Wireless Encryption

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).

Golden Rules

- Do not use wireless if you don't have to
- Always use WPA or above. WEP is not secure.
- Never use names, telephone numbers or personal information as passwords or network names
- Don't steal wireless from your neighbour. What goes around, comes around.
- Change your wireless key at least every 3 months if you live in a built up area
- If you suspect your wireless has been hacked, immediately turn it off. Contact your ISP and change your wireless key.

Connect to your Eircom Router

Do everything below using an Ethernet Cable connection. Using Wireless can be problematic.

Log Into Your Router

- Open your internet browser (Firefox, IE, Opera) and type in the address bar: http://192.168.1.254
- Enter your username and password if you are asked for one
- You should now be in the routers home page

Setting Up WPA (aka A Wireless Key)

Golden Rule of Wireless: Never use WEP. It is the equilevent of tissue paper. it is breakable in 1 minute. You can break it faster than you can set it up.

- From your routers home page, click Wireless (Left Hand Side)
- Give your wireless a name. (Hint: Do not use your address, phone number or real name)
- Set Privacy to: WPA-PSK
- Set your Pre Shared Key to a long password. Letters, Number and Symbols are best. Do not use one word. WPA is hacked by dictionary attacks, as such if you use a word in a dictionary it is hackable.

(Download this program: http://www.soroban.co.uk/wepkeygen.htm and create at least a 56 character passphrase Extended WPA KEY)

Similar to this:

O[õê+å®ºÆë8Ï·S`X§9\Y¦¯æà©ÑN,!#Qûîh5ôÑIéëÂiØJ_Ô¥Â&"ÀÚÎs«í

or

dDC>Bs\BC:=Cc&rW]R4k22$s#M!:1:&[%b?b 8P#D/>$8/Mz2-wrhX[v

- Copy and paste your new key to NotePad and into the Pre Shared Key box on your router
- Click Save Changes and say yes to restarting your router
- Once the router has rebooted, open Windows Wireless Networks, search for your network, then use NotePad to copy and paste your new code in when required

Your router is now almost 100% secure.

Advanced Securing - MAC Limiting

- Log into your router
- Click Expert Mode
- Click Statistics
- Click LAN
- Connect every device you have to your wireless. Once you have done this, refresh your browser (Press F5)
- Note every devices MAC Address exactly.
- Click return to your routers home page: http://192.168.1.254
- Click Wireless
- Click Advanced Configuration Options
- Click Limit Wireless Access by MAC Address
- Click Add, then add each devices MAC Address, clicking Submit each time.
- Once finished, click Save Changes and Restart your router.

Explanation: Your router will now only allow devices on the allowed list to connect to your router. This adds an extra layer of protection to your router, thus stopping someone who may have cracked your wireless password from using your wireless. However, MAC Address's can be spoofed, so this is a basic level of protection.

Adding a Router Log In Password (Not the same as your WPA / Wireless Key):

- Go to http://192.168.1.254/indexExptCfgRES...uterpasswd.htm
- Create a new password and ensure the box is checked saying "Enable Local Admin Login"
- Click Save Changes and allow your router to restart if required.
- Now when you log into your router at http://192.168.1.254 your username is "admin" and your password is the one you just created

Explanation: This password will stop anyone who has access to your LAN or Wireless from changing settings or locking you out of your own network.