



Waterford Institute of Technology

The Modern Reality of WPS

Jack Donoghue

Jack Donoghue

BSc (Hons) in Computer Forensics and Security – Year 2

20072172

Donoghuej97@gmail.com

Contents

Introduction	3
Creation	3
Concept	3
How it works	4
Brute Force Exploit	5
Brute Force Practical.....	6
Setup.....	6
Theory	6
Method	7
Defences	9
Conclusion	9
Default PIN Practical	10
Setup.....	10
Method	10
Defences	13
Conclusion	13
Pixie Dust Attack Analysis	14
Theory	14
Exploit	15
Defences	15
Conclusion	16
References	17

Introduction

The purpose of this report is to highlight the insecurity that has come with the introduction of WPS as a widely used and implemented protocol in the routing and home computing industry, I will look at the trade-off that has taken place with the introduction of WPS and how we have sacrificed security for convenience.

Creation

The Wi-Fi Protected Setup protocol was created by the Wi-Fi Alliance as a solution to the community who had little knowledge of the security aspects involved in home computing, the Wi-Fi Alliance believed that WPA2 and other password encryption features were not very user friendly and therefore opted for a solution that would help to accommodate new users and users with little computer based knowledge. (Higgins, 2008)

Concept

WPS was conceived by the Wi-Fi Alliance as a result of many of the industries large technology companies efforts to produce a quick and easy solution that allowed their consumers to connect to their home routers with ease. WPS was the standardised solution to the many ideas put forward by large technology companies such as Broadcom, Microsoft and Intel, WPS implemented many of the features used by these companies and created WPS as we know it today, it was essentially created to normalise the market behind one standard rather than having a separate protocol for each router brand. (Higgins, 2008) This is similar to how mobile phone companies were forced to use generic universal chargers rather than having their own unique interfaces for each device. These decisions are made to protect consumer's rights and also to ensure their privacy is protected by a globally accepted protocol. (O'Reilly, 2013) However as this report will reveal this has not been the case with WPS and its implementation has become an unnecessary security risk for minimal convenience.

How it works

The WPS protocol uses an eight digit PIN that is printed on the host router, this PIN needs to be entered by anyone who wishes to connect to the router via WPS, it is essentially a local public password that you can share with people that you want to connect to your router without having to enter a long or private password. However this is very counter intuitive as this 8 digit code when guessed correctly will reveal the routers password, essentially making having a strong mixed case password redundant, as it can be obtained by successfully guessing an 8 digit PIN.

(Ducklin, 2014)

The alternative method of connection with WPS is the push-button configuration (PBC) this is where a person will press the WPS button on a router and then intercept the broadcast from the router on the device that they wish to connect to the router, however this method is also unsafe as anyone nearby can also intercept the broadcast and connect to the router.

Brute Force Exploit

The main exploit detected in the WPS protocol is to do with the PIN feature that it uses to add new devices to the network, this PIN is eight digits long, and this means that to brute force the pin of a router it would take 100 million or 10^7 possible combinations compared to the millions upon millions of possible combinations that it would take to crack a stand WPA2 password. However 100 million possible combinations is still a sizeable amount, the exploit lies in the way the protocol is used, when a new user enters a PIN there is a back and forth interaction between the 'registrar'¹ and the 'enrollee'² called a 'cryptodance', this process is where the enrollee and the registrar attempt to prove to each other that they know the PIN, this is where the brute force exploit is prevalent, because of this process the protocol splits the eight digit PIN into two four digit pins, then compares the first half of the enrollee's PIN to the existing PIN held by the registrar, if they match then the process moves on to the second half of the PIN.

(Ducklin, 2014)

When the exploit was first found it was concluded that you only needed to match the first 4 digits which is a maximum of 10,000 digits or 10^4 and since the second section of the PIN contains a check digit, or a digit that is automatically calculated from the previous seven, meaning there is only 1,000 or 10^3 possible outcomes for the second section of the PIN.

(Ducklin, 2014)

This revelation allows any WPS enabled router vulnerable to having their PIN brute forced in the space of 30 minutes to 4 hours.

¹ The device that either grants or denies credentials to a network, usually integrated into the router.

