ACSIJ Advances in Computer Science: an International Journal, Vol. 4, Issue 5, No.17 , September 2015
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

New attacks on Wi-Fi Protected Setup

Hamed Mohtadi [1], Alireza Rahimi [2]

[1] Imam Hossein Comprehensive University
Tehran, Iran
hmohtadi@ihu.ac.ir

[2] Imam Hossein Comprehensive University
Tehran, Iran
arahimi@ihu.ac.ir

Abstract

Wi-Fi Protected Setup (WPS) is a network security standard that is used to secure networks in home and office, introduced in 2006 by the Wi-Fi Alliance. It provides easier configuration setup and is used in almost all recent Wi-Fi devices. In this paper we propose two attacks on this standard. The first attack is an offline brute force attack that uses imbalance on registration protocol. This attack needs user action, but it is more efficient than previous attacks. The second attack uses weaknesses in the implementation of WPS and provides an improved *evil twin* attack. This attack shows that even by completely disabling the WPS on the routers, all vulnerabilities are not covered.

Keywords: *Wi-Fi, WPS, evil twin, wireless network, security vulnerability.*

1. Introduction

The importance of wireless networks in today's life is undeniable. Wireless local area network (WLAN) has become more popular than the past and widely has been used in several equipment due to convenience of installing and using it. In the meantime, Wi-Fi Alliance as a non-profit organization has taken leading role to become it ubiquitous. This organization created from gathering several companies with a vision to "Connecting everyone and everything, everywhere", makes good coordination between devices by creating Wi-Fi® trademark and certifying products. Nowadays, in more than 25 percent of homes around the world, Wi-Fi is used and by 2013 about two billion Wi-Fi devices were sold [1]. Using Wi-Fi networks to help positioning systems, proves this universality [2].

There must always be a balance between convenience and security on the network. Because of the medium used in wireless networks, safety has to be specially considered. The first standard to secure WLAN, introduced by the IEEE LAN/MAN Standards Committee called WEP as part of the IEEE802.11 standard in 1997 [3]. Four years later in 2001, the first attack against WEP was published [4]. Immediately IEEE 802.11i task group established to solve the problem. Several attacks introduced against WEP [5] [6] and finally in 2003 Wi-Fi Alliance introduced WPA. It was a security protocol that Wi-Fi Alliance derived it from RSN standard [7] which was ratified in 2004. This standard called as WPA2 in products and has a few differences with WPA. Both contain two security protocols, TKIP and CCMP. TKIP was built around WEP to fix flaws without the need to hardware upgrade and CCMP designed to secure WLAN without hardware restriction. When WEP had been failed completely [8] [9], Beck and Tews introduced an attack against TKIP in 2008 [10]. The attack was limited and couldn't break the security of TKIP.

Next to security, the Wi-Fi Alliance tried to improve convenience of connection and configuration of Wi-Fi networks and then introduced Wi-Fi Protected Setup (WPS) security standard in 2006 [11]. Gradually this Standard was used in devices, so that today, almost all of them support the WPS. This optional standard made configuration very simple, but vulnerabilities made it unusable quickly. However devices still support WPS and it's just inadvisable.

The paper is structured as follows. First, we describe WPS in details. Next, we explain two brute force attacks against the WPS. Finally, we introduce two new attacks for connecting to WLAN clients via WPS vulnerabilities.

2. Wi-Fi Protected Setup structure

Wi-Fi Protected Setup as a security standard determines WLAN establishing, member connection and authentication methods. In fact, WPS is used along with WPA/WPA2 standards in order to facilitate initial configuration of the network. Basically, there are two methods to establish networks in this standard: in-band and out-of-band. In the case of in-band method, configuration data transfer using the WLAN channel and authentication is performed by PIN code entry or the push button method. If data transfer using another channel other than the WLAN, this is called out-of-band method and

authentication is performed using USB flash drive or Near-Field-Communication (NFC) technology. Here we discuss only on the in-band method.

