Secura

WILL WPA3 FINALLY ENSURE SECURE WI-FI?

By Tom Tervoort, Security Specialist at Secura

July 2018

SECURA

Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T +31 (0)40 23 77 990
E info@secura.com
W www.secura.com

Follow us on

Will WPA3 Finally Ensure Secure Wi-Fi?

In the two decades since its introduction, Wi-Fi has become omnipresent: from laptops to TVs, from phones to 'smart' toothbrushes. And when devices want to wirelessly communicate online or with each other, they are probably using Wi-Fi. Unfortunately the underlying protocols have various vulnerabilities, and enable attackers to eavesdrop wireless communication or gain access to restricted networks. Now, the Wi-Fi Alliance has released the improved Wi-Fi security standard WPA3, along with two sister standards. Will these improvements finally allow us to put more trust in the security of our wireless communications? Major vulnerabilities in WPA2 are fixed, but some shortcomings are still present.

The Need for Wi-Fi Security

The original designers of IEEE 802.11, the Wi-Fi standard, already realised that wireless communication introduces a number of security issues, when compared to connections via wired networks. In order to attack wireless networks, attackers do not need to dig up cables or sneak into a building to access the internal network. Instead, they just need to be in the proximity of a victim and/or access point. You are going to need some rather thick walls (or a Faraday cage) to keep them out.

This issue was originally addressed by the WEP protocol introduced in 1997. It allowed access control based on a password, and used cryptography to protect against eavesdroppers. Unfortunately WEP had a number of large cryptographic flaws, and was completely broken within a few years after its introduction. It was succeeded by first WPA and then WPA2, and researchers started to find flaws in these protocols as well, shortly after their introduction.

The most recent attack against WPA2, called KRACK, was published in October 2017, and allowed attackers to partially decrypt information from protected connections. See our previous post: How broken is WPA2 really and what to do? In this case, vendors could apply patches that mitigate this issue without breaking compatibility. Unfortunately some issues with WPA2 are more fundamental in nature, and cannot simply be patched out without changing the protocol itself.

Of course one can simply assume that Wi-Fi is insecure, and rely on transport- or application-level security (using the TLS protocol, for example) to guard the confidentiality and integrity of communications. This puts the burden of protecting communications on developers and other third parties, instead of the owner of the network. While the adoption of secure protocols by applications has increased considerably, this remains largely invisible for the end-user: they usually have no

means of assessing that it is fine to use app A when connected to their trains' Wi-Fi network, while using app B is risky because its developers didn't take the right measures to implement transport security.

Being able to eavesdrop upon or modify data in transit is one issue, but it should not be forgotten that proper access control to networks can also be very important. This is usually not very problematic within typical home networks (although it may be annoying that the neighbours are using your bandwidth to stream Netflix or try to access your NAS). However it can become a significant issue in corporate settings, since for many companies, it can be beneficial to allow wireless access from employee devices to (parts of) the internal corporate network. An attacker who can subvert Wi-Fi security, may therefore be able to gain a foothold within the internal network, and use that as a basis for further attacks.

The State of Wi-Fi Security Today

So, what are the Wi-Fi security issues that are still present today? Despite problems that can be mitigated by software patches or configuration changes, contemporary Wi-Fi standards still have the following problems:

- **Open/public Wi-Fi is not encrypted.** The WPA2 standard does not support 'open' access points: i.e. public Wi-Fi networks for which the user do not need to enter a password. Therefore, whenever you want to offer a hassle-free guest network, or Wi-Fi as a public service, the users of the system will be at risk. Attackers can passively 'sniff' any nearby traffic with commodity hardware.

- **WPA2 Personal passwords can be cracked offline.** The WPA2 Personal standard allows setting up Wi-Fi access points that are protected by a password; a common set-up for home networks. Unfortunately, when an attacker sniffs the handshake used to establish a connection, they can try to figure out both the encryption key and the password by performing an offline brute-force attack. This means that they can do thousands of automatic password guesses per second, with no limit on the amount of tries. The only way to counter this is to set long and complex passwords that users will have a hard time remembering or entering.

- **Users of the same WPA2 Personal network can decrypt each other's traffic.** As open Wi-Fi networks are unencrypted, companies often offer Wi-Fi access based on passwords that are handed out on request, or shown on a sign. The extra security offered by this solution is very limited, though, as an attacker who knows the password can decrypt the traffic of anyone else using the same network, even if they intercepted the encrypted traffic before learning the value of the password. This means that it is not possible to securely separate different users of the same WPA2 network: as long as they use the same password, users can decrypt each others' traffic. This problem also significantly increases the impact of a successful brute-force attack against the password.

