12-3-2012

An Investigation into the Wi-Fi Protected Setup PIN of the Linksys WRT160N v2

Symon Aked
Edith Cowan University

Christopher Bolan
Edith Cowan University

Murray Brand
Edith Cowan University

DOI: 10.4225/75/57b5554fcd8d5
10th Australian Information Security Management Conference, Novotel Langley Hotel, Perth, Western Australia, 3rd-5th December, 2012

AN INVESTIGATION INTO THE WI-FI PROTECTED SETUP PIN OF THE LINKSYS WRT160N V2

Symon Aked[1], Christopher Bolan[2, 1], Murray Brand[3,1,2]
[1]School of Computer and Security Science, Edith Cowan University, Perth, Western Australia
[2]SRI - Security Research Institute, Edith Cowan University, Perth Western Australia
[1]secau.2012@tanstaafl.com.au, [2]c.bolan@ecu.edu.au, [3]m.brand@ecu.edu.au

Abstract
Wi-Fi Protected Setup (WPS) is a method of allowing a consumer to set up a secure wireless network in a user friendly way. However, in December 2011 it was discovered that a brute force attack exists that reduces the WPS key space from 108 to 104+103. This resulted in a proof of concept tool that was able to search all possible combinations of PINs within a few days.This research presents a methodology to test wireless devices to determine their susceptibility to the external registrar PIN authentication design vulnerability. A number of devices were audited, and the Linksys WRT160N v2 router was selected to be examined in detail. The results demonstrate that the router is highly susceptible to having its WPN PIN brute forced. It also details that even with WPS disabled in the router configuration, WPS was still active and the PIN was equally vulnerable.

Keywords
Wi-Fi protected setup, WPS, wireless security, brute force.

INTRODUCTION

Wi-Fi Protected Setup (WPS) is a standard created in 2007 by the Wi-Fi Alliance, a non-profit organisation that promotes the adoption of 802.11 wireless devices ("Wi-Fi Protected Setup™," 2012) WPS can be implemented in wireless devices by one of four methods ("Frequently Asked Questions: Wi-Fi Protected Setup™," 2006):

- PIN - The WPS PIN is usually either printed on the device, or is displayed inside the router configuration webpage. Either the new or existing device's PIN can be entered into the device that will be connecting directly to it.
- PBC (Push Button Connect) - A button, either physical or virtual, in pressed on both the new wireless device, and the existing wireless access point or router.
- NFC (Near Field Communication) - The new wireless device is brought within NFC communications range of the wireless network device. The WPS PIN is then exchanged between the two devices.
- USB - A flash based USB drive is used to copy WPS connectivity data from the new device to the destination wireless device.

The incorporation of WPS in wireless devices is to allow for easier configuration of wireless devices on a network, when compared to previous methods such as manually exchanging WEP, WPA or WPA passphrases. However, Viehböck (2011a) detailed a flaw in the design and implementation of WPS. This flaw allows for the brute force of the PIN method of connecting a device to the WPS enabled wireless network. According to Viehböck, the brute force is feasible due to the lack of 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 10^8 to 10^4+10^4. Further, as the eighth digit of the PIN is a checksum of the previous seven numbers, the key space to be searched is reduced to 10^4+10^3, adding to the efficacy of attacks.

Viehböck (2011a) reports that the WPS vulnerability appears to be widespread. However, he tested only one device from each of four vendors, with only one version of firmware per device. This does not give a comprehensive view of just how widespread the WPS security issue is. It also fails to detail what effect (if any) disabling WPS would have on the vulnerability i.e. does it negate the attack vector? The development of a testing methodology, which is then used as the basis of a comprehensive audit of wireless devices available on the Australian market, would therefore give a much better understanding of how widespread this issue is.

