

## Technological Trends

### Wi-Fi Client Device Security Part 2: WPA2-Enterprise

*This is the second of three articles on Wi-Fi client security. The first article explains the need for strong Wi-Fi security. The second article explains why WPA2-Enterprise is required for solid Wi-Fi security. The third article provides three best practices for ensuring strong Wi-Fi client security.*

While wireless LAN (WLAN) security threats are real, they can be mitigated through good WLAN security practices. The foundation of any WLAN security approach should be the Enterprise version of Wi-Fi Protected Access<sup>™</sup> 2, or WPA2-Enterprise.

#### WEP: Insufficient

Early in this decade, as Wi-Fi<sup>®</sup> became popular on mainstream client devices such as laptops, it was determined that the original WLAN security mechanism of Wired Equivalent Privacy (WEP) was insufficient for several reasons, including:

- **No access control:** While it defines a means to scramble, or encrypt, transmitted data, WEP provides no means to control access to a WLAN. If you know the WEP encryption key, then you can gain access to the WLAN.
- **Vulnerable keys:** Due to weaknesses in WEP, a hacker can “crack” or decipher a WEP key by collecting WEP-encrypted data packets and running them through a WEP-cracking tool. Today, using sophisticated tools, even a 104-bit WEP key can be cracked in less than an hour.
- **Static keys:** The only way to avoid the use of a WEP key that has been cracked by a hacker is to change all WEP keys regularly, which today means more frequently than every hour. Because the most common way of deploying WEP keys is to define them statically on all devices that used them, changing WEP keys is an administrative nightmare.

The IEEE, which defines the standards for WLANs and how they operate, formed a task group, called the 802.11i task group, to define a standard for stronger WLAN security. As the process for defining a standard dragged on, the market grew increasingly impatient for something better than WEP. The Wi-Fi Alliance<sup>®</sup>, a non-profit industry association of more than 300 member companies, responded to market pressure by teaming with the 802.11i task group to create WPA, which the Alliance termed “a significant near-term enhancement to Wi-Fi security”. WPA was designed to be supported in software by Wi-Fi CERTIFIED<sup>™</sup> products that previously had supported WEP.

#### WPA: Good Enough...Until Recently

There are two versions of WPA: Personal and Enterprise. Both encrypt and decrypt transmitted data using Temporal Key Integrity Protocol, or TKIP. Like WEP, TKIP uses RC4 encryption, but TKIP is designed to address vulnerabilities of WEP. The key used for TKIP encryption and decryption is derived dynamically from the information exchanged between the Wi-Fi client and the WLAN during the authentication process that proceeds the client’s connecting to the WLAN.

#### WPA-Personal

With WPA-Personal, the authentication process uses a pre-shared key (PSK) or passphrase that generates a PSK. If the PSK on the Wi-Fi client matches the PSK on the AP to which the client is trying to associate, then the authentication succeeds, and an encryption key for that client is derived and stored on the client and the AP.

While PSKs and passphrases are easy to implement on small networks, a hacker can “guess” a short PSK or passphrase using a dictionary attack. In such an attack, the hacker captures packets that were created using the PSK and then, using a dictionary of potential PSKs and the published algorithm for WPA, tries to

recreate the capture packets. If he is successful, then he has determined the PSK, and he can use it to gain access to the WLAN. The IEEE and various researchers recommend that, if you use a PSK, that PSK should be a random string of at least 20 characters, including characters other than letters and digits.

## WPA-Enterprise

While WPA-Personal relies on a pre-shared key or passphrase for authentication, WPA-Enterprise relies on IEEE 802.1X, a ratified standard for network access control. 802.1X supports a set of Extensible Authentication Protocol, or EAP, types for mutual authentication of the client device and the network to which it is trying to connect. 802.1X authentication with an EAP type such as PEAP or EAP-TLS is extremely strong.

