

Technological Trends

Wi-Fi Client Device Security Part 3: Best Practices

This is the third 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.

When proper wireless LAN (WLAN) security is not in place, a hacker can use intercepted Wi-Fi® packets to do one or more of the following: view sensitive information, gain access to the WLAN, or trick users into communicating with him instead of the network. The best way to mitigate these threats is to implement a WLAN security scheme that relies on WPA2-Enterprise. With WPA2-Enterprise:

- A Wi-Fi client cannot connect to a WLAN until the client and the network use IEEE 802.1X, which includes:
 - Strong, mutual authentication of the client and the network using an Extensible Authentication Protocol (EAP) type
 - Dynamic derivation of an encryption key
- All transmitted data is encrypted using a strong encryption method known as AES-CCMP.

Figure 1 provides an overview of WPA2-Enterprise:

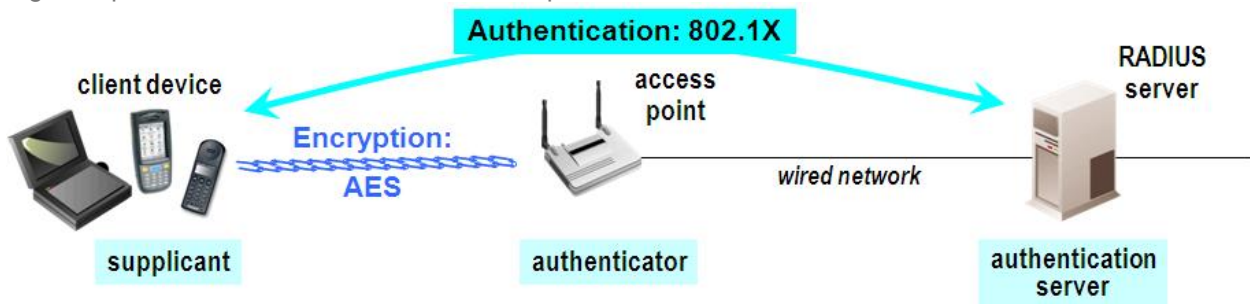


Figure 1: WPA2-Enterprise

As you can see from Figure 1, WPA2-Enterprise security requires the interaction of three types of devices:

1. Client devices that connect to the WLAN
2. WLAN infrastructure devices such as access points and controllers
3. Authentication servers such as RADIUS servers

WPA2-Enterprise and Client Devices

Nearly all business-class WLAN infrastructure devices and authentication servers support WPA2-Enterprise. Client device support for WPA2-Enterprise is less widespread. Two types of devices that support Wi-Fi but may not support WPA2-Enterprise are:

1. Mobile phones and other devices that are sold primarily to consumers: These devices often support only the Personal version of WPA2 and not the Enterprise version of WPA2. With WPA2-Personal, authentication uses a pre-shared key (PSK) or a passphrase that generates a PSK, and a hacker can “guess” a short PSK or passphrase.
2. Older business-class devices: These devices may support the Enterprise version of WPA but not the Enterprise version of WPA2. The WPA encryption method has a vulnerability that is not present with WPA2.

When you have Wi-Fi devices that lack support for WPA2-Enterprise, ensuring that you have strong Wi-Fi security for all devices can be difficult. Your options include:

Technological Trends

- Install and configure an 802.1X supplicant on each device: Only a few commercial supplicants exist. None is free, and none supports every client device operating system.
- Rely on alternatives to WPA2-Enterprise: If you configure your infrastructure to support WPA2-Personal or WPA-Enterprise for some devices, then you run the risk of exposing your network or your transmitted data to hackers. By guessing the PSK of a WPA2-Personal client, a hacker can pose as that client and gain access to your network. By breaking the WPA-Enterprise encryption key, a hacker can decipher transmitted packets of information.
- Rely on virtual private networks (VPNs) instead of WPA2-Enterprise: VPNs operate at Layer 3 and provide no protection against Layer 2 security attacks. Implementing, configuring, and maintaining a VPN scheme for many client devices can be challenging and expensive. VPN software may not run on certain client devices.
- Use firewalls to protect sensitive data on your network: The goal of a firewall is to prevent untrusted client devices from gaining access to sensitive data and applications that manage sensitive data. To determine which devices are trusted and which are untrusted, every device must authenticate to the network in a way that cannot be forged by a hacker. If authentication is at Layer 3 or above, then the security scheme provides no protection against Layer 2 security attacks.