The Wi-Fi Alliance ("Annual Report 2011," 2011) has nearly 500 member companies, and runs a number of optional product certification schemes. By the end of 2011, it has certified more than 12,000 products ("Annual Report 2011," 2011), of which over 2,400 have been WPS certified ("Wi-Fi Alliance Member Symposium.," 2011) . Although WPS certification is optional, the more recent Wi-Fi Direct certification ("Wi-Fi CERTIFIED

Wi-Fi Direct.," 2010) has a mandatory requirement that WPS be included in every device that is to be certified. Wi-Fi Direct is designed to allow devices to talk directly to each other, to replace situations where cables have traditionally been used. This requirement means that any device that bears the Wi-Fi Direct logo will have WPS capabilities, and thus will likely have WPS enabled by default. Wi-Fi Direct is designed to allow for simple connectivity of new devices into wireless networks, but the Wi-Fi Alliance Wi-Fi Direct white paper ("Wi-Fi CERTIFIED Wi-Fi Direct.," 2010) does not highlight the external registrar PIN authentication design vulnerability. Whether or not a device is Wi-Fi Direct certified was thus selected to be one of the attributes recorded in the wireless device audit, conducted as part of this research.

It has been noted by Turab and Moldovenau (2009) that WPS is a secure channel by which to authenticate wireless devices with active brute force protection. Although briefly mentioned, it is stated that the registrar will warn a user, and will not automatically reuse the PIN, should a PIN authentication or communication error occur. However, it appears that although some device manufacturers may implement a delay when an incorrect PIN is used, the length of this timeout is manufacturer and perhaps device or firmware specific. These uncertainties led to the inclusion of this parameter in the research.

Microsoft's implementation of WPS in their operating systems released after Windows XP is Windows Connect Now-NET ("Windows Connect Now–NET.," 2006). It 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 ("Windows Connect Now–NET.," 2006) 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*.". It is further stated that "*…the use of the access point's PIN for adding external registrars is disabled in this state*". Again, this led to the inclusion of these factors within the research.

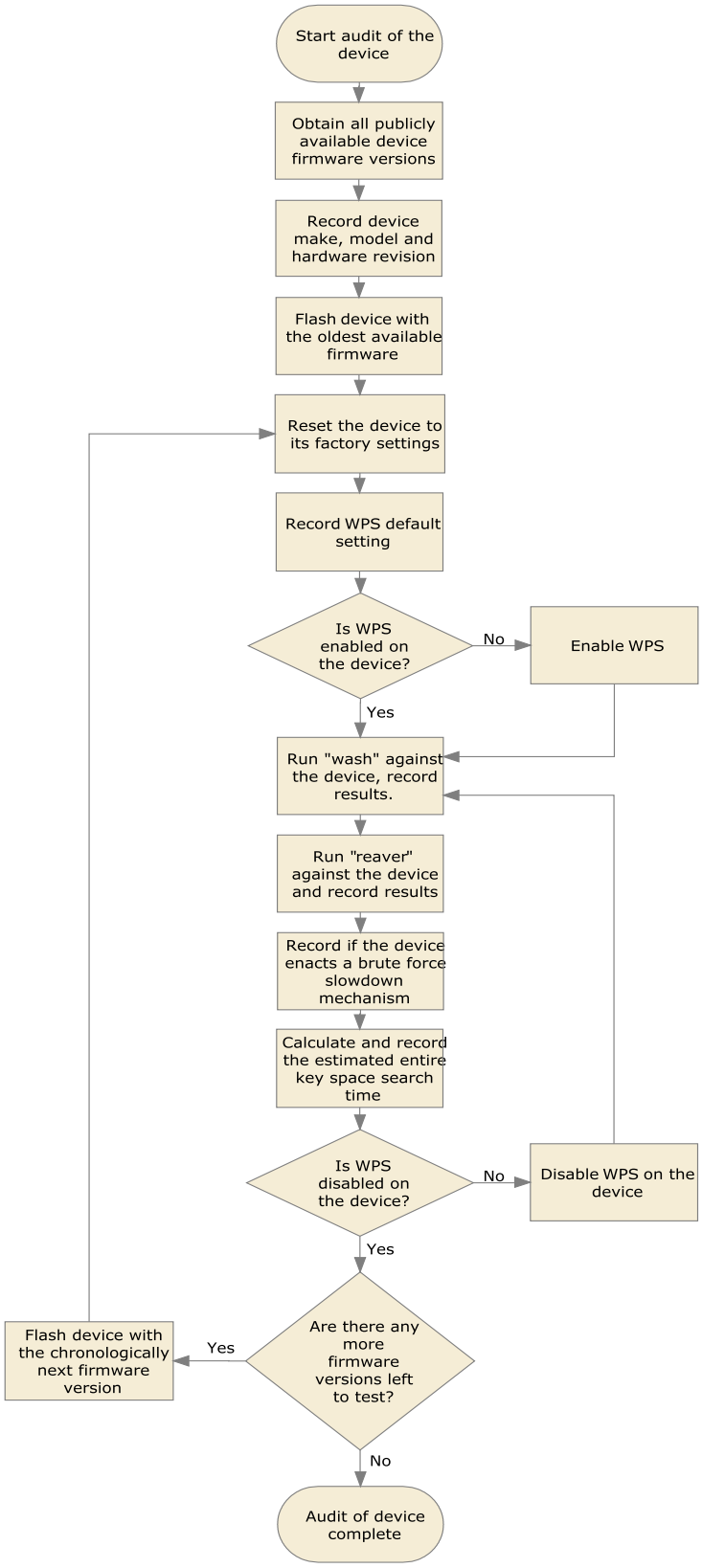
A United States Computer Emergency Readiness Team (US-CERT) vulnerability note was created when information of the vulnerability was disclosed. VU#723755 gives an overview of the vulnerability and shows that a number of vendors have devices that are confirmed to be vulnerable (Allar, 2011). US-CERT recommends disabling WPS as a workaround, but do not note that this does not guarantee that this will close the attack vector (Allar, 2011). A brief Common Vulnerabilities and Exposures entry ("CVE-2011-5053.," 2011), which is also covered at the National Vulnerability Database website ("Vulnerability Summary for CVE-2011-5053.," 2012), gives links to details of the vulnerability.

