Analysis of WPS Security in Wireless Access Points

AMIRMOHAMMAD SADEGHIAN
Advanced Informatics School (AIS)
Universiti Teknologi Malaysia (UTM)
UTM, Jalan Semarak, Kuala Lumpur
MALAYSIA
i@root25.com
http://www.root25.com

Abstract: Usage of wireless technology for ease of communication is growing rapidly. Such transmissions channel might contain valuable information, therefore securing these networks is compulsory to assure about the confidentiality of information. Currently there are few main security standards for securing wireless networks and configuration of these networks needs moderated networking skills. WPS is standing for Wi-Fi Protected Setup, a standard that introduced by Wi-Fi Alliance in 2007 to make the process of establishing a secure wireless network more convenience for users. Currently all of certified wireless equipment might have Wi-Fi Protected Setup feature. This standard allow users with little or no information about networking to setup a secure wireless network or add new devices to their existing network without hassle of entering the password. Currently almost all of well-known networking brands of wireless equipment that are in the market or already are in use have WPS-certificate and WPS feature is by default enabled in them. In December 2011 a researcher found a security flaw that allows the attacker to perform brute-force attack against the WPS pin number. In result of a successful attack the pin code of the network will raveled and attacker can gain access to the wireless network. This paper aims to analysis this security issue with practical implementation and attacks, following by the solution.

Key-Words: WPS; WPA2; Wi-Fi; Wireless Network; PIN code; Security Vulnerability

1 Introduction

Over the last few years Wireless networks have gained high popularity for making an easy and flexible communication method between devices such as computers, tablets, mobiles and printers. This system provide mobility features for the users to access to network from everywhere without hassle of wires and network configurations. After rapid adaption to wireless networks the issue of security inside them arises and researchers tried to improve the security inside Wi-Fi network by proposing new solutions. But implementing of all these solutions need good knowledge of networking and security to setup and configure the wireless network in a way that attacker cannot penetrate into that. Most of Wi-Fi users do not use security features due to complicated configuration are necessary to establish a secure wireless network, therefore this will lead to their network become vulnerable to outsider threats. For addressing this problem Wi-Fi Alliance designed Wi-Fi Protected Setup (WPS) certificate to simplify this process for wireless users [1].

2 Wi-Fi Protected Setup Structure

Wi-Fi Protected Setup also known as Wi-Fi Simple Configuration. This standard use four main method to establish the security network: Push buttons, PIN code entry, Near Field Communication, USB flash drive [2]. The last two methods known as out-of-band because they use a second technique other than Wi-Fi for making the communication, also they are not covered by WPS certification.

- PIN entry: In this technique there is a label on back side of the wireless equipment (router/access point) containing a personal identification number (PIN) that should be read by the user and entered into the new device that wants to connect to the secure wireless network. This PIN provided by the manufacturer of the wireless device and existence of this feature in all WPS certified devices is necessary.

- Push-Button: In this technique user has to push a button on the access point (AP) and in the same time on the new wireless device that want to join. This button might be a physical button or either a button in software environment. Existence of this feature in the access point is necessary but optional in the client. The period that access point will wait for the client to join is two minutes and any device in the signal range is able to join by pushing the WPS button.

- USB flash drive: In this technique configuration data are stored in a flash drive and will transfer to the new client without using of wireless. Existence of this feature is optional.

- Near-Field-Communication (NFC): In this technique by using the near field communication, client brings the new device nearby the access point to transfer the network configuration without entering any pin. Existence of this feature is optional.

WPS standard uses Diffie–Hellman key exchange for establishing a secure channel to transfer network credentials such as network key. Diffie–Hellman is a well-known key-exchange technique that allows two users without having any background knowledge of each other to make a shared key in an insecure channel [3]. Client and access point (AP) pass 4 main stages for establishing a channel between them. In the first stage client will send an authentication request to the AP in result AP will reply it with authentication response. In the second stage client send association request to the AP in reply AP will send an association response to the client. In the EAP Initiation stage client send EAPOL-Start to the AP. AP will ask for the EAP identity, in reply client will sends its EAP identity. Figure 1 is showing details of the key exchange [4].