² The device that is attempting to connect to the router

Brute Force Practical

Setup

The setup for this practical required Kali Linux which was setup in virtual box, the software used in Kali is called Reaver, this piece of software is used to exploit the PIN bug found in the WPS protocol, recently there has been a further exploitation found in WPS and we will also use Reaver to show this exploit, however this practical is based on a brute force attack, where Reaver will try every possible PIN combination for the first four digits and then when successful it will continue to the last three digits.

Theory

To further understand where this brute force attack takes place I have included a diagram from Sophos as seen below.

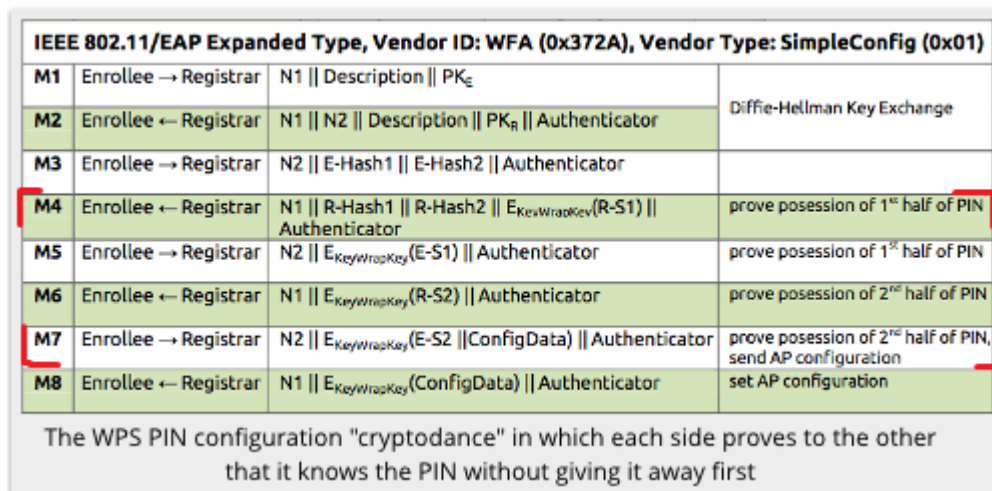


Figure 1 cryptodance WPS

(Ducklin, 2014)

In the above diagram we see the back and forth communication that occurs in the WPS protocol, the brute force attacks only focuses on the steps M4 – M7, in steps M4 and M5 the enrollee and the registrar compare their PINs and check for a match, in Reaver we can loop this process and try every possible combination until we find a match, then we proceed to M6 where we attempt to guess the second section of the PIN.

Method

I began by adding my USB wireless adapter to my Kali Linux via virtual box

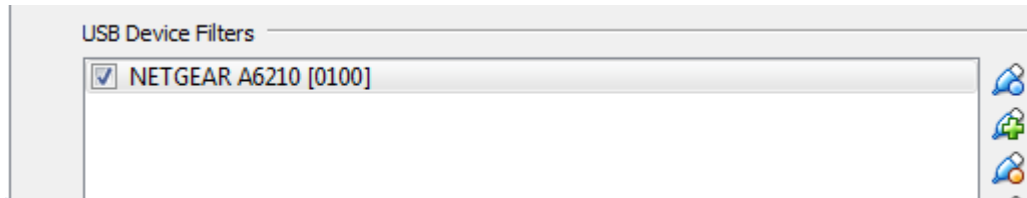


Figure 2 remote adding of USB device

By doing this I allow Kali to recognise my USB adapter, it can then connect to the internet as if it were the host machine having direct access to the USB device.

Then I began to setup my wlan0 to monitor all networks in range of my adapter.

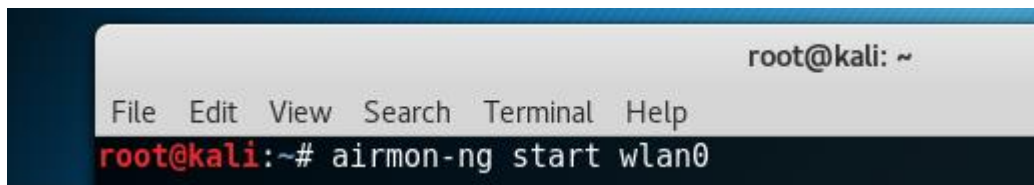


Figure 3 aircrack being used to configure adapter

Here I use the airmon command which is part of the Aircrack-ng toolkit which is essentially a cracker and analysis tool for 802.11 wireless local area networks. This command puts our wlan0 interface into monitoring mode.

