Wi-Fi Security Improvements

Opportunistic Wireless Encryption

Open Wi-Fi networks are ubiquitous. They are used for guest access, connectivity at airports, while we're working at a cafe, and more. But it is also unencrypted. While Opportunistic Wireless Encryption (OWE) was left out of the Wi-Fi Alliance WPA3 Certification, it was branched out into its own as Wi-Fi Alliance Enhanced Open certification.

The goal of OWE is to replace 802.11 Open Authentication with a method of securing Wi-Fi transmissions over open Wi-Fi networks. It is deployed when one might otherwise settle for cleartext.

A network supporting OWE will advertise the use of Authentication and Key Management (AKM) with the authentication type set to OWE. During association, a Diffie-Hellman parameter element exists, in the RSNA, which will contain the client's public key in the Association Request frame and an access point's (AP) public key in an Association Response frame.

These two frames describe the Diffie-Hellman key exchange between the client and AP. The result is a pairwise secret with the 4-way handshake, instead of a pre-shared key (PSK) used in the 4-way handshake. Between the client and AP, they will generate a secret and a secret identifier. The key exchange uses a hash algorithm since mutual authentication between the client and AP is not performed.

Keep in mind, OWE implements unauthenticated, encrypted communication. This method does not authenticate the identities of the client or the AP, making Man-in-the-Middle attacks possible. It doesn't prevent a malicious person from setting up a rogue access point broadcasting the same SSID and hijacking user traffic.

Although there is the possibility of spoofing or MiTM attacks, the OWE Wi-Fi security enhancement for open networks is a big step forward. It increases the security posture of already insecure Wi-Fi networks.

There is no mandate to implement OWE since it was removed from WPA3. To gain widespread use, we must generate demand by requiring vendors to implement it into their products.

Device Provisioning Protocol

Wi-Fi Protected Setup (WPS) turned out not to be very protective at all. It is vulnerable to a brute force attack due to the PIN, used as a shared secret, and used to provide connection information such as WEP and WPA passwords and keys.

Device Provisioning Protocol (DPP) was created to replace WPS and its security weaknesses. With the proliferation of IoT Wi-Fi devices containing no easy method of connecting to Wi-Fi networks, DPP can be utilized for provisioning through another device, such as a mobile phone. If an IoT device has no user interface, another device can use various methods, such as NFC, Bluetooth, password, and QR Code, for provisioning to get the IoT device connected securely.

DPP protects against threats such as eavesdropping, active attacks to add unauthorized devices to existing networks, and denial of service blocking provisioning. DPP defines three phases: bootstrapping, authentication, and network access.

In the bootstrapping phase, the transfer of public key credentials are transferred between entities.
In the authentication phase, PMK and PMKSA are created.

DPP authentication frames are exchanged and the keys from the bootstrapping phase are used during authentication. Then the device needing to join the network is provisioned. In the final phase, network access, this is where the devices mutually derive a PMK and PMKID. The network keys are then used to gain access to the network.

WPA3

The Wi-Fi Alliance announced the release of their WPA3 specification aimed at improving key exchanges in pre-shared key and enterprise networks. The biggest improvement revolves around the implementation of Simultaneous Authentication of Equals (SAE). It's the only mandatory requirement from the Wi-Fi Alliance WPA3 certification.

SAE, also known as dragonfly (a variant), implements an enhanced key exchange handshake to mitigate against vulnerabilities seen in WPA2. Those vulnerabilities attacked the 4-way handshake through a key reinstallation attack (or KRACK) and the cracking of WPA2 through brute force by capturing a single EAPOL frame. The former is patched in software by an update from Wi-Fi vendors. The latter makes weak password protected networks highly vulnerable.

The improvement of the handshake in SAE makes it resistant to offline dictionary attacks where WPA2 networks are vulnerable. A Diffie-Hellman key exchange is used to perform encryption key generation and mutual authentication. Another improvement with SAE is forward secrecy. This protects previously captured data from being compromised due to the private key being stolen or known. How SAE achieves this is by generating a unique session key for every session initiated by the user.

Networks will undergo a transition to utilizing SAE. Under WPA3 there are two modes of operation, WPA3-SAE Mode and WPA3-SAE Transition Mode.

Under WPA3-SAE, an SSID is configured to support WPA3-SAE Mode and advertises its requirement for Protected Management Frame (PMF). All devices must be SAE capable and must support PMF.

Under WPA3-SAE Transition Mode, both WPA2-PSK and WPA3-SAE are configured on the same SSID in a mixed mode. PMF is not required but the SSID will advertise its capability to support it.

For enterprises requiring further protection, WPA3-Enterprise allows an optional feature, 192-bit Mode.

When WPA3-Enterprise 192-bit Mode is used, PMF is still required. In addition, there are supported EAP cipher suites available for use with WPA3-Enterprise:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

The above cipher suites offer improved cryptographic strength for authentication. However, use of 192-bit Mode is optional for WPA3 certification.

Conclusion

It's been over a decade since we last saw advancements in Wi-Fi security. The Wi-Fi Alliance has created different certifications to push widespread use of higher security and cryptography solutions.

While some features were pushed out of WPA3 and into their own certifications, we hope to see Wi-Fi vendors implement them into their products for the purpose of driving better security methods into the primary connectivity choice of many users.

About Ekahau

Ekahau is the global leader in solutions for enterprise wireless network design, optimization and troubleshooting. More than 15,000 customers, including 30% of Fortune 500 companies, run their networks with Ekahau's Wi-Fi planning and measurement solutions.

Our software and hardware solutions design and manage superior wireless networks by minimizing network deployment time and ensuring sufficient wireless coverage across all industries, project sizes, building infrastructures and levels of complexity. We are recognized for delivering the easiest-to-use, most reliable solutions for Wi-Fi planning, site surveys, troubleshooting and optimization. Whether a corporate office, hotel, hospital or university – if the Wi-Fi works well, it has likely been built using Ekahau's Wi-Fi Design solutions.

Learn more about Ekahau's solutions to design, optimize and troubleshoot Wi-Fi networks at www.ekahau.com or contact us at 1-866-435-2428.