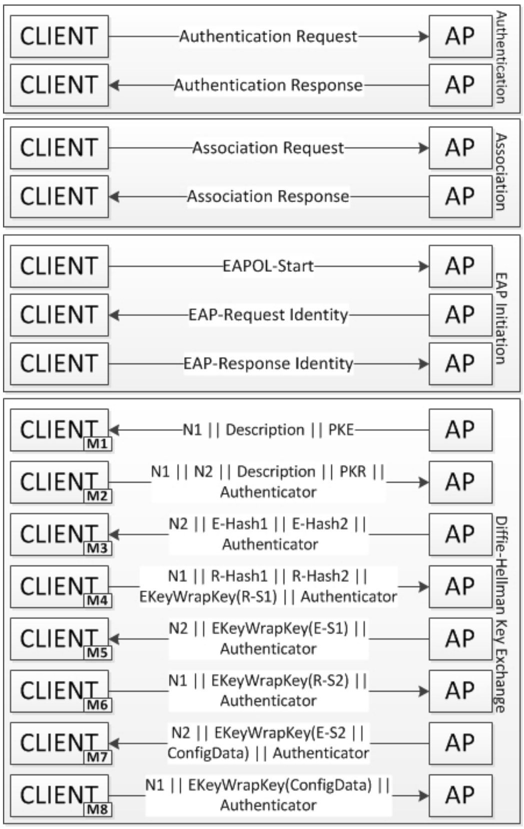
Authentication
CLIENT
Authentication Request
AP
Authentication Response
Association
Association Request
Association Response
EAP Initiation
EAPOL-Start
EAP-Request Identity
EAP-Response Identity
Diffie-Hellman Key Exchange
M1
N1 || Description || PKE
M2
N1 || N2 || Description || PKR || Authenticator
M3
N2 || E-Hash1 || E-Hash2 || Authenticator
M4
N1 || R-Hash1 || R-Hash2 || EKeyWrapKey(R-S1) || Authenticator
M5
N2 || EKeyWrapKey(E-S1) || Authenticator
M6
N1 || EKeyWrapKey(R-S2) || Authenticator
M7
N2 || EKeyWrapKey(E-S2 || ConfigData) || Authenticator
M8
N1 || EKeyWrapKey(ConfigData) || Authenticator

Figure1. Key exchange in external registrar.

Sooner we mentioned that there are four main techniques for establishing the connection between new device and the AP, The first method was pin entry that can be two types:

- Internal Registrar: Entering the PIN in the AP web interface.
- External Registrar: The new user just needs to enter the AP PIN in his device.

2 WPS Vulnerability

In year 2011 Stefan Viehböck security researcher report to CERT that WPS enabled devices suffer from a security vulnerability that allow the attacker to brute-force the WPS PIN number [5]. In external registrar mode there is no need to any verification other than PIN and this make it vulnerable to brute-force attack. In brute-force attack a software try to guess the key by trying all possible combination of characters and there should be a stop condition exist that it can understand found the correct result.

The vulnerability source is the acknowledgement messages that sent between the client and the access point when it tries to validate the WPS PIN, this acknowledge message act as the stop condition for the brute-force attack and let the attacker know if he tried the right combination or not. The WPS PIN is an eight digit number that used to add the new client to the network. When a client attempts to join the network using WPS PIN, the access point will check the validity of the PIN separately in two halves. The first half is four digits (10000 possibilities) and second half consist of three usable digits and one check sum digit that result in three effective digit (1000 possibilities). This design greatly decrease the number of tries needed to brute force the PIN and make it more feasible. The number of attempts goes from 100,000,000 to 10,000 + 1000 which is 11,000 attempts in total [5].

Table1. WPS PIN Structure.

First half				Second half			
1	2	3	4	5	6	7	CHK

When the PIN validation is not successful the access point will return an EAP-NACK (Acknowledgement) message to the client. If the EAP-NACK received in level M5 that means the first half of the PIN was not correct. If EAP-NACK received in level M7 means the second half was not correct.

Based on a report by CERT until now product from many brands such as Belkin, Buffalo, Cisco, D-link, Linksys, Netgear, Technicolor, TP-Link, ZyXEL are affected with this vulnerability [6]. WPS feature is enabled by default in most of wireless access points and routers. In case of a successful attack the WPS PIN will reveal to the attacker, in additional to the PIN the network key also will reveal to the attacker, then by using the network key can easily join and use all resources shared on the wireless network such as internet, mass storages, printers, and other computers on the same network.

The network key length is not an effective factor in this attack because attacker cracks the WPS PIN and in result AP will reveal the network key to the new client, so basically the cracking time needed for an eight character network key is equal to 64 character key.