Now that the interface is in monitoring mode we can search for local networks that are broadcasting with WPS enabled, using the command 'airmon-ng wlan0mon -wps' this will scan for networks, the addition of '-wps' ensures that only routers with WPS enabled will be returned.

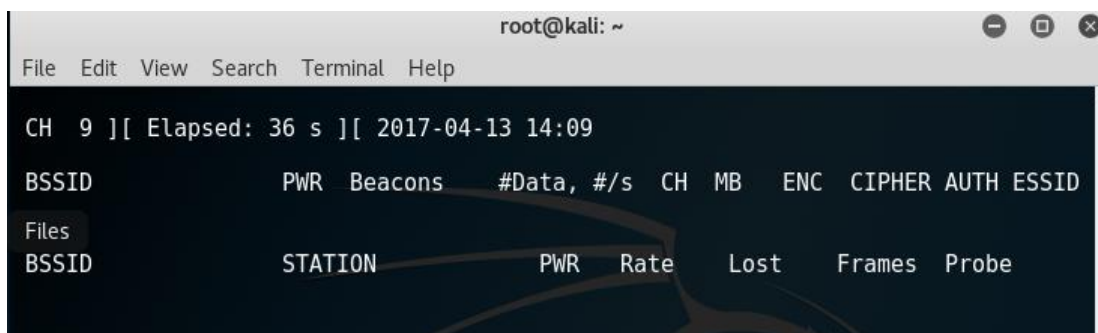
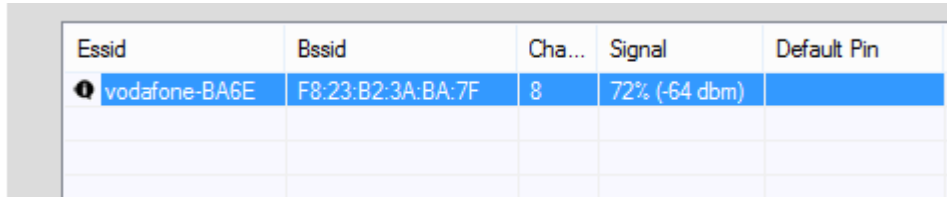


Figure 4 Network scan begins

This layout is similar to how a comparable piece of software works, Dumpper is a Windows based application that is used for the automation of default PIN attacks, as seen below it also returns the same results as Aircrack-ng.

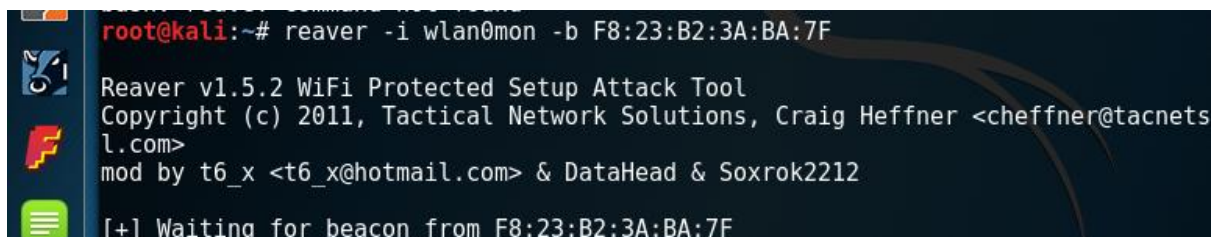


Essid	Bssid	Cha...	Signal	Default Pin
vodafone-BA6E	F8:23:B2:3A:BA:7F	8	72% (-64 dbm)	

Figure 5 dumpper returns similar statistics.

Here we can now see the routers BSSID and its Channel, this is necessary information to complete the brute force attack.

The next step requires use of Reaver's looping and brute force attacking feature, by using the recovered information from our previous steps I can now enter the details of the router that is to be attacked and wait for the brute force attack to complete.

