The 8th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT
IN THE 21st CENTURY"
Braşov, November 14th 2013

Wi-Fi PROTECTED SETUP – SECURITY ENHANCEMENT OR THREAT?

Daniel SORA eng. PhD

National Defense University of Romania "Carol I"/ The Regional Department of Defense Resources Management Studies / Brasov / Romania

Abstract:

Even if you've encrypted and secured your wireless network with Wi-Fi Protected Access (WPA or WPA2), a security hole affecting most wireless routers may make it fairly easy for those with the right tools to hack your network and connect. They could then steal the wireless Internet access, possibly connect to your computers, and snoop on your network traffic to perhaps capture your passwords and hijack your online accounts. This security hole comes from the Wi-Fi Protected Setup (WPS) feature designed by the Wi-Fi Alliance to – ironically – make securing and connecting Wi-Fi devices easier and has been included on the majority of wireless routers made since 2007.

Key words: WPS, wireless, security, threat, network, router.

1.Introduction

"Wi-Fi Protected Setup" (WPS; originally Wi-Fi Simple Config) is an optional certification program from the Wi-Fi Alliance that is designed to ease the task of setting up and configuring security on wireless local area networks. Introduced by the Wi-Fi Alliance in early 2007, the program provides an industry-wide set of network setup solutions for homes and small office (SOHO) environments. The goal of the WPS protocol is to allow home users who know little of wireless security and may be intimidated by the available security options to set up Wi-Fi Protected Access, as well as making it easy to add new devices to an existing network without entering long passphrases. Prior to the standard, several competing solutions were developed by different vendors to address the same need.

The Wi-Fi Simple Configuration Specification (WSC) is the underlying technology for the Wi-Fi Protected Setup certification. Almost all major vendors (including Cisco/Linksys, Netgear, D-Link, Belkin, Buffalo, ZyXEL and Technicolor) have WPS-certified devices, other vendors (eg. TP-Link) sell devices with WPS-support which are not WPS-certified.

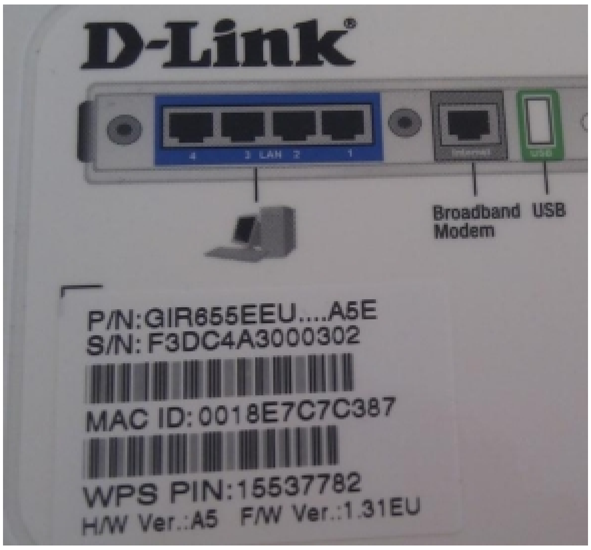
Although WPS is marketed as being a secure way of configuring a wireless device, there are design and implementation flaws which enable an attacker to gain access to an otherwise sufficiently secured wireless network. WPS has been shown to easily fall to brute-force attacks. A major security flaw was revealed in December 2011 that affects wireless routers with the WPS feature, which most recent models have enabled by default. The flaw allows a remote attacker to recover the WPS PIN in a few hours and, with it, the network's WPA/WPA2 pre-shared key. Users have been urged to turn off the WPS feature, although this may not be possible on some router models.

Terminology:

- The ***enrollee*** is a new device that does not have the settings for the wireless network.
- The ***registrar*** provides wireless settings to the enrollee.
- The ***access point*** (AP) provides normal wireless network hosting and also proxies messages between the enrollee and the registrar.

2. The Wi-Fi Protected Setup Security Hole

Wireless vendors have a few ways to implement WPS, but the PIN method is the only one required, and is the source of the security hole. The way the PIN information is exchanged between the router and clients makes it much easier to brute-force the PIN, repeatedly sending guesses to the router from a client using a tool like Reaver or WPScrack. After a few hours, these tools will likely reveal the target router's WPS PIN and the WPA or WPA2 passphrase, both of which can be used to connect to the network.

