User Services (RADIUS) servers before seeing their start-up webpage on the internet or their corporate network.

The recommendations include a set of attributes to be used in configuring authentication servers and databases based on the RADIUS protocol.

Approved beginning of November, the Wi-Fi Alliance document outlines the steps needed for wireless LAN service providers to create a simple, consistent user logon experience. The document outlines a way for users to log in to any WISPr wireless LAN with only a wireless adapter and a Web browser.