2.1 Components

There are three major components involved in WPS: the registrar, the enrollee and the AP. The AP is an infrastructure-mode 802.11 Access Point, The registrar is one of the network's members and has the authority to issue and revoke credentials and a device seeking to join to network is called enrollee. It's allowed to these logical components be co-located, so if the AP could be the registrar simultaneously, it called as internal-registrar and if not, called at the external-registrar.
All devices seeking to join the network and also the AP can be the registrar or the enrollee. It's expected new devices join to the network as the enrollee, but more often AP is the enrollee and new devices join as external registrar. Figure 1 shows the usual setup for WPS components.

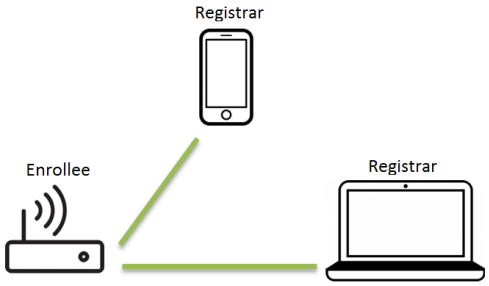

Fig. 1 Usual setup for WPS components

2.2 Registration Protocol

In the case of in-band method, authentication is based on a secret value called *Device Password*. This value varies due to the technique used. The WPS uses nonces, enrollee MAC address and Diffie-Hellman key exchange protocol to protect confidentiality of the messages. Diffie-Hellman protocol is a method to exchange secure keys in a public channel and allows the parties to jointly establish a shared secret without prior knowledge.
The Registration Protocol is done in 3 phases. In the first phase, four packets are exchanged to create a common channel between two parties. First the client sends authentication request message to the AP and receives authentication response. Next it sends association request message and receive association response as well. The second phase is about EAP initiation. The Client send EAP-start message, in response the AP asks EAP identity from the client, and the client sends it as an EAP-response identity message to the AP. In third phase Diffie-Hellman is used and then authentication messages between two parties are exchanged [11]. Table 1 illustrates first and second phases.

Table 1: First and second phases of registration protocol.

802.11 authentication and association		
Client	Authentication Request →	AP
Client	Authentication Response ←	AP
Client	Association Request →	AP
Client	Association Request ←	AP
EAP initiation		
Client	EAPOL-Start →	AP
Client	EAP-Request Identity ←	AP
Client	EAP-Response Identity →	AP

In the third phase Diffie-Hellman protocol is used and then authentication messages between two parties are exchanged. In Diffie-Hellman protocol, both sides choose a large prime number P as modulus and a base G which is a primitive root modulo P. Then each one chooses a secret integer as the private key, is shown by A and B. So public keys, private keys and shared key are determined [12]. Table 2 illustrates Diffie-Hellman keys and table 3 shows the third phase of the registration protocol.

Table 2: Diffie-Hellman keys

Public Key	Private Key		Public Key	Private Key
$PK_1 = G^A \bmod P$	A		$PK_2 = G^B \bmod P$	B
Shared key				
$PK_1^B \bmod P = PK_2^A \bmod P = G^{AB} \bmod P$				

Table 3: third phase of registration protocol.

M_1 through M_8 packets			
Registrar	$N1 \| Description \| PK_E$ ←	Enrollee	M_1
Registrar	$N1 \| N2 \| Description \| PK_R \| HMAC_{AuthKey}(M_1 \| M_2^*)$ →	Enrollee	M_2
Registrar	$N2 \| E\text{-}Hash1 \| E\text{-}Hash2 \| HMAC_{AuthKey}(M_2 \| M_3^*)$ ←	Enrollee	M_3
Registrar	$N1 \| R\text{-}Hash1 \| R\text{-}Hash2 \| ENC_{KeyWrapKey}(R\text{-}S1) \| HMAC_{AuthKey}(M_3 \| M_4^*)$ →	Enrollee	M_4
Registrar	$N2 \| ENC_{KeyWrapKey}(E\text{-}S1) \| HMAC_{AuthKey}(M_4 \| M_5^*)$ ←	Enrollee	M_5
Registrar	$N1 \| ENC_{KeyWrapKey}(R\text{-}S2) \| HMAC_{AuthKey}(M_5 \| M_6^*)$ →	Enrollee	M_6
Registrar	$N2 \| ENC_{KeyWrapKey}(E\text{-}S2 \| ConfigData) \| HMAC_{AuthKey}(M_6 \| M_7^*)$ ←	Enrollee	M_7
Registrar	$N1 \| ENC_{KeyWrapKey}(ConfigData) \| HMAC_{AuthKey}(M_7 \| M_8^*)$ →	Enrollee	M_8