3 Experiment Results

A tool was developed by Craig Heffner in python for Linux operating system to implement WPS brute-force attack named Reaver [7]. In this study we setup three honeypot with different configuration to test this vulnerability in practice. We used D-link

DIR615 for two experiments, each one with different network key configuration. The other experiment was on TP-Link TL-WR841N wireless router. In this experiment we used Reaver V1.4 embedded in Back Track 5r3 with the help of Alfa AWUS036H as wireless network card.

Table2. WPS Brute-Force Experimental Results.

Brand	D-Link	D-Link	TP-LINK
Model	DIR-615	DIR-615	TL-WR841N
Device type	Wireless router	Wireless router	Wireless router
Firmware version	7.09	7.09	7
Security type	WPA2	WPA	WPA2
Encryption type	AES	TKIP	AES
Chanel	Auto	9	Auto
Distance/Meter	~2	<1	~3.5
Wall existence	•	-	•
Time elapsed to crack/Second	48837	40124	36164

Based on what we learnt from this experience network keys attributes are not effective in brute force time, however the distance and existence of wall in between the client and the AP was effective in the cracking time. Another factor is that sometimes accidently the access point delayed in replaying and it might be because of bugs inside the AP firmware.

4 Solution

It seems network equipment manufacturers are not interested in taking off this service from their products due to ease of use for users, so some of them tried to mitigate the WPS vulnerabilities. One of these techniques is lock down. Some routers this method to lock down the WPS feature in case that it detect several unsuccessful WPS request made in short period of time.

But if the router is not new or is not using the latest version of firmware from the vendor, there is high chance of vulnerability.

We suggest disabling the WPS feature until the proper fix release, for this aim you should go to access point configuration via web interface and look for “WiFi Protected Setup (WPS)” or something similar and disable it. In some rare cases the router is not able to disable the WPS feature, for example in Cisco WRP400 and Cisco WAP4410N [8]. Therefore the only solution is to update the firmware.

5 Conclusion

The vulnerability in WPS is result of poor design in authentication algorithm and no existence of a defense system against brute force attack. Due to wide spread of WPS service in most of well-known network equipment brand products and existence of “external registrar” as compulsory part of this standard we expect high amount of vulnerable products. The impact of this attack can be very high for business that use these vulnerable access points, because after joining the network using the revealed network key the attacker can launch the Man in the Middle Attack (MITM) and sniff all confidential information from the network so fixing this vulnerability should happen URGENTLY. Wireless equipment vendors also need to identify all vulnerable devices and design a new firmware including the patch for WPS. More news and article should be broadcasted about this vulnerability that end-users get alerted about this vulnerability and try to update their firmware or completely disable this feature.

References:

[1] Wi-Fi. Alliance, "Wi-Fi CERTIFIED Wi-Fi Direct." White Paper: http://www.wi-fi.

org/news_articles.php (2010).

[2] Wi-Fi. Alliance, " Wi-Fi CERTIFIED™ for Wi-Fi Protected Setup™: Easing the User Experience for Home and Small Office Wi-Fi® Networks" White Paper: http://www.wi-fi.org/knowledge-center/white-papers/wi-fi-certified-wi-fi-protected-setup™-easing-user-experience-home-a-0 (2010).

[3] Al-Aali, Ghadeer, Brett Boneau, and Kevin Landers. "Diffie-Hellman Key Exchange." Proceedings of CSE 331, Data Structures Fall 2000 (2000).

[4] Microsoft Connect Now Net, White Paper: http://download.microsoflcom/download/aim/at7777e5-7dcd-4S00-8aOa-bIS336565f5b/WCN-Netspec.doc (2006)

[5] Viehböck, Stefan. "Brute forcing wi-fi protected setup." Wi-Fi Protected Setup. Retrieved March 3 (2011).

[6] CERT Vulnerability Database "WiFi Protected Setup (WPS) PIN brute force vulnerability" http://www.kb.cert.org/vuls/id/723755 (2011)

[7] Craig Heffner "reaver wps brute-force tool" https://code.google.com/p/reaver-wps/ (2013)

[8] Cisco "Wi-Fi Protected Setup PIN Brute Force Vulnerability" http://tools.cisco.com/security/center/content/CiscoSecurityResponse/cisco-sr-20120111-wps (2012)