The Difference Between WEP, WPA, and WPA2 Wi-Fi Passwords

Even if you know you need to secure your Wi-Fi network (and have already done so), you probably find all the encryption acronyms a little bit puzzling. Read on as we highlight the differences between encryption standards like WEP, WPA, and WPA2–and why it matters which acronym you slap on your home Wi-Fi network.

What Does It Matter?

You did what you were told to do, you logged into your router after you purchased it and plugged it in for the first time, and set a password. What does it matter what the little acronym next to the security encryption standard you chose was? As it turns out, it matters a whole lot: as is the case with all encryption standards, increasing computer power and exposed vulnerabilities have rendered older standards at risk. It's your network, it's your data, and if someone hijacks your network for their illegal hijinks, it'll be the police knocking on your door. Understanding the differences between encryption protocols and implementing the most advanced one your router can support (or upgrading it if it can't support current gen secure standards) is the difference between offering someone easy access to your home network and sitting secure.

WEP, WPA, and WPA2: Wi-Fi Security Through the Ages

Since the late 1990s, Wi-Fi security algorithms have undergone multiple upgrades with outright depreciation of older algorithms and significant revision to newer algorithms. A stroll through the history of Wi-Fi security serves to highlight both what's out there right now and why you should avoid older standards.

Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) is the most widely used Wi-Fi security algorithm in the world. This is a function of age, backwards compatibility, and the fact that it appears first in the encryption type selection menus in many router control panels.

WEP was ratified as a Wi-Fi security standard in September of 1999. The first versions of WEP weren't particularly strong, even for the time they were released, because U.S. restrictions on the export of various cryptographic technology led to manufacturers restricting their devices to only 64-bit encryption. When the restrictions were lifted, it was increased to 128-bit. Despite the introduction of 256-bit WEP encryption, 128-bit remains one of the most common implementations.

Despite revisions to the algorithm and an increased key size, over time numerous security flaws were discovered in the WEP standard and, as computing power increased, it became easier and easier to exploit them. As early as 2001 proof-of-concept exploits were floating around and by 2005 the FBI gave a public demonstration (in an effort to increase awareness of WEP's weaknesses) where they cracked WEP passwords in minutes using freely available software.

Despite various improvements, work-arounds, and other attempts to shore up the WEP system, it remains highly vulnerable and systems that rely on WEP should be upgraded or, if security upgrades are not an option, replaced. The Wi-Fi Alliance officially retired WEP in 2004.

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access was the Wi-Fi Alliance's direct response and replacement to the increasingly apparent vulnerabilities of the WEP standard. It was formally adopted in 2003, a year before WEP was officially retired. The most common WPA configuration is WPA-PSK (Pre-Shared Key). The keys used by WPA are 256-bit, a significant increase over the 64-bit and 128-bit keys used in the WEP system.

Some of the significant changes implemented with WPA included message integrity checks (to determine if an attacker had captured or altered packets passed between the access point and client) and the Temporal Key Integrity Protocol (TKIP). TKIP employs a per-packet key system that was radically more secure than fixed key used in the WEP system. TKIP was later superseded by Advanced Encryption Standard (AES).

Despite what a significant improvement WPA was over WEP, the ghost of WEP haunted WPA. TKIP, a core component of WPA, was designed to be easily rolled out via firmware upgrades onto existing WEP-enabled devices. As such it had to recycle certain elements used in the WEP system which, ultimately, were also exploited.

WPA, like its predecessor WEP, has been shown via both proof-of-concept and applied public demonstrations to be vulnerable to intrusion. Interestingly the process by which WPA is usually breached is not a direct attack on the WPA algorithm (although such attacks have been successfully demonstrated) but by attacks on a supplementary system that was rolled out with WPA, Wi-Fi Protected Setup (WPS), designed to make it easy to link devices to modern access points.