- **WPA2 Enterprise clients are difficult to configure securely.** The WPA2 Enterprise standards allow different users to log in with a combination of a username and a password, and optionally also with a private key stored on their device. When every user has unique credentials, it becomes possible to avoid the attacks as described above in WPA2 Personal. However, all the commonly implemented authentication protocols are vulnerable to attackers who impersonate an access point, and who are then capable of stealing user credentials and decrypting traffic. This can be protected against with the PEAP protocol, but this is only effective when the client device correctly verifies a servers' certificate. Doing so requires that all users of the network are provided with a certificate and configure their devices to check it. The latter is difficult to do, especially on mobile devices. Most importantly, when system administrators have no control over user devices, they are not able to enforce them to connect securely. There are additional mitigating measures that, for example, detect rogue access points, but these are not directly linked to the WPA2 technology.

- **It is difficult to securely connect IoT devices.** IoT developers are currently struggling with how they can design devices that securely communicate with each other or the home networks of users. This is especially difficult when devices do not have a display or input device that users can use to enter their home's Wi-Fi password. A protocol called WPS was designed with the intend of solving this issue: by pressing a button on their device and router at the same time, or by entering a short PIN code, users can quickly connect devices to their network. Unfortunately the cryptographic protocol employed by WPS is insecure, and encryption keys can be retrieved by attackers after about half an hour of computation.

Due to these issues, it is currently very difficult to offer user-friendly Wi-Fi to people, without exposing them to significant risks.

The New WPA3 Standard

The new standards are supposed to address vulnerabilities as discussed above. WPA3 once again defines two variations: WPA3 Personal (authentication with a password), and WPA3 Enterprise (authentication with user-specific credentials). Furthermore, the Wi-Fi alliance has also released two related standards: Wi-Fi Enhanced Open (which is intended to improve security of public networks with no authentication) and Wi-Fi Easy Connect (a successor to WPS that offers an alternative method of connection).

Wi-Fi Enhanced Open

With the Wi-Fi Enhanced Open standard, it finally becomes possible to offer encrypted public Wi-Fi, without requiring users to enter any password. Encryption in this case means opportunistic encryption: by performing a cryptographic key exchange, attackers who passively sniff network traffic will not be able to find out what the key is, and can therefore not decrypt intercepted traffic. Unfortunately the scheme does not offer any mechanism to authenticate access points. This means that an active attacker, who impersonates an access point, can still trick clients into setting up an (encrypted) connection with them instead of the network they wish to connect to. They are still able to change and eavesdrop upon all traffic.

In practice, this means that open Wi-Fi is still insecure, it just means that attackers have somewhat fewer options for exploiting this fact. Active interfering is more difficult than passively listening, and is actually possible to detect. Furthermore, the standards' requirement to make use of Protected Management Frames make a so-called de-authentication attack (which forces devices to reconnect) more difficult.

Nonetheless, an attacker can still simply set up a hotspot with the same name as a popular public Wi-Fi network (e.g. "Wi-Fi in my coffee shop") and snoop on traffic. They just need to send stronger signals than the legitimate network, or set it up in a different location and rely on devices connecting to it automatically without their users noticing.

This is of course a fundamental issue with public Wi-Fi: anyone can call their network whatever name they want, and users do not have the option to verify the authenticity of the access points they're connecting to. However, the attack opportunities can be decreased dramatically if a Trust On First Use (TOFU) system were to be employed. In practice, users only select that they want to use a particular network once, and their device will automatically keep connecting to it in the future. If the device were to transmit a public key during that first connection, it could be used to identify itself for any future connections. Unfortunately, the Wi-Fi Enhanced Open standard does not provide such a solution, which is a missed opportunity.

WPA 3 Personal

WPA3 Personal offers the same type of functionality as its WPA2 equivalent: an encrypted Wi-Fi network to which you authenticate with a password.

The most significant improvement of this protocol is the introduction of the SAE handshake protocol. SAE is a cryptographic password-authenticated key agreement protocol, which allows two parties (in this case a client device and an access point) to prove to each other that they are in possession of the same password, without revealing any information to a potential attacker that could be used to recompute this password.

This mechanism prevents attackers from performing off-line password guessing attacks. They can only try online attacks: i.e. try to do a handshake with a single password and see if it is accepted. This is significantly slower than an offline attack and can easily be detected or defended against, since it requires an attacker to perform a large volume of failed authentication attempts.

When an attacker does know the password, they are still not able to passively decrypt any encrypted data they intercepted without interfering with the handshake. This implies forward secrecy, learning the password in the future does not allow you to decrypt communication that was sniffed in the past. Unfortunately, an attacker who does know the password can still impersonate an access point and thus perform a man-in-the-middle-attack to eavesdrop on traffic.

