Learn about WPA3, the latest WiFi security standard today

Wi-Fi Alliance has just announced WPA3, a Wi-Fi security standard that will replace WPA2. This is one of the coolest things ever published at CES 2018. In a few years, when robots fold smart clothes and refrigerators will be forgotten, WPA3 will be everywhere that makes hacking. Wi-Fi becomes more difficult.

Wi-Fi Alliance has just announced WPA3, a Wi-Fi security standard that will replace WPA2. This is one of the coolest things ever published at CES 2018. In a few years, when robots fold smart clothes and refrigerators will be forgotten, WPA3 will be everywhere that makes hacking. Wi-Fi becomes more difficult.

1. Wifi security: should use WPA2-AES, WPA2-TKIP or both?

What is WPA2 and WPA3?

"WPA" stands for Wi-Fi Protected Access. If you have a password on your home Wi-Fi, you can use WPA2 to protect your network, WPA2 is the second version of the Wi-Fi Protected Access standard. There are older standards like WPA (also known as WPA1) and WEP, but they are no longer secure.

1. Wireless security: Say NO to WEP and YES to WPA

WPA2 is a security standard that regulates what happens when connecting to a Wi-Fi network that is closed with a password. WPA2 determines the protocol that the router and Wi-Fi client device uses to perform "handshakes", allowing them to securely connect and how they communicate. Unlike the original WPA standard, WPA2 requires AES encryption to be stronger and much more difficult to crack. This encryption ensures that Wi-Fi access points (such as routers) and Wi-Fi clients (such as laptops or phones) can communicate wirelessly without

traffic.

Technically, WPA2 and WPA3 are hardware certifications that device manufacturers must register. The device manufacturer must fulfill the required security features before marketing their device "Wi-Fi CERTIFIED ™ WPA2 ™" or "Wi-Fi CERTIFIED ™ WPA3 ™".

WPA2 standards have served us well, but it has been around for a long time since 2004, 14 years ago. WPA3 will improve the WPA2 protocol with more security features.

How is WPA3 different from WPA2?

The WPA3 standard has four additional features that you won't find in WPA2. Manufacturers must fully implement these four features to market their device "Wi-Fi CERTIFIED ™ WPA3 ™".

Security on public Wi-Fi networks

Currently, open Wi-Fi networks like the ones you can find at airports, hotels, cafes and other public places are not highly secure. Because they open and allow people to connect, traffic is sent through them unencrypted. For example, when logging into the site using an open network, everything sent via the connection is sent in plain text that people can view and steal. The increase in encrypted HTTPS connections on the web has improved everything, but people can still see which websites you have connected and see HTTP content pages.

WPA3 fixes this problem by using "personal data encryption". When connecting to an open Wi-Fi network, the traffic between the device and the Wi-Fi access point is encrypted, although you do not enter a password when connecting. This will make public and open Wi-Fi networks more private. Hackers won't be able to 'snoop' you without actually cracking the encryption. The problem with public Wi-Fi hotspots needs to be solved a long time ago, but at least now it has been fixed.

Protection against Brute-Force attacks

When a device connects to a Wi-Fi access point, these devices will perform a "handshake", ensuring you use the correct password to connect and "negotiate" the encryption used to protect it. Secret connection. This handshake proved the possibility of being attacked by KRACK in 2017, although existing WPA2 devices can be fixed with

this software update.

WPA3 defines a new handshake "will provide strong protection even when users choose a short and uncomplicated password. In other words, even if you are using a weak password, the WPA3 standard will protect against brute-force attacks, this is the type of attack that a client tries to guess the password, this action repeats until it finds the correct password. Mathy Vanhoef, home Security research has discovered KRACK, which is very enthusiastic about security improvements in WPA3.

The connection process is easier for devices without screens

The world has changed a lot in fourteen years. Today, you often see Wi-Fi-enabled devices without screens. Everything from Amazon Echo and Google Home to smart plugs and light bulbs can connect to Wi-Fi networks. But people often find it difficult to connect these devices to Wi-Fi networks because they don't have a screen or keyboard to enter the password. To connect devices, users often use the smartphone application to enter a Wi-Fi password (or temporarily connect to a second network).

WPA3 has a promising feature that "simplifies the security configuration process for devices that have limited or no display interface". It's not clear how it works, but this feature may be similar to the Wi-Fi Protected Setup feature, just press the button on the router to connect the device. Wi-Fi Protected Setup has its own security issues and does not simplify connecting devices without screens, so it will be interesting to see exactly how this feature works and its safety level.

Higher security for government, defense and industrial applications

Home users may not be interested in this final feature, but the Wi-Fi Alliance also claims that WPA3 will include a "192-bit security suite, corresponding to the CNSA solution (Commercial National Security Algorithm).) of the Committee on National Security Systems, which is intended for government, defense, and industrial applications.

The National Security System Committee (CNSS) is part of the US National Security Agency, so this change will add a feature required by the US government to allow stronger encryption on Important Wi-Fi networks.

When can you use this standard?

According to the Wi-Fi Alliance, devices that support WPA3 will be released at the end of 2018. The device must be WPA3 certified to implement these features, in other words, they must register and be granted "Wi- Fi CERTIFIED ™ WPA3 ™ ", so you will start to see this logo on new routers and other wireless devices starting at the end of 2018.

Wi-Fi Alliance has not announced anything about current devices that receive WPA3 support, but we do not expect that many devices will receive software or firmware updates to support WPA3. Device manufacturers can theoretically create software updates that add these features to existing routers and other Wi-Fi devices, but they have to go through the trouble of applying. and receive WPA3 certification for current hardware before making an update. Most manufacturers can take the time to develop new hardware devices instead.

Even if you have a WPA3 router, you'll need WPA-compatible client devices, such as laptops, phones and anything that connects to Wi-Fi to get the most out of these new features. The good news is that the same router can accept WPA2 and WPA3 connections at the same time.

When all devices support WPA3, you can disable the WPA2 connection on the router to improve security, the same way you disable WPA and WEP connections and only allow WPA2 connections on the router.

See more:

1. Upgrade Wi-Fi security from WEP to WPA2
2. 3 steps to enhance wireless router security
3. KRACK attack breaks down the WPA2 WiFi protocol