Written by Alice Marshall
27 June 2018

The Wifi Alliance announces the next generation wifi security standard-- Wifi Certified WPA3, a set of security protocols adding on the feature set of WPA2 with capabilities aimed at both personal and enterprise networks.

WPA3 promises to simplify wifi security while enabling more robust authentication, deliver increased cryptographic strength and maintain resiliency of mission critical networks. It remains interoperable with WPA2, even as it disallows outdated legacy protocols and demands use of Protected Management Frames (PMF). While optional at launch, WPA3 certification should become required in the future.

The standard comes in two flavours-- WPA3-Personal and WPA-3 Enterprise. The Personal variant is aimed at consumers, and replaces the Pre-shared Key (PSK) of WPA2-Personal with Simultaneous Authentication of Equals (SAE), a technology resistant to offline dictionary attacks. As a result, users can choose natural, easy to remember passwords and data traffic remains protected even if the password is compromised.

Meanwhile WPA3-Enterprise adds more security for enterprise, governments and financial institutions, with optional 192-bit security protocols, 256-bit Galois/Counter Mode Protcol (GCMP-256) encryption, 384-bit Hashed Messaged Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384), Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) using a 384-bit elliptic curve and 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256).

Until WPA3 becomes standard the 12-year old WPA2 is also getting updates-- PMF use is

mandatory for all current generation Wifi Certified devices, and vendor security implementations are enhanced to reduce vulnerabilities due to network misconfiguration and further safeguard managed networks with centralised authentication services.

Go Wifi Certified WPA3