WiFi Security

There are several types of wireless security that you'll come across – here's a quick rundown on the details.

WEP

Wired Equivalent Privacy, aka WEP, is the grandfather of wireless security types, dating back to 1999. When a client connects to a WEP-protected network, the WEP key is added to some data to create an "initialization vector," or "IV" for short. For example, a 128-bit hexadecimal key is comprised of 26 characters from the keyboard (totaling 104 bits) combined with a 24-bit IV. When a client goes to connect to an AP, it sends a request to authenticate, which is met with a challenge reply from the AP. The client encrypts the challenge with the key, the AP decrypts it, and if the challenge it receives matches the original one it sent, the AP will authenticate the client.

(//metageek.link/inssider-product-page)

This may sound secure, but there was room in this scheme for an exploit to be discovered. The risk presents itself when a client sends its request to the access point – the portion containing the IV is transmitted wirelessly in clear-text (not encrypted). In addition, the IV is simple compared to the key, and when there are several clients using the same WEP key on a network, IVs have an increased probability of repeating. In a busy environment, a malicious user wishing to gain access to a network utilizing WEP security can passively eavesdrop and quickly collect IVs. When enough IVs have been collected, the key becomes trivial to decrypt.

Clearly, WEP is not the correct choice for securing your network, and in light of this, other types of wireless security were created.

WPA

WiFi Protected Access (WPA) was ratified by the WiFi Alliance in 2003 as a response to the insecurities that were discovered in WEP. This new security standard, the Temporal Key Integrity Protocol (TKIP), included several enhancements over WEP, including a new message integrity check nicknamed “Michael.”

While Michael offered a great deal of improvement over the old way of securing networks, there was still some worry about some security issues with using a similar (though much stronger) implementation.

WPA2

The concerns about Michael led to WPA2’s introduction in 2004. At the center of WPA2 is its use of a security protocol based on Advanced Encryption Standard (AES), the U.S. Government’s preferred choice of encryption.

As it stands now, the only people who should still be using TKIP on a wireless network are those who are dealing with hardware that is rated for 802.11g only.

WPS

In 2007, a new security method - WiFi Protected Setup (WPS) - began to show up on wireless access points. With this type of security, a user is able to add new devices to their network by simply pushing a button (within administration software or physically on the router) and then typing in an 8-digit PIN number on the client device. The PIN feature acts as a sort of shortcut for entering

in a longer WPA (WiFi Protected Access) key. The basic idea behind WPS is that having physical access to the AP to hit a button and reading a sticker would provide a more secure implementation of WiFi authentication. Everything was well and good in the WPS world, until last winter, when a security researcher discovered the Achilles Heel in the implementation.

Here's how it works:

The eighth and final digit of the PIN number is a checksum, which is used to make sure the 7 digits that matter don't get corrupted. From these 7 digits, we can see that there are 10,000,000 possibilities (since each of the 7 digits can be 0-9, with repeats allowed). This is still a pretty huge amount of possibilities, and alone could arguably still be considered quite safe -- but there's a flaw in the checking process. When a PIN is being examined by the AP, the first 4 digits (10,000 possibilities) are checked separately from the last 3 digits (1,000 possibilities). This translates into a malicious user only needing to make at most 11,000 guesses, which a computer can handle in a matter of hours!

As you can see, if you or someone you know is currently using WPS on an access point, you should disable the feature ASAP.

Our Recommendation

If your access point or clients are only capable of using WEP, it's time for you to look at upgrading your technology, for the sake of increased security – not to mention increased throughput speeds on newer devices.

Right now, the best security for your WiFi network is **WPA2 with WPS disabled** . Using this security combination provides the most secure WiFi network possible today, and gives you the peace of mind you need to "set it and forget it."

Besides, do you really want to trust a single button to provide all the security for your network? If WPA2 with WPS disabled ever becomes vulnerable, we'll be sure and keep you updated on the adjustments you should make to remain secure.

Next Lesson...
Designing a Dual-Band WiFi Network (design-dual-band-wifi.html)

PRODUCTS

Wi-Spy Air (/products/wi-spy-air/)

MetaGeek Complete (/products/complete/)

Chanalyzer + Wi-Spy (/products/wi-spy/)

Eye P.A. (/products/eye-pa/)

TamoGraph Site Survey (/products/map-plan/tamograph)

inSSIDer & MetaGeek Plus (//metageek.link/inssider-product-page)

SALES

Product Comparison (/products/)

Contact Sales (/store/contact/)

Request a Quote (/store/quote/)

Find a Reseller (/store/resellers/)

Product Catalog (/store/catalog/)

Partner Login (//store.metageek.com/myaccount.asp)

SUPPORT

Downloads (/support/downloads/)

MetaGeek Community (//community.metageek.com)

Knowledge Base (http://support.metageek.com)

WiFi Education (/training/)

My.MetaGeek Login (//my.metageek.com/login)

Working from Home (/work-from-home-wifi)

METAGEEK

Contact (/company/contact/)

About (/company/about/)

Careers (/company/jobs/)

Our WiFi Partners (/partner/)

Legal Stuff (/legal)

Blog (//blogs.metageek.net)

(http://www.facebook.com/pages/MetaGeek/322588047766226)