A Google Drive online spreadsheet (Jagermo, 2012) was created to crowd source a list of WPS PIN brute force vulnerable devices and firmware versions. The list is fairly comprehensive, with 141 entries covering many router and wireless access point vendors. Although the information is presented in a coherent way, there is little uniformity of the data, and the accuracy of the data has not been verified. The information contained in the spreadsheet supports the theory that the WPS PIN vulnerability is widespread. It could also be interpreted to show that a refined testing methodology, along with a controlled series of tests and logging of data, would be of value to the Information Security community, and to wireless device owners eager to discover if their devices are vulnerable.

As the WPS external registrar PIN authentication design vulnerability has only recently been discovered, the amount of literature on the subject is minimal. Papers published prior to December 2011 note that WPS is a secure method of easing the burden of securely connecting to a wireless network. After the discovery of the WPS PIN vulnerability, and especially after the publication of open source tools such as reaver (Heffner & Eacmen, 2012) and WPScrack (Viehböck, 2011b), the potential impact of the issue is very apparent.

The design of a WPS vulnerability testing methodology was developed and published in prior research (Aked, Bolan, & Brand, 2012). It contains an overview of how the auditing process could be implemented, as well detailing why certain tools and procedures were chosen. This methodology is used to audit the Linksys WRT160N v2 router.

METHOD



The method can be broken down into 5 distinct phases:

1) Gather all publically available wireless device firmware versions. To see if any changes to WPS behaviour or settings were made between firmware revisions, all available firmware versions need to be

obtained. This is usually accomplished by downloading firmware directly from the wireless device manufacturer's website, but can also be obtained at third party websites. A device manufacturer may change the version of firmware that is shipped with the device at any time, and as there is no guarantee that a user will upgrade the firmware, testing all releases also ensures that as many standard installations as possible are tested.

2) Record details of the wireless device. This step ensures that all relevant details of the device are documented for future use. Some details, such as the hardware revision of the device may be situated on the underside of the hardware, or in the web configuration interface, and is manufacturer dependant.
3) Record the WPS default setting. Whether or not a manufacturer decides to enable WPS by default is at their discretion, but should the device be vulnerable to PIN brute forcing, this step is important to gauge as to whether a device with standard factory settings is vulnerable.
4) Run wash against the device. Wash will show all routers in wireless reception range that it believes to be running a WPS daemon. If wash is proven to be accurate, this may allow for future rapid surveys of a large number of devices that may be vulnerable to the WPS attack.
5) Run reaver against the device. Reaver is the primary tool used in this audit to see whether or not the device is vulnerable to having its PIN brute forced. Reaver only requires the MAC address and wireless channel that the wireless device listens on for it to start working on the PIN. The number of PINs reaver is attempting per second is displayed, as well as any measures it has detected that are slowing down its ability to test PINs. Should the listening WPS daemon crash or otherwise stop accepting PINs from reaver, an error will be displayed.

