Wireless Security Protocols: WEP, WPA, WPA2, and WPA3

WE'LL TRY TO EXPLAIN THE DIFFERENCES AMONG THE ENCRYPTION STANDARDS LIKE WEP, WPA, WPA2, AND WPA3 SO YOU CAN SEE WHICH ONE WILL WORK BEST FOR YOUR NETWORK ENVIRONMENT.

WiFi security algorithms have been through many changes and upgrades since the 1990s to become more secure and effective. Different types of wireless security protocols were developed for home wireless networks protection. The wireless security protocols are WEP, WPA, and WPA2, serving the same purpose but being different at the same time.

Not only do the wireless security protocols prevent unwanted parties from connecting to your wireless network, but also encrypt your private data sent over the airwaves.

No matter how protected and encrypted, wireless networks cannot keep up in safety with wired networks. The latter, at their most basic level, transmit data between two points, A and B, connected by a network cable. To send data from A to B, wireless networks broadcast it within their range in every direction to every connected device that happens to be listening.

Let's have a closer look at WEP, WPA, WPA2, and WPA3 wireless security protocols.

PROTOCOL #1

WEP. Wired Equivalent Privacy

1999 - 2004 standard. Easy to break and hard to configure. Abandoned.

1

Security • Poor

1

Configurable • Hard

WEP was developed for wireless networks and approved as a Wi-Fi security standard in September 1999. WEP was supposed to offer the same security level as wired networks, however there are a lot of well-known security issues in WEP, which is also easy to break and hard to configure.

Despite all the work that has been done to improve the WEP system it still is a highly vulnerable solution. Systems that rely on this protocol should be either upgraded or replaced in case security upgrade is not possible. WEP was officially abandoned by the Wi-Fi Alliance in 2004.

PROTOCOL #2

WPA. Wi-Fi Protected Access

Was used as a temporary enhancement for WEP. Easy to break. Configuration: moderate

2

Security • Poor

3

Configurable • More or less

For the time the 802.11i wireless security standard was in development, WPA was used as a temporary security enhancement for WEP. One year before WEP was officially abandoned, WPA was formally adopted. Most modern WPA applications use a pre-shared key (PSK), most often referred to as WPA Personal, and the Temporal Key Integrity Protocol or TKIP (/tiːˈkɪp/) for encryption. WPA Enterprise uses an authentication server for keys and certificates generation.

WPA was a significant enhancement over WEP, but as the core components were made so they could be rolled out through firmware upgrades on WEP-enabled devices, they still relied onto exploited elements.

WPA, just like WEP, after being put through proof-of-concept and applied public demonstrations turned out to be pretty vulnerable to intrusion. The attacks that posed the most threat to the protocol were however not the direct ones, but those that were made on Wi-Fi Protected Setup (WPS) - auxiliary system developed to simplify the linking of devices to modern access points.

PROTOCOL #3

WPA2. Wi-Fi Protected Access version 2

Since 2004. AES encryption.

4

Security • Good

4

Configurable • Norm

The 802.11i wireless security standard based protocol was introduced in 2004. The most important improvement of WPA2 over WPA was the usage of the Advanced Encryption Standard (AES). AES is approved by the U.S. government for encrypting the information classified as top secret, so it must be good enough to protect home networks.

ADVANCED ENCRYPTION STANDARD IS APPROVED BY THE U.S. GOVERNMENT

At this time the main vulnerability to a WPA2 (/krack-wifi-vulnerability-wpa2.html) system is when the attacker already has access to a secured WiFi network and can gain access to certain keys to perform an attack on other devices on the network. This being said, the security suggestions for the known WPA2 vulnerabilities are mostly significant to the networks of enterprise levels, and not really relevant for small home networks.

Unfortunately, the possibility of attacks via the Wi-Fi Protected Setup (WPS), is still high in the current WPA2-capable access points, which is the issue with WPA too. And even though breaking into a WPA/WPA2 secured network through this hole will take anywhere around 2 to 14 hours it is still a real security issue and WPS should be disabled and it would be good if the access point firmware could be reset to a distribution not supporting WPS to entirely exclude this attack vector.

Which security method will work for your network

Here is the basic rating from best to worst of the modern WiFi security (/wifi-network-security.html) methods available on modern (after 2006) routers:

WPA2 + AES
WPA + AES
WPA + TKIP/AES (TKIP is there as a fallback method)
WPA + TKIP
WEP
Open Network (no security at all)

The best way to go is to deactivate Wi-Fi Protected Setup (WPS) and set the router to WPA2 +AES. As you go down the list, you are getting less security for your network.

Purpose
Both WPA and WPA2 are supposed to secure wireless Internet networks from unauthorized access. If you leave your router with no security then anyone can steal the bandwidth, perform illegal actions out of your connection and name, monitor your web activity, and easily install malicious apps in your network.

WPA vs. WPA2

WiFi routers (/choose-wifi-router.html) support a variety of security protocols to secure wireless networks: WEP, WPA and WPA2. However WPA2 is recommended over its predecessor WPA (Wi-Fi Protected Access).

