1-1-2012

A Proposed Method for Examining Wireless Device Vulnerability to Brute Force Attacks via WPS External Registrar PIN Authentication Design Vulnerability

Symon Aked

Christopher Bolan
Edith Cowan University

Murray Brand
Edith Cowan University

A Proposed Method for Examining Wireless Device Vulnerability to Brute Force Attacks via WPS External Registrar PIN Authentication Design Vulnerability

S. Aked[1], C. Bolan[1,2] and M. Brand[1,2]
[1]School of Computer and Security Science, Edith Cowan University, Perth Western Australia
[2]secau – Security Research Centre, Perth Western Australia

Abstract *- Wi-Fi Protected Setup (WPS) is a certification scheme introduced in 2007 to ensure that wireless SOHO (Small Office, Home Office) and home networks could be connected to in a trusted, yet user friendly manner. Recently, WPS was shown to have a design and implementation flaw which makes the feature highly susceptible to attack. Although open-source tools have been written and released, no formal testing methodology has been developed. This research presents a proposed method for the testing of this vulnerability in a measured and systematic way.*

Keywords: Wireless LAN, Computer Security, Data Security

1 Introduction

Access to Local Area Networks (LAN) have traditionally been restricted to wired connections via coaxial cable, CAT 3, 4, 5 or 6 cables, and Unshielded Twisted Pair (UTP). However, in 1997 the Institute of Electrical and Electronics Engineers (IEEE) helped establish the 802.11 set of standards by which communications could be facilitated wirelessly [1]. Alongside the evolution of these standards came an increase in the adoption of this technology in both both consumer and enterprise grade wireless communication devices. Today, mobility has become a significant component of the high consumers demand for electronic devices such as mobile phones, notebook computers and tablets. Worldwide shipment of Wi-Fi integrated circuits increased 28% between 2008 and 2009, with wireless integrated circuits in mobile handsets alone increasing by 50% in 2009 [2]. Instat predict that more than a billion Wi-Fi chipsets will be shipped in 2012 alone, with Wi-Fi chipsets for mobile phones and notebook computers to exceed one billion dollars in 2015 [3].

Alongside this surge in usage has come an increased awareness of security and its associated issues. In an effort to ensure the security of the technology when used in consumer devices the Wi-Fi Alliance drafted the Wi-Fi Protected Setup (WPS) specification and certification in 2007 [4]. Three methods of using WPS were created:

1. Push Button Configuration Method - A physical or virtual button is pushed on both the wireless client that wants to join the network, and the wireless router or access point that will be the gateway into the network.

2. Personal Identification Number (Internal Registrar) - The PIN of the wireless client that wants to join the network is entered into a web interface of the wireless gateway. The PIN can be written on the wireless device, or may be generated in software.

3. Personal Identification Number (External Registrar) - The PIN of the wireless gateway that allows access to the wireless network is entered into an interface of the wireless client.

The PIN (External Registrar) method of authentication was found to be vulnerable to a brute force attack in late 2011 [5]. This vulnerability allows for an attacker to gain unauthorized access to a wireless network within a matter of minutes to days, no matter how strong the Wi-Fi Protected Access (WPA) passphrase is.

2 Background

2.1 Significance

The aim of this research was is produce a rigorous and comprehensive methodology and procedure that will allow for a wireless device to be tested for its susceptibility to the WPS external registrar PIN authentication design vulnerability. Currently there is no formal testing methodology that may be applied to a wireless device that will give a comprehensive and detailed view of its susceptibility to the vulnerability.

Once in place the method will allow for the systemized testing and evaluation of wireless consumer devices. To date only sporadic data from unnamed sources has been available. Whilst such data of an unknown nature claims to prove vulnerability for a given device, the methodology used is not disclosed or document. Therefore, the method proposed in this work may be used to verify such results ensuring both consistency and reliability in the gathered data.

The information obtained by this research may be useful to owners of wireless devices as a credible and reliable guide to the vulnerability of their devices. It may also be used to expose manufacturers that have yet to patch the vulnerability in their products. This is of particular concern due to the rise of wireless related attacks becoming a feature in modern criminal enterprise [6].

2.2 WPS & Vulnerability

Wi-Fi Protected Setup (WPS) is an optional certification from the Wi-Fi Alliance, a non-profit organization that promotes the adoption of 802.11 wireless devices. It has almost 500 members and has certified well over 9,000 products. The standard was introduced in 2007, and currently has over 2,000 certified devices [7]. The standard purports to allow for the setup of wireless devices to be easier for the average consumer, providing for wireless access without the need for a complex passphrase exchange.