Strong network security relies on strong authentication and strong data encryption. WPA2-Enterprise ensures both, and alternatives to WPA2-Enterprise have significant limitations and costs. Stated simply, the first best practice for solid Wi-Fi security is to phase out any client devices that do not support WPA-Enterprise, replacing those devices with ones that support WPA2-Enterprise.

Best practice: Replace Wi-Fi client devices that lack WPA2-Enterprise support with those that support WPA2-Enterprise.

Two Other Best Practices

Having the ability to support WPA2-Enterprise is not the same as supporting WPA2-Enterprise in practice. The latter requires configuration of the device.

To connect to a WLAN that is configured for WPA2-Enterprise, a client device must be configured with:

- The correct service set identifier (SSID) for that WLAN
- Valid authentication credentials, typically a username that is found in the authentication server database and the correct password for that username
- WPA2 encryption

Most of today's mobile computers and other business-critical mobile devices run Windows Embedded CE, Windows Mobile, or Windows XP. All three operating systems include a WLAN configuration facility called Windows Zero Config (WZC), which enables a user or administrator to configure the device to associate to a WLAN, provided that the WLAN uses one of the EAP types supported by WZC: PEAP with EAP-MSCHAPv2 as the inner method (PEAP-MSCHAP) or EAP-TLS. Many organizations, however, rely on other EAP types – such as LEAP, EAP-FAST, and PEAP-GTC – because those types provides a better “fit” with infrastructure and security requirements.

To use an EAP type that is not supported natively by the Windows operating systems, a client device must include a supplicant that supports that EAP type. That supplicant typically is provided with the Wi-Fi radio in the client device.

To simplify administration of Wi-Fi client devices, you should choose devices with software that supports a wide range of EAP types and ensures that the devices are configured to connect only to your trusted WLAN using your chosen EAP type. Ideally, this software will support a means to distribute the same configuration to many devices with minimal intervention.

Best practice: Configure every trusted Wi-Fi client device to connect only to trusted WLANs.

Once you configure all of your trusted clients to use WPA2-Enterprise to connect to your trusted WLANs, those devices are safe from:

- Transmitting information that can be intercepted by a hacker

Technological Trends

- Enabling a hacker from gaining access to a trusted network
- Being tricked into communicating with a hacker's device instead of a trusted network

Any client device that is not configured to use WPA2-Enterprise to connect to your trusted WLANs is an untrusted device. An untrusted device:

- May expose data to a hacker, but that data will not be from your trusted networks
- Cannot enable a hacker to gain access to a trusted network
- May be tricked into communicating with a hacker's device but will not expose to the hacker data from your trusted network

Even with WPA2-Enterprise protecting your networks and data, you still want to be aware of illicit Wi-Fi activity in and near your business locations. For example, if someone places an unauthorized or rogue AP on your trusted network, then that AP may enable hackers to gain access to that network. Because a rogue AP may be in place only for a few days or even a few hours, periodic use of a wireless analyzer is insufficient. Only a wireless intrusion detection system (IDS) or intrusion prevention system (IPS) that provides constant monitoring is sufficient to detect most rogue APs.

Wireless IDS or IPS tools are important for detecting rogue APs. When your WLANs rely on WPA2-Enterprise, however, these tools are unnecessary for protecting WLANs and the data that they transmit and receive. You can use the tools to demonstrate that your WLAN security policies are implemented properly and are thwarting all attempts to gain unauthorized WLAN access or view sensitive data that is transmitted wirelessly. Those tools may even catch potential attackers in the act.

Best practice: Use ongoing monitoring to demonstrate the effectiveness of your WLAN security approach.