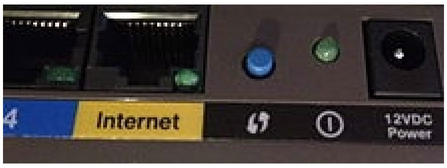


Label with WPS PIN on the back of a D-Link router

The standard emphasizes usability and security, and allows up to four usage modes aimed at a home network user adding a new device to the network:

1. PIN Method, in which a personal identification number (PIN) has to be read from either a sticker or the display on the new wireless device. This PIN must then be entered at the "representant" of the network, usually the access point of the network. Alternately, a PIN on the Access Point may be entered into the new device. The PIN Method is the mandatory baseline mode; every Wi-Fi Protected Setup certified product must support it.
2. Push-Button-Method, in which the user simply has to push a button, either an actual or virtual one, on both the access point and the new wireless client device. Support of this mode is mandatory for access points and optional for connecting devices.
3. Near-Field-Communication Method, in which the user simply has to bring the new client close to the access point to allow a near field communication between the devices. NFC Forum compliant RFID tags can also be used. Support of this mode is optional.

4. USB Method, in which the user uses a USB flash drive to transfer data between the new client device and the access point of the network. Support of this mode is optional, but deprecated.



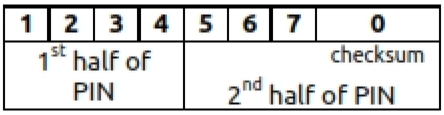
The WPS push button (center, blue) on a wireless router

The last two modes are usually referred as out-of-band methods as there is a transfer of information by a channel other than the Wi-Fi channel itself. Only the first two modes are currently covered by the Wi-Fi Protected Setup certification. The USB method has been deprecated and is not part of the Alliance's certification testing.

In December 2011, researcher Stefan Viehböck[1] reported a design and implementation flaw that makes brute-force attacks against PIN-based WPS feasible to perform on WPS-enabled Wi-Fi networks. A successful attack on WPS allows unauthorized parties to gain access to the network. The only effective workaround is to disable WPS.

The vulnerability centers around the acknowledgement messages sent between the registrar and enrollee when attempting to validate a PIN. The PIN is an eight digit number used to add new WPA enrollees to the network. Since the last digit is a checksum of the previous digits, there are seven unknown digits in each PIN, yielding 10^7 = 10,000,000 possible combinations.

When an enrollee attempts to gain access using a PIN, the registrar reports the validity of the first and second halves of the PIN separately. Since the first half of the pin consists of four digits (10,000 possibilities) and the second half has only three active digits (1000 possibilities), at most 11,000 guesses are needed before the PIN is recovered. This is a reduction by three orders of magnitude from the number of PINs that would have to be tested.



1	2	3	4	5	6	7	0
1st half of PIN				2nd half of PIN			checksum

An attacker can derive information about the correctness of parts the PIN from the AP´s responses.

- If the attacker receives an EAP-NACK message after sending M4, he knows that the 1st half of the PIN was incorrect.
- If the attacker receives an EAP-NACK message after sending M6, he knows that the 2nd half of the PIN was incorrect.

This form of authentication dramatically decreases the maximum possible authentication attempts needed from 10^8 (=100.000.000) to 10^4+ 10^4 (=20.000).

As the 8th digit of the PIN is always a checksum of digit one to digit seven, there are at most $10^4 + 10^3$ (=11.000) attempts needed to find the correct PIN.

As a result, an attack can be completed in less than four hours. The ease or difficulty of exploiting this flaw is implementation dependent, as Wi-Fi router manufacturers could defend against such attacks by slowing or disabling the WPS feature after several failed PIN validation attempts.

[1] http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

In some devices, disabling WPS in the user interface does not result in the feature actually being disabled. The device remains vulnerable to attack. Firmware updates have been released for some of these devices so that WPS can be disabled completely.

3. Protecting your network from the WPS security hole

Since the vulnerability lies in the implementation of WPS, your network should be safe if you can simply turn off WPS (or, even better, if your router doesn't support it in the first place). Unfortunately, even with WPS manually turned off through his router's settings, Reaver was still able to crack his password. The inability to shut this vulnerability down is widespread. We have found it to occur with every Linksys and Cisco Valet wireless access point. On all of the Linksys routers, you cannot manually disable WPS. While the Web interface has a radio button that allegedly turns off WPS configuration, it's still on and still vulnerable.