Although WPS was an optional certification, the more recent Wi-Fi Direct certification (has a mandatory requirement that WPS be included in any device that is to be certified [8]. Wi-Fi Direct is designed to allow devices to talk directly to each other, to replace situations where cables are traditionally used. This requirement means that any device that bears the Wi-Fi Direct logo will have WPS capabilities, and will likely have WPS enabled by default.

However, in 2011 a detailed a flaw in the design and implementation of WPS was discovered [5]. The flaw allows for the brute force of the WPS PINs used in Wi-Fi Alliance certified devices. The approach is based on flaws within authentication when using a PIN via an external registrar, and the timing of EAP-NACK messages that reduce the searchable key space of the attack from 108 to 104+104. This keys pace is further reduced as the 8th digit of the PIN is a checksum of the previous seven numbers. Thus, the effective key space is actually only 104+103.

Whilst initially claimed that the WPS vulnerability appears to be widespread a limited number of devices were included in testing [5]. Thus, whilst it is suspected that a significant amount of devices would include this vulnerability, it is difficult to ascertain from current literature the true scope of the problem. As many devices may allow for the disabling of the feature it has yet to be conclusively determined if this approach represents a true solution to the issue. Therefore the method proposed in this work would allow for a true quantification of the issue and the subsequent questions that arise.

2.3 Reported Mitigations

As mitigation, some claim that WPS is a secure channel by which to authenticate wireless devices with active brute force protection [9]. Although briefly mentioned, it is stated that the registrar will warn a user, and will not automatically reuse the PIN if a PIN authentication or communication error occur. Whilst it appears that some manufacturers have implemented a delay when an incorrect PIN is used, the length of this timeout is manufacturer and perhaps device or firmware specific.

Microsoft's implementation of WPS in their operating systems released after Windows XP is Windows Connect Now-NET [10]. The feature allows for the same in-band PIN authentication scheme that has been found to be vulnerable to a brute force attack. Microsoft's specification is very detailed and shows the steps that are taken by both the Enrolee and Registrar to authenticate via a PIN. Microsoft note that the "AP Setup Locked" attribute may be set at the access point, and that "The access point should enter this state if it believes a brute force attack is underway against the access point's PIN" [10]. It is further stated, "…the use of the access point's PIN for adding external registrars is disabled in this state" [10]. However, the strength of the implementation and the extent to which supposedly compliant manufacturers implement this timeout, and the duration of the timeout have yet to be investigated. Again a standardized approach would be integral to any research on this subject.

As with most known vulnerabilities, a United States Computer Emergency Readiness Team (US-CERT) Vulnerability Note was created when information of the vulnerability was disclosed [11]. Such alerts are accompanied by a recommendation to disable WPS as a workaround, however as mentioned previously, this may not guarantee the cessation of the attack vector. A second online vulnerability database entry was created with the reference CVE-2011-5053 [12][13]. No workarounds or recommendations are provided.

Recently, an effort to crowd source the detection of the vulnerability across devices and firmware versions has arisen online [14]. The list is fairly comprehensive, with 133 entries covering most router and wireless access point vendors. However, whilst the information is presented in a coherent and uniform way, the accuracy of the data cannot be verified. It must be noted that the information does seem to support the theory that the WPS PIN vulnerability is widespread.

Since the discovery of the WPS PIN vulnerability a number of open source tools have surfaced that allow for testing and exploitation such as Reaver and WPSCrack [15][16]. Thus in conjunction with these tools a standardized approach to testing the vulnerability would allow both individual and systematic audit of all devices giving clear quantification of the problem as well as certifiable testing of mitigation approaches. It is therefore proposed that once established, the methodology described in this research will be utilized to audit and report on the security of popular Wi-Fi devices.

3 Proposed Method

As wireless devices that are to be audited may either be delivered to the customers with any version of publicly (and privately) available firmware, it is important that as many versions as possible are tested. It is not enough to assume that if the vulnerability that is to be tested is patched in one version, that all subsequent versions will also not be vulnerable.

Flashing the device to its factory default is an important step, as it is in this state that the initial customer will receive it. It also negates the chances that, if the device was not purchased new, the previous owner changed settings that would affect the results of an audit. Testing devices with both WPS enabled and disabled will ensure that the device manufacturer has not made an error, and that disabling the WPS feature in

the configuration truly does disable the feature. This is important as it is logical for a consumer to assume they are not vulnerable if the vulnerable service is not seemingly enabled.

