New WPA3 WiFi Standard Released

by Sharon D. Nelson and John W. Simek

Well, it's finally here. In the fall of 2017, a vulnerability in WPA2 wireless encryption was discovered. Known as the Krack Attack, the flaw impacts every implementation of WPA2. The manufacturers needed to provide a patch update to fix the flaw. The Wi-Fi Alliance has now announced the availability of the WPA3 standard (to be implemented in certified devices starting later this year), vastly improving security over WPA2, which has been around for over 15 years and should be the current WiFi encryption of choice. WPA3 provides a new security protocol that contains improvements in terms of configuration, authentication and encryption. Just like WPA2, WPA3 will be available in personal and enterprise versions. Some of the new features of WPA3 include:

- Information on public networks will always be encrypted
- Encryption per session
- Protection against brute force attacks at the authentication level (limited attempts for successful authentication)
- Support for using a smartphone or tablet to set up security on IoT devices
- 192-bit security suite to protect networks with higher security requirements (e.g. governments, hospitals, etc.)

WPA3 replaces the Pre-Shared Key with the "Dragonfly" Simultaneous Authentication of Equals (SAE) algorithm. SAE blocks offline password attempts after a single incorrect attempt, therefore, attacks must be made on a live connection, one try at a time. Even though WPA3 will make connecting to public networks a lot more secure, it does not protect against rogue access points, which means the WiFi Pineapple will still be an effective penetration testing tool. What SAE will protect against is dictionary attacks where the bad guys try to guess the network's password by using cloud-based server farms trying various passwords in rapid succession.

SAE also implements a cryptography method called forward secrecy. Basically, it is contains a key-exchange authentication protocol where session keys are independent and won't be compromised even if the private key of the server is compromised. This means that an attacker won't be able to decrypt previously captured traffic even if they know the network's password.

WP3 helps fix the security mess when connecting to public Wi-Fi networks. Traffic between your device and the Wi-Fi access point will be encrypted, even if you don't enter a password at the time of connection. Attackers won't be able to snoop on your traffic as a result.

In addition to the WPA3 release, the Wi-Fi Alliance announced a new feature called Wi-Fi Easy Connect, which is a replacement for Wi-Fi Protected Setup (WPS). That's good news since nobody should be using WPS as it is known to be insecure. One of our recommendations is to turn off WPS for all of your Wi-Fi devices. Easy Connect will allow you to pair your router and smart device simply by scanning a QR code

with your smartphone, which will automatically send the Wi-Fi credentials to the new smart device. This will make it much easier to connect IoT (Internet of Things) devices, especially those with limited or no displays.

Certified WPA3 devices should be available later this year with mass adoption expected late in 2019. When you get a WPA3-enabled router, you'll also need WPA3-compatible client devices (e.g. phone, laptop, etc.) to take full advantage of the new features. The good news is that both WPA2 and WPA3 connections can be accepted at the same time with a new WPA3 router.

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, cybersecurity and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com