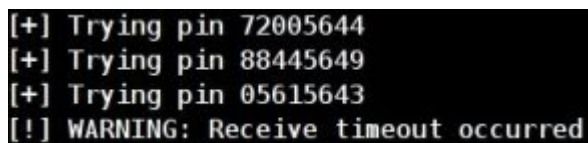


```
root@kali:~# reaver -i wlan0mon -b F8:23:B2:3A:BA:7F
Reaver v1.5.2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnets
l.com>
mod by t6_x <t6_x@hotmail.com> & DataHead & Soxrok2212
[+] Waiting for beacon from F8:23:B2:3A:BA:7F
```

Figure 6 reaver attempts to brute force the routers PIN

Defences

The brute force method of attack is the oldest known WPS exploit, this means that many modern routers will have in-built protection to prevent multiple re-entering of PINs, the router I used for the brute force demonstration was relatively new, its defensive solution to dealing with multiple PIN entry's was to first lock WPS PIN for a pre-determined period of time entry after three invalid attempts, depending on the router it would then either disable WPS or keep locking after a certain amount of attempts.



```
[+] Trying pin 72005644  
[+] Trying pin 88445649  
[+] Trying pin 05615643  
[!] WARNING: Receive timeout occurred
```

(Tape, 2012)

Figure 7 timeout example

Conclusion

However this does not mean that the router is secure with WPS enabled, as seen in the picture above timeouts do occur but often they only last from ten to thirty seconds and in most cases it will only lock out after ten invalid inputs.

(Netgear, 2016)

This increases the amount of time required to brute force a router from several hours to two or three days, the main reason it will not prevent a determined attacker is because tools like Reaver save the inputs they have already given to the router, so that even when a router locks out, Reaver will know where to start from again, in the case of brute force it is always just a matter of how determined someone is.

Default PIN Practical

Setup

The default PIN practical is the most user friendly of all the ways a user can exploit WPS, it involves attempting to access a WPS PIN enabled router with the default PIN given to the router, this default PIN is calculated using the routers BSSID. For this practical I will be using Dumpper which is a Windows based program that retrieves information similar to Aircrack-ng and Reaver, Dumpper essentially automates the steps that Reaver takes in the previous practical, however it also retrieves the default PIN for each router after it finds the BSSID of the router, it then attempts to connect to the router using the default PIN.

Method

The approach to this practical is relatively basic and it implements two pieces of software that are run in unison with each other, the first and main piece of software is Dumpper and it is run in conjunction with JumpStart also known as JumpLittle, JumpStart is used to connect to the router while Dumpper is used to retrieve the information that JumpStart will use.

Here we can see Dumpper retrieving information about networks in my area.

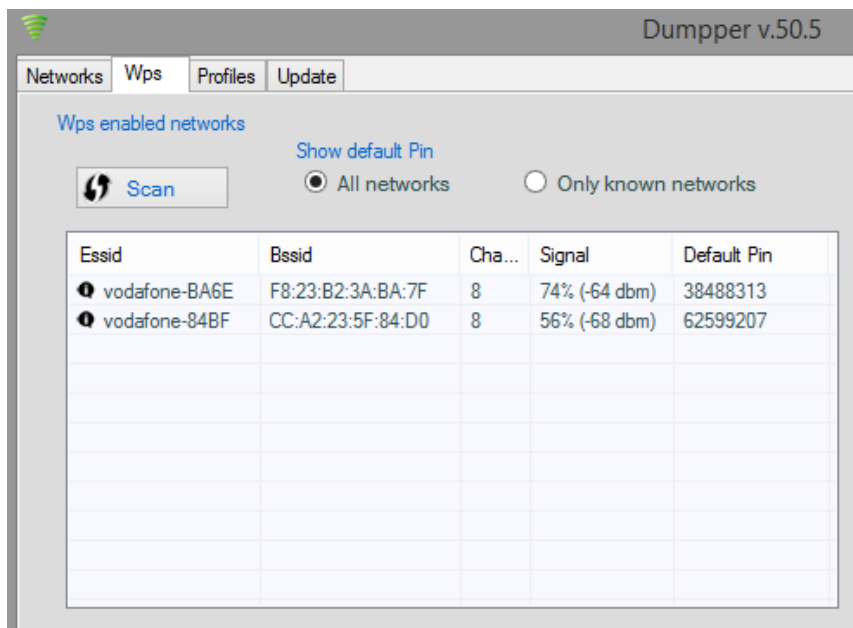


Figure 8 Two networks detected

Here we can see two networks being retrieved by Dumpper, the first network is my home network and the second network is an unknown network that I have never seen before, Dumpper is still able to retrieve both their BSSID/ ESSID and their default PINS.

