WPA3 security protocol will keep Wi-Fi connections safer

June 27 2018, by Nancy Owano

Credit: CC0 Public Domain

Networking experts who would like to see wireless vulnerabilities swept away can enjoy the good news that Wi-Fi security has taken on next-gen status, after 14 too-long years to the contrary.

Laura Hautala covers the cybersecurity beat for CNET and she was one of several tech writers reporting there on the new standard for securing Wi-Fi connections, WPA3.

Most notably, the WPA3 standard "brings individualized data encryption that should protect your data against eavesdropping from within the WiFi network," said Jon Fingas in *Engadget*.

Long time coming: WPA2 was introduced in 2004, which is a considerable run as the wireless security protocol, and allowing intruders to deploy, as *Wired* pointed out, a so-called offline dictionary attack to guess a victim's password. The report said an attacker can take as many shots as desired to hit the jackpot and guess your credentials "cycling through the entire dictionary—and beyond—in relatively short order."

CNET said the WPA3 Wi-Fi, however, is harder to hack. Hautala said, "new Wi-Fi routers will come with stronger protections for the data that flows between your computers, phones or smart home devices and your internet connection."

Actually, the standard involves two modes of operation: WPA3-Personal and WPA3-Enterprise. The latter will boost security in workplace Wi-Fi networks. The announcement said WPA3-Enterprise offers the equivalent of 192-bit cryptographic strength. This would translate into additional protection for networks transmitting sensitive data, such as government or finance.

As for Personal mode, the good news is that WPA3 leverages Simultaneous Authentication of Equals (SAE). This is a secure key establishment protocol between devices. Expect stronger protections for users against third-party attempts at guessing passwords. Interestingly, the take-home from the major tech watching sites seems to be that the new standard will not be as vulnerable to attack (and the problem is not

helped when we choose weak passwords that are easy to guess).

Brian Barrett on Tuesday , talking about the WPA3 in *Wired*, said, "Not only is it going to keep Wi-Fi connections safer, but also it will help save you from your own security shortcomings."

Jacob Kastrenakes, Circuit Breaker editor, *The Verge*, gave readers a good idea of WPA3's power to protect against attackers using password-guessing as their access tool.

"The first big new feature in WPA3 is protection against offline, password-guessing attacks. This is where an attacker captures data from your Wi-Fi stream, brings it back to a private computer, and guesses passwords over and over again until they find a match. With WPA3, attackers are only supposed to be able to make a single guess against that offline data before it becomes useless; they'll instead have to interact with the live Wi-Fi device every time they want to make a guess. (And that's harder since they need to be physically present, and devices can be set up to protect against repeat guesses.)"-

The Wi-Fi Alliance, a trade group that oversees WPA3, on Monday announced the protocol had been finalized. Now what? "WPA3 maintains interoperability with WPA2 devices through a transitional mode of operation," the announcement stated. What is more, the announcement said, "As market adoption of WPA3 grows, the new generation of Wi-Fi security will become required for all Wi-Fi CERTIFIED devices."

More specifically, Barrett said in *Wired* that the Alliance expected broad implementation late 2019 at the earliest.

More information: www.wi-fi.org/news-events/news … tified-wpa3-security