

WPA2 migration made easy

Lisa Phifer

12.05.2006

Do you need a strategy for upgrading a customer's equipment to WPA2? VARs and consultants can use this tip, originally part of the [Wireless Security Lunchtime Learning](#) series on [SearchSecurity.com](#), to help upgrade equipment and software, enable coexistence and configure clients for a painless migration.

WEP has been cracked, WPA is a bandage, and your customer's CSO wants to upgrade to WPA2. Great, but that's just not going to happen overnight. How do you migrate a customer's installed base of legacy equipment? This tip recommends a workable strategy for migration, permitting peaceful coexistence between old and new devices with divergent security features.

Upgrading equipment

WPA version 2 (WPA2) is the Wi-Fi Alliance certification program for products that implement IEEE 802.11i security enhancements. WPA2-certified products have been available since September 2004. Today, most enterprise and many new residential Wi-Fi products support WPA2, and as of March 2006, WPA2 is mandatory.

To determine whether your customer's devices speak WPA2, consult the Wi-Fi Alliance certified products list. If your customer's gear is old and isn't WPA (version 1) certified, retire it -- if not immediately, then soon. To upgrade other devices to WPA2, check the vendor's support site for new AP firmware or card drivers. You'll need hardware that's no more than two years old; WPA2 requires chipsets that implement the Advanced Encryption Standard (AES). If you're buying new APs, make sure they are WPA2-certified.

Upgrading software

WPA2 comes in two flavors: WPA2-Personal and WPA2-Enterprise. WPA2-Enterprise requires an 802.1X-capable RADIUS server. SOHOs without RADIUS can either use WPA2-Personal with a passphrase of 20+ random characters, or a hosted RADIUS service like McAfee Wireless Security or Witopia SecureMyWiFi.

Most businesses prefer to run WPA2-Enterprise with their own in-house RADIUS server, like Cisco ACS, FreeRADIUS, Funk Odyssey, Interlink RAD, Meetinghouse AEGIS, Microsoft IAS or Open.com Radiator. The differences between WPA and WPA2-Enterprise have little impact on RADIUS servers, so if your customer already runs WPA, you may not need additional RADIUS upgrades for WPA2.

To run either flavor of WPA2, you'll also need client-side software. This may involve an OS patch, an 802.1X supplicant, and/or new wireless card drivers. For example, Windows XP SP2 already supports WPA, but using WPA2 requires installing the XP WPA2 patch. For other operating systems, you'll need WPA2-capable client software from the wireless vendor (e.g., Cisco) or a third-party (e.g., Funk, Meetinghouse, wpa_supplicant, Devicescape). WPA2 clients and drivers may never be available atypical devices with embedded Wi-Fi (e.g., VoWi-Fi phones, bar code scanners) or aging adapters that simply cannot support AES.

Enabling coexistence

As you upgrade your customer to WPA2, begin phasing out older, less secure equipment. Realistically,

your customer will probably need to continue supporting WPA and/or WEP for some time. In other words, you'll need a plan for coexistence between whatever they have today and WPA2.

One tactic is to deploy WPA2 as a new overlay network. This means installing new APs side-by-side with old APs, creating two independent WLANs with different security policies and names (Extended Service Set Identifiers, a.k.a. SSIDs). This approach is expensive, but can make sense if the customer is ready for a "forklift" upgrade anyway -- for example, when replacing a legacy WLAN with a next-generation switched WLAN.

Another tactic is to update firmware on existing APs and/or replace APs, gradually upgrading the [WLAN infrastructure](#) to support WPA2. Fortunately, WPA2-certified products must support WPA for backwards compatibility with products in the field. Most business-grade APs can be configured to simultaneously support both old and new security policies. Over time, as legacy clients are retired or upgraded, you can eliminate old security policies.

This kind of multi-policy WLAN can be accomplished in at least two ways:

If the AP supports multiple SSIDs, define a new SSID for WPA2, preserving the old SSID(s) and associated security policies. For example, when T-Mobile added WPA to its hotspots, it created a new SSID. Clients running T-Mobile's Connection Manager now use WPA-Enterprise by associating to "tmobile1x" while non-WPA clients can still associate to the old "tmobile." In this scenario, the same physical AP may appear as multiple virtual APs, avoiding any impact on older clients.

If the AP supports WPA2 Mixed Mode, you can extend an existing SSID to support multiple security policies. With this Wi-Fi Alliance WPA2 option, APs send beacons for one SSID that advertise several ciphers (e.g., TKIP [WPA], CCMP [WPA2]). Choosing a cipher from the AP's list is up to the client, which of course must be able to understand the AP's beacon. Note that old WEP clients may not work in Mixed Mode, since TKIP is used to encrypt LAN broadcast/multicast.

Some APs offer other vendor-proprietary options, like Cisco's WPA Migration Mode. Consider vendor-proprietary options if the WLAN is homogenous and the client device mix cannot be supported by other alternatives.

No matter how you get there, WPA2 coexistence with weaker security measures should be a temporary step. During transition, you may want to segregate WPA2 and non-WPA2 traffic -- for example, applying different VLAN tags to traffic originating from old and new SSIDs, then asserting different traffic policies based on those tags. Why? Attackers prefer low-hanging fruit; older APs, SSIDs and cipher options are more likely to draw their attention.

Configuring clients

In SOHO WLANs moving to WPA2-Personal, client configuration requires little effort. Once you've upgraded client software, choose "WPA2-PSK" from configuration menus, enter a group passphrase, and you're good to go. If you're using a WPA2-capable card with Windows XP but don't see WPA2-PSK as a configuration choice, you haven't installed the XP WPA2 patch. If you've installed the patch but don't see that choice, you're missing WPA2 card drivers. And don't be fooled by products that support WPA with AES -- that's not WPA2. To use WPA2-Personal, both cards and APs must choose *WPA2-PSK* and AES.

In WLANs moving to WPA2-Enterprise, especially large WLANs, upgrading clients can be a huge task. In addition to updating client-side software, you must choose an 802.1X authentication method, issue (or reuse) client credentials, and tie your RADIUS server to a user account database. The good news is if you've deployed WPA-Enterprise, then you've already covered this ground, and you won't have to do it

all again.

About the author

Lisa Phifer owns Core Competence, Inc., a consulting firm specializing in network security and management technology. Core Competence produces The Internet Security Conference (TISC), an annual symposium for network security professionals. Phifer has been involved in the design, implementation, and evaluation of data communications, internetworking, security, and network management products for nearly 20 years.

This tip originally appeared on SearchSecurity.com.