It is also possible to find the default PIN of the router using only the BSSID, below is a website that creates default PINs based on the BSSID entered.

Essid	Bssid	Cha...	Signal	Default Pin
vodafone-BA6E	F8:23:B2:3A:BA:7F	8	100% (-60 db...	38488313

Figure 9 Dumpper's Default pin

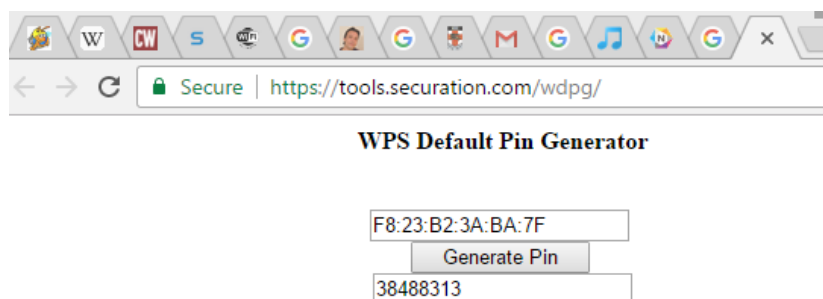


Figure 10 Default PIN matches Dumpper's.

The default PIN will work in many cases, even though my router was able to protect against brute force attacks, it was still vulnerable to a simple default PIN attack, after the attack has completed we can see the log history which shows the M2 – M8 messages and the final Wsc_Nack acknowledgment that the PIN matches.

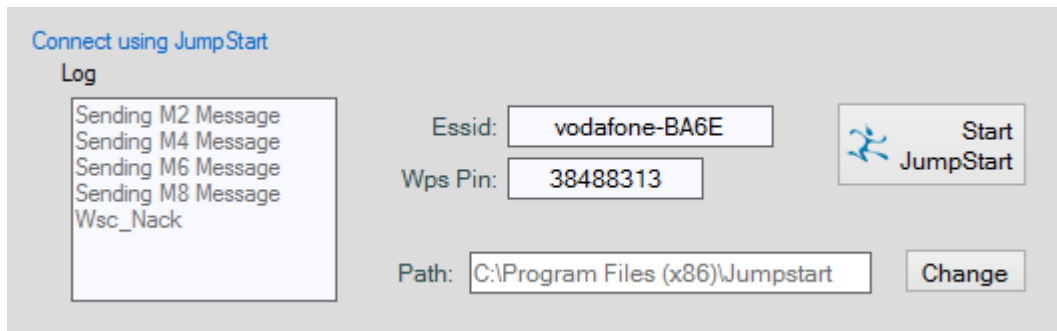


Figure 11 log messages.

However if I were to enter the first four digits correctly but changed one of the digits in the second section I would only get to the M6 stage (The stage where I send my second section of the PIN to the router to check its validity) it would then fail and drop.

Now that I have gained access to the router I can enter my command prompt and recover the WPA2 key of the router.