Probably the only downside of WPA2 is how much processing power it needs to protect your network. This means more powerful hardware is needed to avoid lower network performance. This issue concerns older access points that were implemented before WPA2 and only support WPA2 via a firmware upgrade. Most of the current access points have been supplied with more capable hardware.

Definitely use WPA2 if you can and only use WPA if there is no way your access point will support WPA2. Using WPA is also a possibility when your access point regularly experiences high loads and the network speed suffers from the WPA2 usage. When security is the top priority then rolling back is not an option, instead one should seriously consider getting better access points. WEP has to be used if there is no possibility to use any of the WPA standards.

Encryption Speed

Depending on what security protocols you use the data speed can be affected. WPA2 is the fastest of the encryption protocols, while WEP is the slowest.

Protect Your WiFi Network

While WPA2 offers more protection than WPA and therefore provides even more protection than WEP, the security of your router heavily depends on the password you set. WPA and WPA2 let you use passwords of up to 63 characters.

Use as many various characters in your WiFi network password (/how-to-change-wifi-password.html) as possible. Hackers are interested in easier targets, if they can't break your password in several minutes, they will most likely move on to look for more vulnerable networks. Summary:

WPA2 is the enhanced version of WPA;
WPA only supports TKIP encryption while WPA2 supports AES;

Theoretically, WPA2 is not hackable while WPA is;

WPA2 needs more processing power than WPA;

Use NetSpot (/netspotpro.html) to check your encryption!

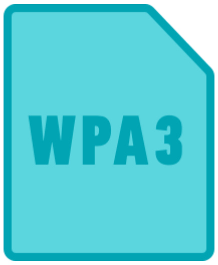
Check your Encryption using NetSpot

Powerful advanced tool for multiple Wi-Fi networks Surveys, Analysis and Troubleshooting.

Get NetSpot → (/netspotpro.html)

macOS 10.10+, Windows 7/8/10

PROTOCOL #4



WPA3. Wi-Fi Protected Access version 3

Coming soon. Password protection. WiFi easy connect.

5

Security • Excellent

5

Configurable • Excellent

UPD: WPA3 is the next generation of WiFi security

Protecting Wi-Fi from hackers is one of the most important tasks in cybersecurity. Which is why the arrival of next-generation wireless security protocol WPA3 deserves your attention: Not only is it going to keep Wi-Fi connections safer, but also it will help save you from your own security shortcomings.
Here is what it offers:

Password Protection

Start with how WPA3 will protect you at home. Specifically, it'll mitigate the damage that might stem from your lazy passwords.

A fundamental weakness of WPA2, the current wireless security protocol that dates back to 2004, is that it lets hackers deploy a so-called offline dictionary attack to guess your password. An attacker can take as many shots as they want at guessing your credentials without being on the same network, cycling through the entire dictionary — and beyond — in relatively short order.

WPA3 will protect against dictionary attacks by implementing a new key exchange protocol. WPA2 used an imperfect four-way handshake between clients and access points to enable encrypted connections; it's what was behind the notorious KRACK vulnerability that impacted basically every connected device. WPA3 will ditch that in favor of the more secure — and widely vetted — Simultaneous Authentication of Equals handshake.

The other benefit comes in the event that your password gets compromised nonetheless. With this new handshake, WPA3 supports forward secrecy, meaning that any traffic that came across your transom before an outsider gained access will remain encrypted. With WPA2, they can decrypt old traffic as well.

Safer Connections

When WPA2 came along in 2004, the Internet of Things had not yet become anything close to the all-consuming security horror that is its present-day hallmark. No wonder, then, that WPA2 offered no streamlined way to safely onboard these devices to an existing Wi-Fi network. And in fact, the predominant method by which that process happens today — Wi-Fi Protected Setup — has had known vulnerabilities since 2011. WPA3 provides a fix.

Wi-Fi Easy Connect, as the Wi-Fi Alliance calls it, makes it easier to get wireless devices that have no (or limited) screen or input mechanism onto your network. When enabled, you'll simply use your smartphone to scan a QR code on your router, then scan a QR code on your printer or speaker or other IoT device, and you're set — they're securely connected. With the QR code method, you're using public key-based encryption to onboard devices that currently largely lack a simple, secure method to do so.

That trend plays out also with Wi-Fi Enhanced Open, which the Wi-Fi Alliance detailed a few weeks before. You've probably heard that you should avoid doing any sensitive browsing or data entry on public Wi-Fi networks. That's because with WPA2, anyone on the same public network as you can observe your activity, and target you with intrusions like man-in-the-middle attacks or traffic sniffing. On WPA3? Not so much.

When you log onto a coffee shop's WPA3 Wi-Fi with a WPA3 device, your connection will automatically be encrypted without the need for additional credentials. It does so using an established standard called Opportunistic Wireless Encryption.

As with the password protections, WPA3's expanded encryption for public networks also keeps Wi-Fi users safe from a vulnerability they may not realize exists in the first place. In fact, if anything it might make Wi-Fi users feel too secure.

WPA3: When Can I Get It On My Wi-Fi?