Once either reaver has obtained the WPS PIN, a pattern has been established in regards to the listening WPS daemon (either lack of stability or brute force mitigation actions enabled), or a WPS connection cannot be established, the audit of that firmware version is deemed to have been completed. The router is then loaded with the chronologically next firmware version, reset to factory settings (which generally also reboots the device), and the process repeated until no more firmware versions are left to test.

TESTING THE LINKSYS WRT160N V2 ROUTER

The Linksys WRT160N v2 - a wireless router utilising the Ralink RT2880F chipset ("Linksys Support," 2012) - was certified for WPS (PIN and PBC) by the Wi-Fi Alliance in May 2008 ("Wi-Fi Certified Interoperability Certificate," 2008) with a certification ID of WFA6231. A detailed overview of the process, as well as results found utilising the aforementioned method, follows.

Obtain all publically available device firmware versions.

According to Cisco's online support personnel, it is Cisco's policy to only provide the current firmware release for their Linksys routers. This meant that previous firmware revisions could not be sourced, so only the firmware supplied with the router and the latest firmware could be tested. Cisco was contacted and asked to provide previous firmware releases ("Online support case with Cisco representative," 2012), but they declined, again stating that it was not policy to provide non-current firmware.

Reset the device to its factory settings.

To ensure the device did not have any previous data or configuration settings from previous use, both the hardware reset switch was used, as well as the "Reset to factory defaults" option in the router's configuration settings.

Record WPS default setting

The WRT160N v2 has WPS enabled by default. This means that the network that the WRT160N v2 connects to could be vulnerable to penetration by the WPS PIN vulnerability without the owner being aware of the risk.

Run "wash" against the device

Wash is a tool used to identify wireless devices that may be susceptible to the WPS PIN vulnerability (Figure 1). It is ran to confirm that if it decrees that a wireless device is vulnerable, then reaver should be able to attempt to find it's PIN via brute forcing.

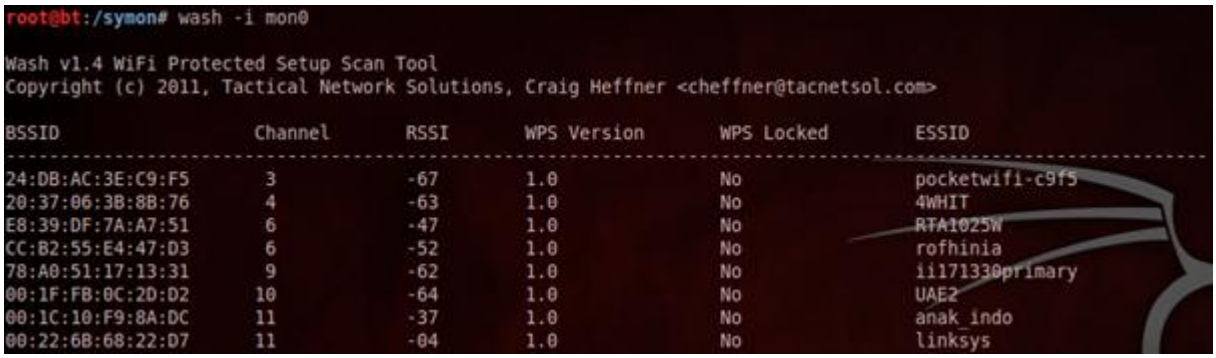


Figure 1: Sample wash output.

Run "reaver" against the device

Reaver is a tool that will allow for brute forcing of the WPS PIN. The rate of PINs that it can attempt may vary, and depends on a number of factors such as the response rate of the router, any rate limiting implemented by the router, and types of responses received from the router. Reaver ran against the WRT160N v2 achieved a consistent rate of 3 seconds per PIN (Figure 2). The WRT160N v2 router running firmware version 2.0.02 does not enact any sort of brute force protection, so the entire key space can be searched in around 9 hours and 10 minutes.