The wash tool was designed to identify wireless devices that have WPS enabled. Proving the effectiveness of this tool in identifying devices that have WPS enabled may help reduce time spent running Reaver against devices that do not have WPS enabled [15]. Reaver has been in development for over a year, and was publicly released in December 2011. The tool is designed to audit wireless devices for the WPS brute force vulnerability. Reaver may either fail to probe a device (either due to the device not having WPS enabled or having other protection mechanisms enabled), succeed but be rate limited (due to the device implementing brute force protection mechanisms), or succeed with little to no impedance.

The proposed method is illustrated below. The method proposes a systematic approach to the testing of any Wi-Fi device allowing for consistency and repeatability. It is envisaged that the implementation of this method will produce a significant volume of reputable data on the WPS vulnerability issue. To this, a study is now underway to verify and utilize the approach against a body of commercial devices.

4 Conclusion

The WPS external registrar PIN authentication design vulnerability is a dangerous security hole for home and SOHO users of wireless devices. The public has been lead to believe that as long as their WPA/WPA2 passphrase is complicated enough, then their networks are safe from unauthorized access. Clearly this is no longer the case, but the scale of the vulnerability has yet to be fully examined.

The development of a reliable WPS external registrar PIN authentication design vulnerability testing methodology will allow for a standardized way to test for weak implementations of WPS by device manufacturers. It will allow for current and future devices to be tested, with reliable results generated from an audit.

The results found from applying the developed auditing methodology to wireless devices will not only allow for the detailed examination of data, but will allow members of the public to easily and reliably ensure the security of their own devices.