Table 1 compares popular EAP types that are used with 802.1X authentication:

Type	Credential(s)	Database(s)	Pros and Cons
LEAP	Microsoft password	Active Directory (AD)	No certificates Strong password required
PEAP with EAP-MSCHAP	Microsoft password	AD	Native support in Windows, CE CA certificate on every client device
PEAP with EAP-GTC	Password, one-time password, token	AD, NDS, LDAP, OTP database	Broad range of credentials CA certificate on every client device
EAP-TTLS	Wide variety	Wide variety	Broad range of credentials Not widely supported
EAP-FAST	Microsoft password, others	AD, others	No certificates Complex provisioning process
EAP-TLS	Client certificate	Certificate authority (CA)	Very strong authentication Native support in Windows, CE CA, user certificates on every client device

**Table 1: Comparison of popular EAP types**

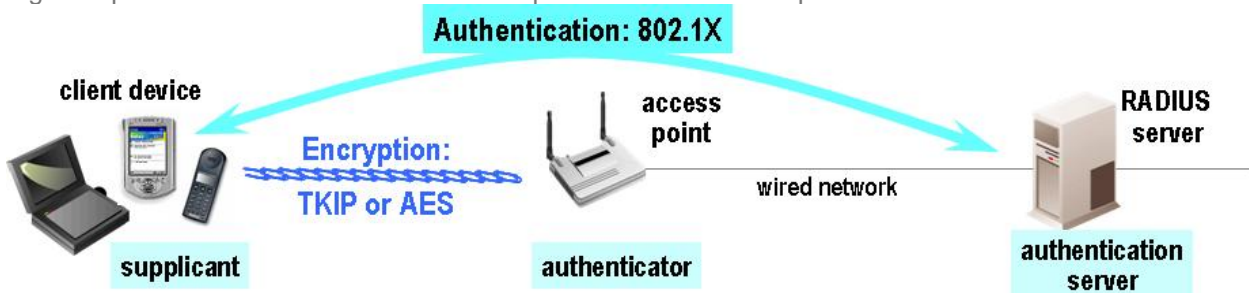
## TKIP: Vulnerable

In late 2008, two German researchers reported that a vulnerability in TKIP could enable an attacker to decrypt individual packets that are encrypted with TKIP. The same vulnerability does not exist with a stronger encryption method, such as one based on the Advanced Encryption Standard (AES) cipher.

## The Right Choice: WPA2-Enterprise

In July 2004, the IEEE approved the full 802.11i specification. Soon after that, the Wi-Fi Alliance introduced a new interoperability testing certification, called WPA2, that incorporates the key elements of 802.11i. WPA2 is essentially the same as WPA, with TKIP replaced by a stronger encryption method called AES-CCMP. In March 2006, the WPA2 certification became mandatory for all new equipment certified by the Wi-Fi Alliance.

Figure 1 provides an overview of WPA-Enterprise and WPA2-Enterprise:



**Figure 1: WPA-Enterprise and WPA2-Enterprise**

The use of WPA2-Enterprise addresses the security threats discussed in the first article in this series:

- **Data exposure:** To prevent the data in Wi-Fi packets from being viewed by a hacker, the sender of those packets must encrypt the data in such a way that only the intended recipient can decrypt the

## Technological Trends

---

packets and view the data in its unscrambled, clear-text form. WPA2 provides a proven mechanism for ensuring that all transmitted data is protected from being viewed by a hacker.

- **Network exposure:** When every Wi-Fi client uses WPA2 with 802.1X authentication to the network, a hacker cannot glean from sniffed packets any information on how to gain access to the network.
- **Man-in-the-middle attacks:** When every Wi-Fi client is configured to use a strong EAP type for mutual authentication to the trusted WLAN, no client will associate inadvertently to a hacker's laptop that is posing as an AP.

The use of WPA2-Enterprise protects all sensitive data and the networks that house that data. Reliance on WPA2-Enterprise is a foundational element of a sound WLAN security strategy. Given that a broad range of client devices support WPA2-Enterprise, every organization should rely on WPA2-Enterprise instead of WPA-Enterprise.

*The next article will provide three best practices for Wi-Fi client security.*