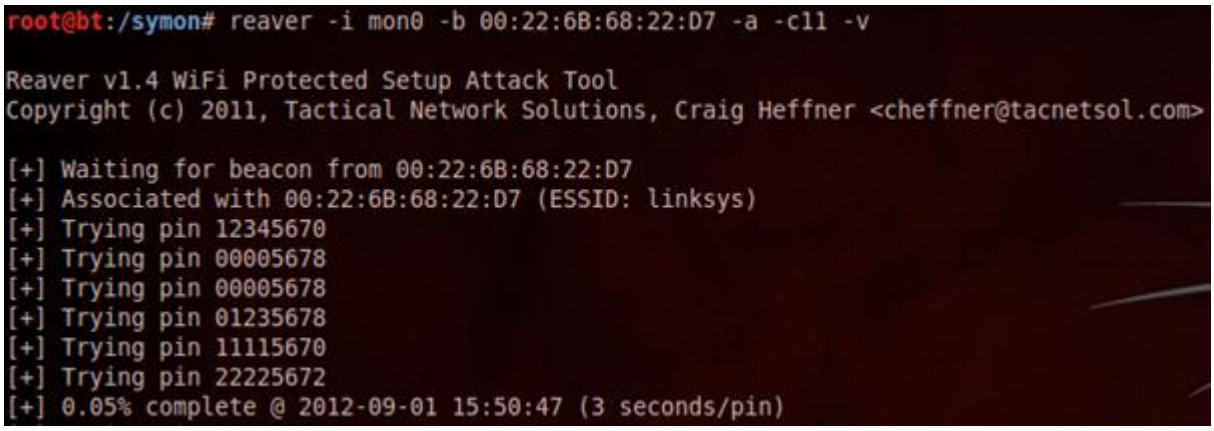


Figure 2: Sample reaver output.

Disable WPS and run the "wash" and "reaver" tests again.

It is important that a user can be sure that settings in the wireless router function as intended. In this case, it is the expected behaviour that setting WPS to a disabled state in the router configuration will disable WPS, and hence mitigate the vulnerability. However, with both versions of the router firmware tested (2.0.02 and 2.0.03) disabling WPS in the "Basic Wireless Settings" configuration menu option did not disable WPS. This would easily lead the user into a false sense of security.

Flash device with the chronologically next firmware revision, reset the device, and run the series of tests again.

Once the results of the audit have been recorded, the process is started again with the next available firmware revision. In the case of the WRT160N v2, there was only one other firmware release available to audit. Once all firmware versions have been audited, the process is complete.

RESULTS

In the initial phase of the research the "wash" tool revealed that the Linksys router was likely vulnerable. Whilst the discussion of how this indication was borne out by the result will follow, the verification step alone might be used by an attacker to quickly identify likely targets. The use of such a tool to rapidly determine susceptibility constitutes a significant risk to vulnerable devices in commercial or industrial installations.

Upon detection of the vulnerability, reaver was able to brute force the WPS PIN of the Linksys router. It is interesting to note that after examination of the attacked device, no alerts were displayed in the router GUI, or in its logs, which means the owner of the device would have no indication that hostile actions were being taken against their network. Upon compromise by the reaver tool, the researchers were successfully able to retrieve the WEP, WPA or WPA2 passphrase when provided said PIN (Figure 3). Such success is of greater concern when viewed against the fact that the WPS PIN does not change automatically, and most routers lack the ability to manually change the PIN. Given this, any future WEP/WPA/WPA2 passphrase or SSID changes would easily be discovered by simply asking the router what the new passphrase is (Figure 4) using the compromised WPS PIN.