Even with the added technical details, talking about WPA3 feels almost premature. While major manufacturers like Qualcomm already have committed to its implementation as early as this summer, to take full advantage of WPA3's many upgrades, the entire ecosystem needs to embrace it. That'll happen in time, just as it did with WPA2.

The Wi-Fi Alliance doesn't expect broad implementation until late 2019 at the earliest.

Once all your devices support WPA3, you could disable WPA2 connectivity on your router to improve security, the same way you might disable WPA and WEP connectivity and only allow WPA2 connections on your router today.

While it will take a while for WPA3 to fully roll out, the important thing is that the transition process is beginning in 2018. This means safer, more secure Wi-Fi networks in the future.

Check your Encryption using NetSpot

Powerful advanced tool for multiple Wi-Fi networks Surveys, Analysis and Troubleshooting.

Get NetSpot → (/netspotpro.html)

macOS 10.10+, Windows 7/8/10

FAQ

What are the types of wireless security protocols?

There are WEP, WPA, WPA2, and WPA3 wireless security protocols:

- WEP (Wired Equivalent Privacy) was approved as a Wi-Fi security standard in September 1999. Initially WEP was expected to offer the same security level for wireless networks as wired networks do, however there are a lot of well-known issues in WEP, which are easy to exploit.

- WPA (Wi-Fi Protected Access) was used as a temporary security enhancement for WEP while the 802.11i wireless security standard was in its development stage. One year before WEP was officially dropped, WPA was formally adopted. Even though WPA was a significant enhancement over WEP, its big issue was that the core components were made so they could be rolled out through firmware upgrades on WEP-enabled devices, so it didn't provide enough security from hacker attacks.

- WPA2 (Wi-Fi Protected Access version 2) was introduced in 2004. The most important improvement this 802.11i wireless security standard offered over its predecessor was the implementation of the Advanced Encryption Standard (AES). AES is approved by the U.S. government for encryption of the top secret data, which speaks for itself. The issue with WPA2 is that if an attacker has direct access to a secured network and can gain access to certain keys they can perform an attack on other devices on the network. This issue is considered significant only for enterprise level networks, smaller and home networks are usually not the target.

- WPA3 (Wi-Fi Protected Access version 3) is the latest security protocol with top standards. WPA3 protects against dictionary attacks and uses Simultaneous Authentication of Equals handshake, which protects its network from attacks that could be possible with WPA2 in place. WPA3 is really good on public networks (say in a coffee place), because it automatically encrypts the connection without any need for additional credentials.

Which security method will work for your network?

Here's the list of modern (after 2006) security methods used on wireless networks, from best to worst:

- WPA2 + AES
- WPA + AES
- WPA + TKIP/AES (TKIP as a fallback method)
- WPA + TKIP
- WEP
- Open Network (no security at all)

How to Protect Your WiFi Network?

Security protocols are important, and the later the version the better your network is protected. But it is also crucial to set a solid password for your network. WPA and WPA2 protocols let you set passwords of up to 63 characters. Make your password hard to break by using special characters, lower and uppercase letters and numbers, avoid simple dictionary words.

Have more questions?
Submit a request (/help/#contactus) or write a couple words.

Read next in All about Wi-Fi

If you want to dive deeper into this Wi-Fi thing, check out the following articles about Wi-Fi security, the best apps for wireless networking, best WiFi routers, etc.

All You Need to Know About WiFi Routers

Learn more (/about-wifi-routers.html) →

The most important WiFi settings you need to know about

Learn more (/the-most-important-wifi-settings.html) →

Check out the list of the best WiFi extenders 2018

Learn more (/best-wifi-extenders-2018.html) →

Other Articles

Learn more about WiFi direct and how it works (/what-is-wifi-direct.html)

FREE WiFi channel scanner for Mac OS X & Windows (/wireless-network-wifi-scanner.html)

Use NetSpot as a WiFi network analyzer (/wlan-wifi-analyzer.html)

How to boost WiFi signal strength — NetSpot for Mac OS X (/wifi-signal-strength.html)

Test & improve WiFi network speed (/wireless-network-speed.html)

Monitor Wi-Fi signal and map Wi-Fi coverage (/wifi-network-monitor.html)

WiFi Security with NetSpot (/wifi-network-security.html)

Choose the best Wi-Fi channel with NetSpot Scanner (/wifi-channel-scanner.html)

PRODUCT

Features (/features.html)

Enterprise (/enterprise.html)

Pricing (/netspotpro.html)

NetSpot Trial (/gettrial.html)

PLATFORMS

For Android (/netspot-wifi-analyzer-for-android.html)

For Windows (/download-win.html)

For macOS (/download-mac.html)

For iOS (/netspot-for-ios.html)

RESOURCES

Help Center (/help/)

Press (/press.html)

Download NetSpot (/downloads.html)

EULA (/help/eula/)

Blog (/mother-of-all-pages.html)

FOLLOW US

Twitter (https://twitter.com/netspotapp)

Facebook (https://www.facebook.com/netspotapp)

YouTube (https://www.youtube.com/user/Paul43883/feed)

CONTACT US

📍 **8 The Green, Suite #5858, Dover, DE 19901**

✉ **Email us (mailto:onair@netspotapp.com)**

Language: English