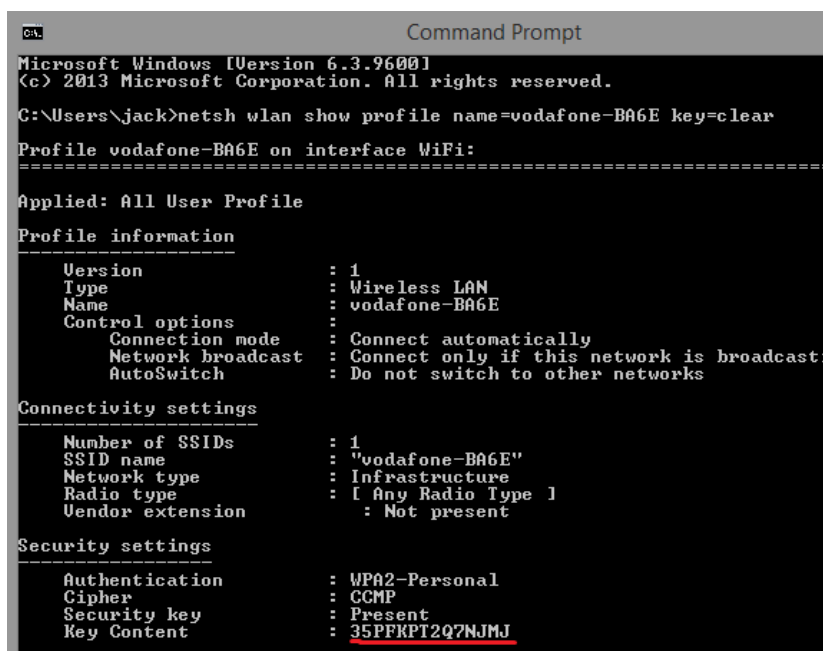


Figure 12 The WPA2 key is recovered

Defences

To defend against being vulnerable to a default PIN attack most routers including mine offer an option to either disable WPS PIN which is advisable, however if you wish to use WPS PIN then there is also an option to generate a new WPS PIN number, I did this to my own router after seeing how susceptible my router was to this process, my Vodafone router has a feature which allows me to generate a new PIN in the routers interface as seen below.

The screenshot shows the 'Wireless Settings' page of a router. The 'WPS' section is expanded, showing options for 'Enable WPS' (checked), 'WPS Mode' (set to 'AP PIN'), and 'AP PIN' (31313711). A red box highlights the 'Generate PIN' button. Other settings visible include 'Mode' (802.11b/g/n), 'Country Code' (IRELAND), 'Channel' (Auto), 'Band Width' (20/40 MHz), 'Guard Interval' (short), 'Transmit power' (100%), 'SSID Index' (SSID1), 'Network Name' (vodafone-BA6E), 'Maximum Number of Accessing Devices' (32), 'Enable SSID' (checked), 'Hide Broadcast' (unchecked), 'Enable WMM' (checked), 'Security Mode' (WPA-PSK/WPA2-PSK), 'WPA Pre-Shared Key' (masked with dots), 'WPA Encryption' (TKIP+AES), and 'Enable WPS' (checked).

Figure 13 generating a new PIN

Conclusion

Having successfully generated a new PIN I could no longer connect to my router using the old default PIN and Dumppper was still showing my default PIN meaning that I was no longer vulnerable to this attack, this vulnerability makes it very easy for people to access routers with WPS PIN enabled, and it takes minimal effort to acquire the software and familiarise yourself with its functionality. While I was able to strengthen my routers security against this kind of attack it did take some steps that many novice users of home computing may not be familiar with, and since WPS was created with the intention of drawing in novice users, it is unfair to expect that these users would know how to generate a new PIN to secure their routers from outside attack.

Pixie Dust Attack Analysis

Theory

The Pixie Dust attack is a more recent exploitation of the WPS protocol, unlike the brute force attack it focuses on the M1 – M3 steps of the WPS crypto dance, the attack focuses on the information that is already given to us by the router.

IEEE 802.11/EAP Expanded Type, Vendor ID: WFA (0x372A), Vendor Type: SimpleConfig (0x01)			
M1	Enrollee → Registrar	N1 Description PK _E	Diffie-Hellman Key Exchange
M2	Enrollee ← Registrar	N1 N2 Description PK _R Authenticator	
M3	Enrollee → Registrar	N2 E-Hash1 E-Hash2 Authenticator	

Figure 14 the steps under analysis

(Ducklin, 2014)

To understand the pixie dust attack we must first analyse the steps taken by WPS in this diagram, at the M1 stage the Enrollee gives the Registrar its public key and in M2 the Registrar replies with its public key, these keys will be referred to as PKE and PKR respectively. These keys initiate communication between the two devices and allow for the exchange of further information. While the M2 message is being sent to the Enrollee, two hash values of the WPS PIN are also sent separately, these are called E-Hash1 and E-Hash2, they represent the first and second parts of the WPS PIN respectively. (Hegelund, 2015)

This attack is considered an offline attack since when we receive that hash values for the PIN at the beginning we don't need to communicate with the router like we do in the brute force attack, we can try all of the inputs 'offline' and then when we have retrieved the correct PIN we submit it.