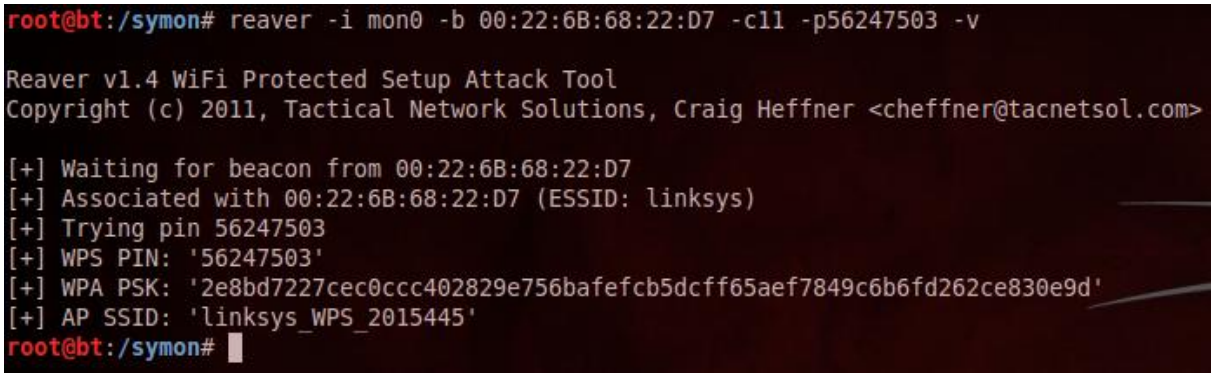


Figure 3: Retrieval of passphrases with compromised PIN.

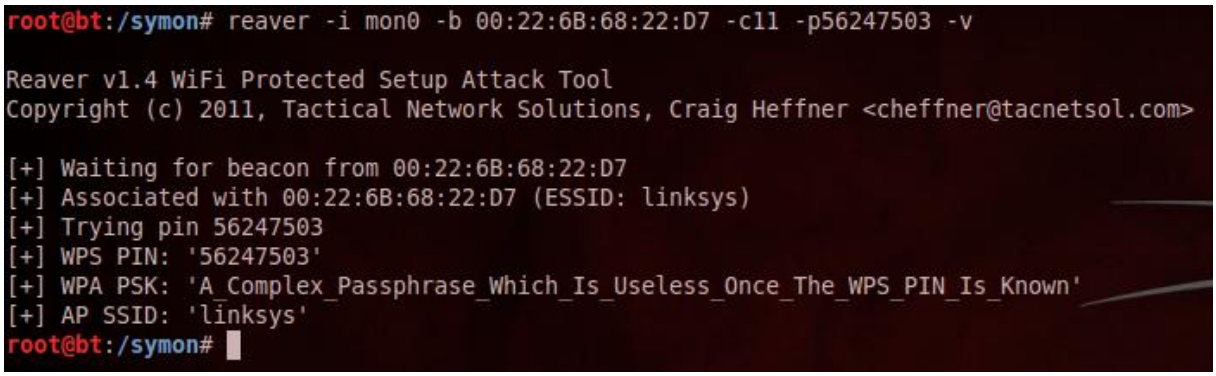


Figure 4: Querying the router for the new passphrase.

Does WPS certification mean a device is safe?

As mentioned previously, the Wi-Fi Alliance Certification process is designed to offer the consumer an assurance that products with their certification logo will interoperate seamlessly with other devices with the same certification. Devices that have WPS as a part of their certification will ensure that they will be able to communicate with other WPS enabled devices, regardless of manufacturer. This certification, however, is not designed to guarantee that a device is free of software or security defects.

The Linksys WRT160N v2 WPS certificate ("Wi-Fi Certified Interoperability Certificate," 2008) clearly details WPS certification; however as the WPS PIN security vulnerability is based on a flaw in the protocol design and implementation, it is not a vendor specific issue. Therefore, WPS certification has no bearing on whether the wireless device vendor has implemented their own security against the WPS PIN being brute-forced.

Is not being able to disable WPS an issue for the average consumer?

During the investigation and in accordance with the established methodology (Aked et al., 2012) it was shown that altering the options on the Linksys WRT160N v2 had no effect on its vulnerability. Thus it is likely that some consumers or even professionals may be deceived in thinking they have removed the vulnerability by altering the routers settings. Such issues, wether intentional or oversights dramatically increase the likelihood of this attack as there is no way to determine a devices' susceptibility without running the attack against owned

devices. Furthermore if the vulnerability is detected there is no remedy available until the device firmware which fixes the vulnerability is released by the manufacturer.

To determine the status of the WRT160N v2 the authors contacted the manufacturer regarding the results to the WPS PIN vulnerability

> *They stated that although some firmware revisions for other Linksys devices are available that allow for WPS to be disabled, not all their products are currently covered ("WPS Vulnerability status update for Linksys devices," 2012). The Linksys WRT160N v2 has an updated firmware availability date of "To Be Determined". Given it has been in excess of 10 months since the vulnerability was first published, it may be construed that an updated firmware might never be released. It also highlights the likelihood that such a vulnerable device may have been exploited for an extended period.* ("Online support case with Cisco representative," 2012).