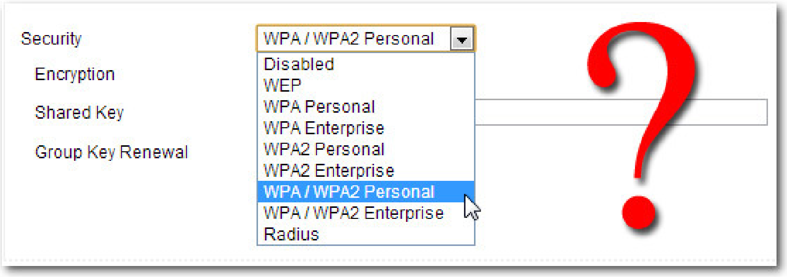
Wi-Fi Protected Access II (WPA2)

WPA has, as of 2006, been officially superseded by WPA2. One of the most significant changes between WPA and WPA2 was the mandatory use of AES algorithms and the introduction of CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) as a replacement for TKIP (still preserved in WPA2 as a fallback system and for interoperability with WPA).

Currently, the primary security vulnerability to the actual WPA2 system is an obscure one (and requires the attacker to already have access to the secured Wi-Fi network in order to gain access to certain keys and then perpetuate an attack against other devices on the network). As such, the security implications of the known WPA2 vulnerabilities are limited almost entirely to enterprise level networks and deserve little to no practical consideration in regard to home network security.

Unfortunately, the same vulnerability that is the biggest hole in the WPA armor, the attack vector through the Wi-Fi Protected Setup (WPS), remains in modern WPA2-capable access points. Although breaking into a WPA/WPA2 secured network using this vulnerability requires anywhere from 2-14 hours of sustained effort with a modern computer, it is still a legitimate security concern and WPS should be disabled (and, if possible, the firmware of the access point should be flashed to a distribution that doesn't even support WPS so the attack vector is entirely removed).

Wi-Fi Security History Acquired; Now What?



Security WPA / WPA2 Personal

At this point, you're either feeling a little smug (because you're confidently using the best encryption scheme available for your Wi-Fi access point) or a little nervous because you picked WEP since it was at the top of the list. If you're in the latter camp, don't fret; we have you covered.

Before we hit you with a further-reading list of our top Wi-Fi security articles, here's the crash course. This is a basic list ranking the current Wi-Fi security methods available on any modern (post-2006) router, ordered from best to worst:

1. WPA2 + AES
2. WPA + AES
3. WPA + TKIP/AES (TKIP is there as a fallback method)
4. WPA + TKIP
5. WEP
6. Open Network (no security at all)

Ideally, you'll disable Wi-Fi Protected Setup (WPS) and set your router to WPA2 +AES. Everything else on the list is a less than ideal step down from that. Once you get to WEP, your security level is so low it's about as effective as a chain link fence–the fence exists simply to say "hey, this is my property" but anyone who actually wanted in would just climb right over it.

If all this thinking about Wi-Fi security and encryption has you curious about other tricks and techniques you can easily deploy to further secure your Wi-Fi network, your next stop should be browsing the following How-To Geek articles:

- How To Secure Your Wi-Fi Network Against Intrusion
- Don't Have a False Sense of Security: 5 Insecure Ways to Secure Your Wi-Fi
- How to Enable a Guest Access Point on Your Wireless Network
- The Best Wi-Fi Articles for Securing Your Network and Optimizing Your Router

Armed with a basic understanding of how Wi-Fi security works and how you can further enhance and upgrade your home network access point, you'll be sitting pretty with a secure Wi-Fi network in short order.

JOIN THE DISCUSSION (3 REPLIES)

Jason Fitzpatrick is a warranty-voiding DIYer who spends his days cracking opening cases and wrestling with code so you don't have to. If it can be modded, optimized, repurposed, or torn apart for fun he's interested (and probably already at the workbench taking it apart). You can follow him on Twitter if you'd like.

- Published 07/16/13

MORE ARTICLES YOU MIGHT LIKE