Exploit

The exploit that is taken advantage of here is the ‘nonces’ created by the router when communicating with a new device, these nonces are called ES1 and ES2 and are generated by the router individually, different brands have different ways of generating these variables, however the exploit lies in how brands generate these numbers, some brands including Ralink, MediaTek and Celeno³ set the ES1 and ES2 values to 0 by default, this means that there is no work involved in working through or resolving this figures, with the ES1 and ES2 values acquired you can then fill into the hash function and try every pin until we get a match with the E-Hash1 and E-Hash2, once we have a match we can retrieve the WPS PIN.

(Hegelund, 2015)

Defences

Unlike the brute force exploit and the default PIN exploit there is no possible way for an end user to modify ES values like how I changed the PIN in the case of the default PIN exploit, the only known way to avoid this type of attack is to research your router and see if it is vulnerable to this attack, while a lot of routers are vulnerable to this method because of the ways they generate these values, some routers that are susceptible to this method of attack often set their ES values to zero. (Sox, 2015)

In the case of some Broadcom branded routers, the rand() function in C was used to generate random ES values. It is advisable that when purchasing a new router or signing up to an ISP that you check the device for the vulnerabilities outlines above, the only way to avoid a pixie dust attack is to have a high-end router that is relatively new, many of the new chipsets will not have ES values set to zero, however until a true fix is determined it is advisable to disable WPS PIN usage. (Broadcom, 2012)

Conclusion

This paper has observed the safety of the Wi-Fi Protected Setup protocol and analysed the various different approaches and weaknesses in separate stages of the WPS crypto dance or ‘handshake’, it is quite apparent from the research done that WPS is still an overwhelmingly vulnerable protocol that aims to draw in an audience of users that may not want to be inconvenienced by traditional WPA2 passwords, and while it is understandable to want to make connecting to a home router a hassle free experience, it is also paramount that the safety of the network is upheld, and if in the process of making a hassle free experience the users networks safety is at risk, then the danger of a breach far outweighs the perks of creating a hassle free experience.

Although WPS remains significantly insecure, there is work being done by leading brands as mentioned above, to improve their contribution to the safety of WPS as a protocol, in the future WPS may become a much safer protocol, but as of now it is a rushed and forced protocol that has been pushed into many homes without proper instruction or support for the problems and insecurities it has brought.

References

Tim Higgins (2008). 'How is WPS supposed to work'

Available at: <https://goo.gl/EDnCGb>

Accessed: 12 March 2017

Kamel Messaoudi (2012) 'Wi-Fi Protected Setup'

Available at: <https://goo.gl/WzUD8M>

Accessed: 3 April 2017

Sudhanshu Chauhan (2012) 'Wi-Fi Security: The Rise and Fall of WPS'

Available at: <https://goo.gl/PC82v2>

Accessed: 2 April 2017

Mads Hegelund (2015) 'WPS Pixie Dust Attack'

Available at: <https://goo.gl/o7sUCQ>

Accessed: 6 April 2017

Tape (2012) 'Cracking WPA using WPS vulnerability with reaver v1.3'

Available at: <https://goo.gl/Csj2mJ>

Accessed: 7 April 2017

Paul Ducklin (2014) ‘Using WPS on your Wi-Fi router may be even more dangerous than you think’

Available at: <https://goo.gl/aho1Lq>

Accessed: 5 April

Quintin O'Reilly (2013) ‘EU passes deal on universal mobile phone charger’

Available at: <https://goo.gl/kOy9sZ>

Accessed: 1 April 2017

Sox (2015) ‘WPS Pixie Dust Attack (Offline WPS Attack)’

Available at: <https://goo.gl/C3WBOe>

Accessed: 9 April 2017

Netgear (2016) ‘How do NETGEAR Home routers defend against WPS PIN vulnerability’

Available at: <https://goo.gl/lmb0Uo>

Accessed: 7 April

Broadcom (2012) C code for random functions.

Available at: <https://goo.gl/zZ8UWb>

Accessed: 11 April