

Securing WLANs: A Bluesocket Perspective on WPA and 802.1x solutions

WPA and 802.11i

On 31 October 2002, the Wi-Fi Alliance announced WPA (Wi-Fi Protected Access), a security offering based on the forthcoming 802.11i security standard (being worked upon by IEEE's Task Group I). WPA is an "interim" standard and the recommended replacement for the much derided WEP (Wired Equivalent Privacy) protocol, known for its weaknesses in 802.11 WLAN environments.

WPA enables 802.1x/EAP authentication along with Temporal Key Integrity Protocol (TKIP) encryption that is based on RC4, and provides for dynamic rekeying to eliminate the problems associated with static keys. The components of WPA include:

- 802.1x authentication framework
- AP-to-client communication security
- Key hierarchy and management
- Cipher and authentication negotiation
- TKIP

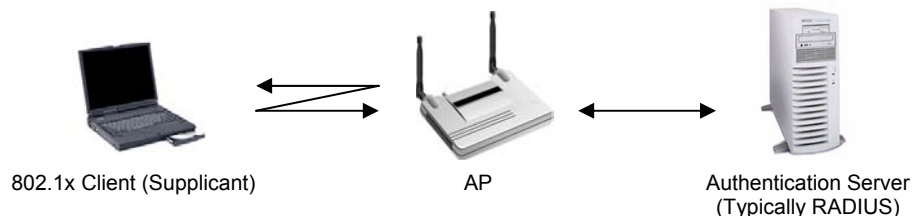
WPA does leave out some aspects of 802.11i that are still work in progress and, quite likely, will require hardware upgrades. These features, including secure fast handoff and de-authentication and disassociation, will be added when 802.11i is finally approved, which is expected sometime in early 2004:

- AES encryption, which will finally replace WEP and RC4
- Pre-authentication
- Peer-to-peer communication security

802.1x

802.1x is an IEEE standard (now part of WPA) ratified in June 2001, which enables authentication and key management for local area networks. Although originally designed as a port authentication mechanism for wired networks, it has recently been applied to address some of the security issues surrounding wireless LANs. 802.1x was augmented to use the Extensible Authentication Protocol (EAP) as a framework for authentication. This allows for a variety of EAP methods and authentication servers to meet the needs of disparate enterprise environments.

In a WPA/802.1x environment, a wireless user would authenticate as follows:



- 1) Wireless client associates with Access Point (AP)
- 2) AP blocks all traffic except 802.1x/EAP
- 3) EAP Traffic is passed to RADIUS Server for authentication

- 4) User is authenticated and given a per user/per session WEP key for encrypting the data as it passes over the wireless link
- 5) TKIP (and other similar protocols) use rapid re-keying to change the WEP key at regular intervals in an effort to make cracking the key more difficult.

Selecting an EAP Protocol

The ability to use a variety of authentication methods makes 802.1x flexible. However, there are several competing EAP Protocols (LEAP, MD5, TTLS, TLS, PEAP, SRP, etc.) which require support on the client device, AP and authentication server. It is critical to choose an EAP Protocol that meets your security requirements, maintains ease of use for the end-user, and will not become obsolete.

WPA/802.1x/EAP Challenges

Deployment of an end-to-end WPA/802.1x solution is not without challenges. Enterprises with WLANs should consider the following:

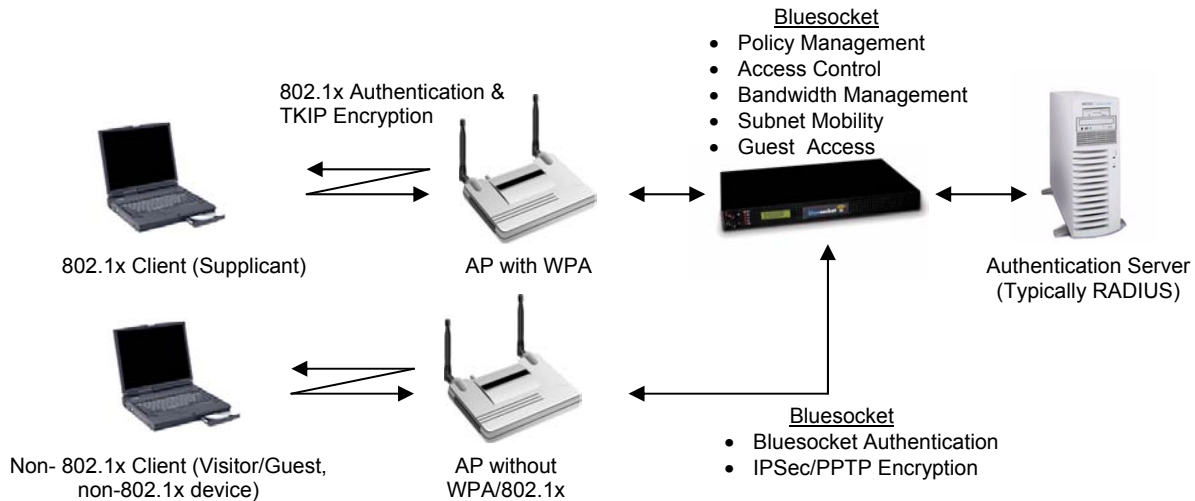
- Although WPA is an interim “standard”, proprietary implementations of 802.1x and EAP require vendor specific APs/NICs, which means that interoperability becomes more complex in multi-vendor environments
- Client software is required to support WPA/802.1x, involving the need to upgrade all client devices
- Hardware upgrades are almost certainly going to be required in 2004 when 802.11i is finally ratified
- Not all devices will work with 802.1x - support for limited device types and operating systems only
- No visitor, guest or non-802.1x user access (PDA’s, Apple MACs, Scanners, VoWLAN Phones)
- Underlying security is still based on WEP with rapid re-keying, requiring extensions to APs
- Access is all or nothing (either on or off the network)
- No provisions for QOS or bandwidth management
- Total cost of implementation should be considered as each device must have WPA/802.1x software and all APs must support the standard and be properly configured

WPA and Bluesocket

To solve all of the issues surrounding WLANs, WPA and 802.1x alone is not sufficient. Using a Bluesocket Wireless Gateway or a combination of 802.1x and Bluesocket technology will allow enterprises to address the complexities of Wireless LANs and successfully implement a production class, 802.11-based wireless network. The following table illustrates the benefits of using Bluesocket’s Wireless Gateway to enhance a WLAN environment that uses WPA-certified solutions including features such as 802.1x:

| Feature | WPA Without Bluesocket | WPA With Bluesocket |
|--|------------------------|---------------------|
| Authentication (802.1x) | X | X |
| Dynamic WEP Encryption (TKIP) | X | X |
| Strong IPSec/PPTP Encryption | | X |
| Role-Based Access Control | | X |
| WLAN Policy Management | | X |
| QOS and Bandwidth Management | | X |
| Guest/Visitor Access (Support for “client-free” devices) | | X |
| Support for any WLAN device | | X |
| Mobility (Secure Roaming) | | X |

The network diagram below demonstrates how Bluesocket facilitates policy enforcement in a WLAN environment where WPA-capable APs are used (including mixed 802.1x and non-802.1x WLANs):



Summary

802.11i is a future security standard for Wireless LANs which will provide for air-link security. When finally ratified, it is expected to have significant implications on customers and vendors alike, including the need to make large-scale hardware and software upgrades to the WLAN infrastructure. In the interim, WPA is a standard being promoted by several Wi-Fi Alliance members. While it does make major improvements over protocols such as WEP for securing WLANs, it is still limited in scope, providing only encryption and authentication options.

A complete WLAN solution requires a comprehensive approach addressing not only encryption and authentication, but policy management, QoS and bandwidth management, mobility, and ubiquitous device, AP and user support. Bluesocket's Wireless Gateways provide such features and work with heterogeneous WLAN infrastructures-- and, where appropriate, can be coupled with WPA implementations to provide comprehensive WLAN security and management solutions.