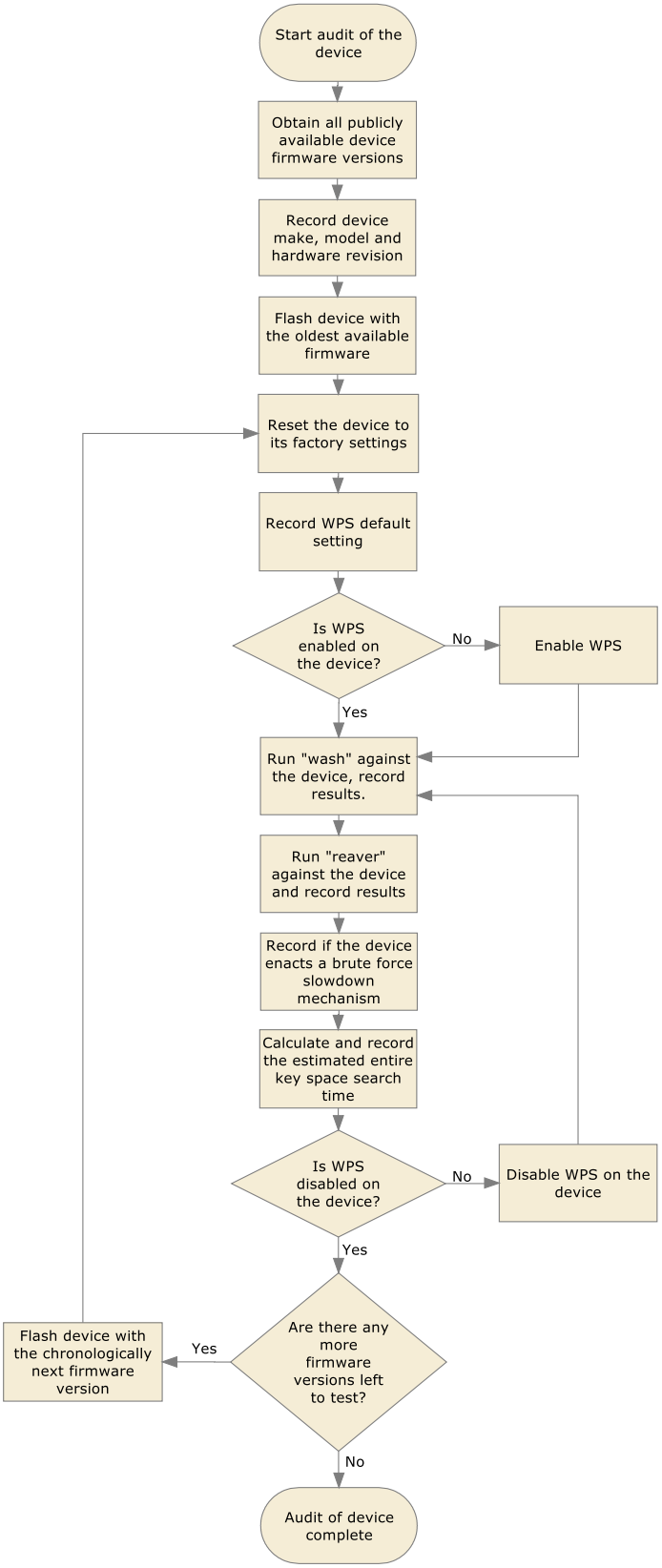

Figure 1 – The Proposed Testing Methodology

5 References

[1] The Economist. (2004). *A brief history of Wi-Fi*. [Online]. Viewed 2012 April 01. Available: http://www.economist.com/node/2724397

[2] Electronics News. (2010, January). *Wi-Fi IC shipments up 28 per cent*. [Online]. Viewed 2012 April 01. Available: http://www.electronicsnews.com.au/news/wi-fi-ic-shipments-up-28-per-cent

[3] J. Happich. (2010, September). *WiFi chipets to pass a billion units per year by 2012*. [Online]. Viewed 2012 April 01. Available: http://www.microwave-eetimes.com/en/wifi-chipsets-to-pass-a-billion-units-per-year-by-2012.html?cmp_id=7&news_id=222901091

[4] Wi-Fi Alliance. (2010, December). *Wi-Fi CERTIFIED Wi-Fi Protected Setup*. [Online]. Viewed 2012 April 01. Available: https://www.wi-fi.org/register.php?file=wp_20101216_Wi-Fi_Protected_Setup.pdf

[5] S. Viehböck. (2011, December). *Brute forcing Wi-Fi Protected Setup*. [Online]. Viewed 2012 March 25. Available: https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

[6] myPolice QPS News. (2012, March). *War Driving Project to help prevent identity theft*. [Online]. Viewed 2012 April 01. Available: http://qpsmedia.govspace.gov.au/2012/03/22/war-driving-project-to-help-prevent-identity-theft/

[7] Wi-Fi Alliance. (2011, April). *Wi-Fi Alliance Member Symposium*. [Online]. Viewed 2012 March 25. Available: http://www.wi-fi.org/files/20110421_China_Symposia_full_merge.pdf

[8] Wi-Fi Alliance. (2010, October). *Wi-Fi CERTIFIED Wi-Fi Direct*. [Online]. Viewed 2012 March 25. Available: http://www.cnetworksolution.com/uploads/wp_Wi-Fi_Direct_20101025_Industry.pdf

[9] N. Turab & F. Moldoveanu. (2009). A Comparison Between Wireless LAN Security Protocols. *Universitatea Politehnica Bucuresti Scientific Bulletin*. [Online]. 71 (1), pp 61-80. Available: http://www.scientificbulletin.upb.ro/rev_docs/arhiva/full7970.pdf

[10] Microsoft. (2006, December). *Windows Connect Now–NET*. [Online]. Viewed 2012 March 25. Available: http://download.microsoft.com/download/a/f/7/af7777e5-7dcd-4800-8a0a-b18336565f5b/WCNNetspec.doc

[11] J. Allar. (2011, December). *Vulnerability Note VU#723755*. [Online]. Viewed 2012 March 25. Available: http://www.kb.cert.org/vuls/id/723755

[12] Common Vulnerability and Exposures. (2012, January). *CVE-2011-5053*. [Online]. Viewed 2012 March 25. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-5053

[13] National Vulnerability Database. (2012, January). *Vulnerability Summary for CVE-2011-5053*. [Online]. Viewed 2012 March 25. Available: http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-5053

[14] Jagermo. (2012). *WPS Flaw Vulnerable Devices*. [Online]. Viewed 2012 March 25. Available: https://docs.google.com/spreadsheet/lv?key=0Ags-JmeLMFP2dFp2dkhJZGIxTTFkdFpEUDNSSHZEN3c

[15] C. Heffner & P. Eacmen. (2012). *reaver-wps*. [Online]. Viewed 2012 March 25. Available: https://code.google.com/p/reaver-wps/

[16] S. Viehböck. (2011). *WPScrack*. [Online]. Viewed 2012 March 25. Available: http://dl.dropbox.com/u/22108808/wpscrack.zip

[17] C. Heffner. (2012, January). *README.WASH*. [Online]. Viewed 2012 March 25. Available: https://code.google.com/p/reaver-wps/source/browse/trunk/docs/README.WASH