CONCLUSION

The application of the auditing methodology to the Linksys WRT160N v2 wireless router has shown that said methodology allows for an accurate assessment of the device's susceptibility to the WPS external registrar PIN authentication design vulnerability.This research has demonstrated that both of the publically available firmware versions for this wireless router are not only susceptible to having it's WPS PIN be brute forced, but also that WPS cannot truly be disabled in the web interface. The security implications of both flaws are significant, as they allow a hostile user to quietly and easily penetrate the security of the router, and to do so even if WPS is apparently disabled. Once the WPS PIN is obtained, it was demonstrated that a change of the WEP, WPA or WPA2 passphrase will not stop an attacker from easily re-connecting with the router, and obtaining the new passphrase within seconds.The methodology is open to further refinement, with automated attempted penetrations via reaver, and multiple reaver iterations using different parameters being potential avenues of further development. Due to the potential of this attack, further studies of popular devices are already underway.

REFERENCES

Aked, Symon, Bolan, Christopher, & Brand, Murray. (2012). *A proposed method for examining wireless device vulnerability to brute force attacks via WPS external registrar PIN authentication design*. Paper presented at the The 2012 International Conference on Security and Management (SAM'12), Las Vegas, USA. http://sam.udmercy.edu/sam12/accepted-papers.html

Allar, Jared. (2011, 09/02/2012). Vulnerability Note VU#723755. Retrieved from http://www.kb.cert.org/vuls/id/723755

Annual Report 2011. (2011). Retrieved from http://www.wi-fi.org/register.php?file=20120228_WFA2011_AR_PUBLIC.pdf

CVE-2011-5053. (2011). Retrieved from https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-5053

Frequently Asked Questions: Wi-Fi Protected Setup™. (2006). Retrieved from http://www.wi-fi.org/files/WFA%20Wi-Fi%20Protected%20Setup%20FAQ.pdf

Heffner, Craig, & Eacmen, Peter. (2012). reaver-wps. Retrieved from https://code.google.com/p/reaver-wps/

Jagermo. (2012). WPS Flaw Vulnerable Devices. Retrieved from https://docs.google.com/spreadsheet/lv?key=0Ags-JmeLMFP2dFp2dkhJZGIxTTFkdFpEUDNSSHZEN3c

Linksys Support. (2012). Retrieved from http://homesupport.cisco.com/en-apac/support/routers/WRT160N

[Online support case with Cisco representative] (2012, 01/09/2012).

Turab, Nidal, & Moldoveanu, Florica. (2009). A COMPARISON BETWEEN WIRELESS LAN SECURITY PROTOCOLS. *Universitatea Politehnica Bucuresti Scientific Bulletin.* Retrieved from http://www.scientificbulletin.upb.ro/rev_docs/arhiva/full7970.pdf

Viehböck, Stefan. (2011a). Brute forcing Wi-Fi Protected Setup. Retrieved from https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

Viehböck, Stefan. (2011b). WPScrack. Retrieved from http://dl.dropbox.com/u/22108808/wpscrack.zip

Vulnerability Summary for CVE-2011-5053. (2012). Retrieved from http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-5053

Wi-Fi Alliance Member Symposium. (2011). Retrieved from http://www.wi-fi.org/files/20110421_China_Symposia_full_merge.pdf

Wi-Fi Certified Interoperability Certificate. (2008). Retrieved from http://certifications.wi-fi.org/pdf_certificate.php?cid=WFA6231

Wi-Fi CERTIFIED Wi-Fi Direct. (2010). Retrieved from http://www.cnetworksolution.com/uploads/wp_Wi-Fi_Direct_20101025_Industry.pdf

Wi-Fi Protected Setup™. (2012). Retrieved from http://www.wi-fi.org/knowledge-center/articles/wi-fi-protected-setup%E2%84%A2

Windows Connect Now–NET. (2006). Retrieved from http://download.microsoft.com/download/a/f/7/af7777e5-7dcd-4800-8a0a-b18336565f5b/WCNNetspec.doc

WPS Vulnerability status update for Linksys devices. (2012). Retrieved from http://www6.nohold.net/Cisco2/ukp.aspx?vw=1&docid=3bccc46248f9417b909e2c1028f6778e_WPS.xml