Like with Wi-Fi Enhanced Open, no TOFU system is in place that could partially mitigate this problem. This means that, even with WPA3, it is still not safe to publish the same password to multiple different users.

WPA3 Enterprise

WPA3 Enterprise disallows some deprecated authentication protocols, but only really offers one new option that is not already present in WPA2: namely 192-bit mode.

This mode simply replaces some of the cryptographic algorithms involved with equivalent versions that use somewhat larger keys. It does not actually protect against any currently known attack, and does not address the complications of certificate verification by clients. In theory, due to a major cryptanalytic breakthrough, an attack could be discovered that would be effective against the standard mode, but happens to be ineffective against 192-bit mode, but this is unlikely.

While the gain from using 192-bit mode is limited, perhaps some companies may find this mode useful for marketing or compliance purposes.

Wi-Fi Easy Connect

Wi-Fi Easy Connect attempts to address the problems WPS originally failed to solve: to make it more user-friendly to securely connect devices, even when these devices do not have a screen or method to enter passwords.

The basic idea is that all systems involved (e.g. routers, phones, IoT devices) own a key pair that uniquely identifies each of them. Once device A is aware of the public key of device B, a secure connection between A and B can be set up through an authenticated key exchange. An attacker will not be able to impersonate device B or perform a man-in-the-middle attack.

Furthermore, once a device has set up a connection with an access point itself, it can also act as a configurator, and grant other devices (of which public keys are known) access to the same access point.

In order for this mechanism to work, some method needs to be available to securely transport public keys among devices. Unlike passwords, these do not have to be kept secret, as long as an attacker cannot substitute them with their own keys. While current IoT devices will largely not be compatible, this does seem the way to go for next generations to come.

The first proposed method to distribute keys is to use QR codes. A typical scenario would be that someone first scans a label on their router with a cell phone, which subsequently gets access to a secure Wi-Fi connection to the internet. Next, a QR code on a device without a screen (say, a printer) can be scanned with the same phone. This allows the phone to set up a secure connection with the printer, which it can then use to tell the printer how to connect to the router. It is not necessary to input any password on the printer itself.

Unlike WPA3 or Wi-Fi Enhanced Open, this system can also be used to offer secure public Wi-Fi: put a QR code on a sign and any user who scans it gains access to a guest network. This is less of a hassle than having to type in a password, and can only be attacked when the attacker physically alters the contents of the sign.

Other key distribution methods are also defined: instead of QR codes it is also possible to use NFC or Bluetooth. Additionally, public keys can be transferred wirelessly, with the possibility to check their authenticity based on a shared secret. These different methods each have different security properties.

Conclusion

The new standards can be considered to be hit-and-miss: connecting to open Wi-Fi networks will remain dangerous despite implementation of Wi-Fi Enhanced Open. Major vulnerabilities in WPA2 are fixed, but some shortcomings are still present. The overview is present in the table below.

Protection against Wi-Fi attacks, per technology

	Open Wi-Fi	WPA2 Personal	WPA2 Enterprise (PEAP)	WPA3 Personal	WPA3 Enterprise (PEAP)	Protected Open	Easy Connect (QR Code)
Passive sniffing	✗	✓	✓	✓	✓	✓	✓
Offline password cracking	N/A	✗	✓	✓	✓	N/A	N/A
Active attack/ spoofed AP	✗	✓	✓/✗[1]	✓	✓/✗[1]	✗	✓
Passive sniffing by an authenticated attacker[2]	✗	✗	✓	✓	✓	✓	✓
Active attack by an authenticated attacker[2]	✗	✗	✓/✗[1]	✗	✓/✗[1]	✗	✓

[1] Only protected when all clients are configured to verify certificates correctly
[2] An attacker who has the credentials to access the network themselves, and targets other users of the same network

The most promising of the standards is Wi-Fi Easy Connect, which among other things can be used to offer secure guest networks, or facilitate secure communication with and between IoT devices. When applied correctly, this has the potential of solving numerous security and usability issues at the same time.

If you would like more details about these standards or an assessment of your Wi-Fi network (configuration) or the security of your IoT devices, feel free to contact us.

About Secura

Secura has worked in information security and privacy for nearly two decades. This is why we uniquely understand the challenges that you face like no one else and would be delighted to help you address your information security matters efficiently and thoroughly. We work in the areas of people, processes and technology. For our customers we offer a range of security testing services varying in depth and scope.

Secura has the mission to support organizations with up-to-date knowledge to work toward a bright and safe future.

Keep updated with the latest insights on digital security and subscribe to our periodical newsletter.

Interested?

Contact us today at info@secura.com or visit secura.com for more information.

SUBSCRIBE

TO OUR NEWSLETTER

Secura