Wireless vendors and/or the Wi-Fi Alliance may help patch this security hole by implementing additional security measures, such as limiting the amount and frequency of PIN guesses. They could possibly fix the issue in new models and in existing models by releasing firmware updates that you may even be able to use with your current router. If they don't make any enhancements, the only way to patch the security hole is to turn WPS off, but even then some routers still might be vulnerable as they may still response to PIN queries.

To see if your router supports WPS—whether or not you should be worried about this security hole—first check if there's an 8-digit PIN number printed on the bottom of your router. Also see if there are any WPS logos on it or on the box it came in. But even if you don't see any evidence, you should still double-check your router's settings for any mention of WPS.

To check or change your router's settings, log on to the web-based interface by typing the router's IP address into a web browser on a computer that's connected to your network. If you don't remember the password to log on, try the default, which can be found in the router's documentation or online. Once logged on, look for WPS settings, perhaps in the wireless or advanced settings.

If you find you have WPS, you can usually disable via the router settings. But again, it may not actually stop people from taking advantage of the security hole.

Before giving up on your router, check the wireless vendor's website and look for any firmware updates for your particular router that were released in January 2012 or after. Then look at the release notes for any mention of a WPS fix or update. If you see one, then you can simply download the firmware file and upload it to your router via the settings interface in your web browser. Otherwise, you might consider checking to see if your router is supported by after-market firmware, like DD-WRT or Tomato, which don't support or include WPS.

As a last resort for full peace of mind, if your router doesn't have firmware updates and can't go the after-market route, you may consider buying a different router model that doesn't come with WPS.

DD-WRT is a Linux based alternative OpenSource firmware suitable for a great variety of WLAN routers and embedded systems. The main emphasis lies on providing the easiest possible handling while at the same time supporting a great number of functionalities within the framework of the respective hardware platform used.

DD-WRT does not support WPS, so there's yet another reason to love the free firmware.

If the router is for business use, consider using the Enterprise (802.1X) mode of WPA2 instead of the personal or PSK mode. When using the enterprise mode, the WPS vulnerability doesn't apply even if you have WPS on your router. This is because WPS only works with the personal mode, and if you don't have it enabled there isn't anything to worry about.

The Enterprise mode, however, is much more complex to set up. It uses 802.1X authentication, which requires a RADIUS server. If you have a domain network, you can use the Internet Authenticate Service (IAS) feature of Windows Server 2000 or 2003 or the Network Policy Server (NPS) feature of Windows Server 2008 or later. If you don't have a Windows Server, consider the free open source FreeRADIUS server. But if you don't want to run your own server, consider APs with built-in RADIUS servers or cloud services that can host the server for you.

Conclusion

As nearly all major router/AP vendors have WPS-certified devices and WPS – PIN (External Registrar) is mandatory for certification, it is expected that a lot of devices are vulnerable to this kind of attack.

Having a sufficiently long lock-down period is most likely not a requirement for certification. However it might be a requirement in the WSC Specification Version 2.

Collaboration with vendors will be necessary for identifying all vulnerable devices. It is up to the vendors to implement mitigations and release new firmware.

Affected end-users will have to be informed about this vulnerability and advised to disable WPS or update their firmware to a more secure version (if available).

References:

[1] http://www.wi-fi.org/knowledge-center/articles/wi-fi-protected-setup%25E2%2584%25A2-0

[2] http://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup

[3] http://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

[4] WPS Flaw Vulnerable Devices list at https://docs.google.com/spreadsheet/ccc?key=0Ags-JmeLMFP2dFp2dkhJZGIxTTFkdFpEUDNSSHZEN3c#gid=0

[5] Default Password List at http://www.phenoelit.org/dpl/dpl.html

[6] http://arstechnica.com/business/2011/12/researchers-publish-open-source-tool-for-hacking-wifi-protected-setup/

[7] http://dd-wrt.com/site/index

[8] https://rstforums.com/forum/75480-how-crack-wi-fi-networks-wpa-password-reaver.rst

[9] https://rstforums.com/forum/73951-wifi-hacking-wpa-2-psk-traffic-decryption.rst

[10] https://rstforums.com/forum/74283-video-hacking-wpa-2-key-evil-twin-method-no-bruteforce.rst

[11] http://www.scribd.com/doc/126108319/Vulnerabilitati-WLAN-WEP-WPA-WPA2

[12] http://www.us-cert.gov/ncas/alerts/ta12-006a

[13] http://www.kb.cert.org/vuls/id/723755

[14] http://www.ciscopress.com/articles/article.asp?p=1847302