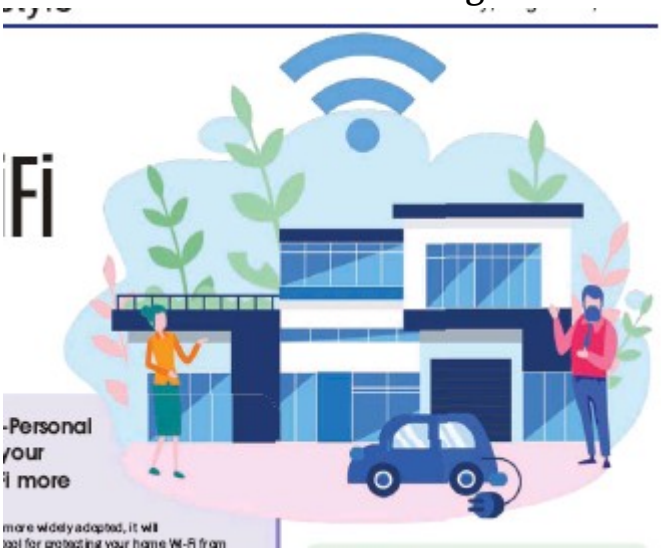
- Internet

Understanding what your future home WiFi network could be

Manila Bulletin · 15 Aug 2018 · C-2 · By JERICHO GONZALES

Wi-Fi Protected Access, or WPA, is the Internet security protocol developed by the Wi-Fi Alliance (owner of the "Wi-Fi" trademark) to secure wireless computer networks. Today, wireless networks use the second generation of WPA called WPA2.



A new era of Wi-Fi security began on June 25, 2018 when the Wi-Fi Alliance introduced WPA3—the latest generation of WPA. It is meant to replace WPA2, which was released in 2004. WPA3 is the most cutting edge wireless security protocol currently available. It utilizes the latest security methods and prevents the use of legacy security protocols.

With its plethora of new security features, WPA3 aims to: ·simplify Wi-Fi security · increase cryptographic strength for sensitive data markets · allow for more robust user authentication

The Wi-Fi Alliance recognizes the fact that Wi-Fi usage and security is different for each user. This is why the organization designed WPA3 to have two distinct capabilities: 1) WPA3-Personal and 2) WPA3-Enterprise. WPA3 Personal is for individual users while WPA3-Enterprise is for businesses, government institutions, and other entities that require high-level internet security.

This article will discuss WPA3 Personal in detail.

WPA3-Personal

Manila Bulletin · 15 Aug 2018 · C-2

WPA3-Personal is equipped with a technology known as "Simultaneous Authentication of Equals" (SAE), which replaces the Pre-Shared Key (PSK) technology present on WPA2.
It's a more robust user authentication feature that's resistant to password guessing attacks like the offline dictionary method, wherein a hacker attempts to guess a network password by entering words found in the dictionary.
SAE is intended to provide home internet users with better password security, even when they choose passwords that don't meet common password complexity standards. Other features of WPA3-Personal include: • Forward secrecy – This protects data in cases when the password is compromised after data istransmitted. • Ease of use – There is no change to how users can connect to a
network, except that they have improved protection. • Natural password selection – Users can create passwords that are easy to remember. They no longer need to nominate highly complicated passwords.

Why WPA3-Personal will make your home Wi-Fi more secure

Manila Bulletin · 15 Aug 2018 · C-2

Once WPA3 is more widely adopted, it will become a crucial tool for protecting your home Wi-Fi from cyberattacks. Unlike WPA2, WPA3-Personal makes your Wi-Fi password difficult to crack. Brute force attacks—where hackers simply try to guess your password until they get it right without interacting with the router—are no longer possible with WPA3-Personal. This is because with WPA3-Personal, every password guess needs to be authenticated by your router in real time. Another feature of WPA3-Personal that will provide you with improved Wi-Fi security at home is the new forward secrecy feature. In the unlikely event that your Wi-Fi is compromised, attackers will not be able to access previous data traffic due to the fact that it is encrypted. Hackers will only be able to see data traffic that occurred after they hijacked your Wi-Fi.

The future of WPA3

Manila Bulletin · 15 Aug 2018 · C-2

At the moment, WPA2 is still the protocol being used worldwide. WPA3 is just an optional certification for Wi-Fi CERTIFIED devices and will only become mandatory once the market has fully adopted the protocol. However, it would likely take a couple of more years for this to happen. WPA3 is still a new technology, so it hasn't been thoroughly reviewed yet. Security experts haven't had the chance to verify whether or not it has any vulnerabilities. Just like any new technology, issues with WPA3 need to be identified and resolved first before wider implementation can be considered. Significant support from the industry might make WPA3 adoption happen sooner rather than later, though. Multinational tech companies like Cisco, Qualcomm Technologies, and Huawei have already stated that they stand behind WPA3 and the Wi-Fi Alliance's efforts to boost Internet security. Right now, all we can do is wait for the day when WPA3 becomes the standard wireless internet security protocol not just for homes, but for businesses as well.

Wi-Fi CERTIFIED Easy Connect

Manila Bulletin · 15 Aug 2018 · C-2

In conjunction with WPA3, the Wi-Fi Alliance also announced a new program called "Wi-Fi CERTIFIED Easy Connect", which makes it easier to onboard new Wi-Fi devices by eliminating the display interface.

With "Wi-Fi Easy Connect", users can add any device to a Wi-Fi network in an instant. All they need to do is scan that device's quick response (QR) code by using another device capable of scanning QR codes (e.g. smartphones).

The Wi-Fi Alliance's goal with the new program is to enhance user experience and maintain high standards of security at the same time.