- N1 and N2 are 128-bit random numbers chosen by the enrollee and the registrar, respectively.
- M^*_n is M_n excluding HMAC value.
- Description is a human-readable text contains a description about device capabilities such as Registration Protocol role, supported algorithms, MAC address, model number, etc.
- PK_E and PK_R are public keys derived from the Diffie-Hellman protocol for the enrollee and the registrar, respectively.
- The encryption algorithm in these packets is AES-CBC using the key KeyWrapKey and shown by $ENC_{KeyWrapKey}$ () notation.
- This notation, $HMAC_{AuthKey}$ () indicates providing integrity of these packets by HMAC-SHA-256 keyed hash function using the key AuthKey.
- E-S1 and E-S2 are 128-bit secret random numbers chosen by the enrollee and used to calculate E-Hash1 and E-Hash2, respectively. These two values prove enrollee's knowledge of the two halves of the device password to the registrar. Similarly R-S1 and R-S2 are 128-bit secret numbers used by the registrar to derive R-Hash1 and R-Hash2 respectively, and used for proving registrar's knowledge of the two halves of the device password, that is actually enrollee's password.
- ConfigData indicates WLAN settings and enrollee's Credentials, which contains passphrase.

All keys which are used in this protocol are derived as follows:

$$KDK = HMAC\_SHA\_256_{DHKey}(N1||EnrolleeMAC||N2) \quad (1)$$

$$DHKey = SHA\_256(g^{AB} mod\ P) \quad (2)$$

$$\text{AuthKey || KeyWrapKey || EMSK} = kdf(KDK, \text{"Wi-Fi Easy and Secure Key Derivation"}, 640) \quad (3)$$

This key derivation function (kdf) uses a UTF-8 string ("Wi-Fi Easy and Secure Key Derivation") for personalization and HMAC-SHA-256 as pseudorandom function (prf). Then 640 bits are generated.

- AuthKey is 256 bits and used for integrity of messages.
- KeyWrapKey is 128 bits. It used to encrypt secret values in registration protocol messages.
- EMSK (Extended Master Session Key) is 256 bits and is used to additional key derivation.

Other formulas:

$$E\_Hash1 = HMAC_{AuthKey}(E\_S1 || PSK1 || PK_E || PK_R) \quad (4)$$
$$E\_Hash2 = HMAC_{AuthKey}(E\_S2 || PSK2 || PK_E || PK_R) \quad (5)$$
$$R\_Hash1 = HMAC_{AuthKey}(R\_S1 || PSK1 || PK_E || PK_R) \quad (6)$$
$$R\_Hash2 = HMAC_{AuthKey}(R\_S2 || PSK2 || PK_E || PK_R) \quad (7)$$

$$PSK1 = first\ 128\ bits\ of\ HMAC_{AuthKey}(1^{st}\ half\ of\ DevicePassword) \quad (8)$$

$$PSK2 = first\ 128\ bits\ of\ HMAC_{AuthKey}(2^{nd}\ half\ of\ DevicePassword) \quad (9)$$

2.3 Push Button Configuration (PBC)

In this method a button on the AP and other devices, is used for authentication. On the one side, the button be activated and within 120 seconds the other side should press the button. The authentication is based on physical access and it has no need to enter any secret value. Figure 2 illustrates an example of using this method where the enrollee button is pressed first. But it doesn't important which one is pressed first. In this method the registration protocol operates using a value of '00000000' for the Device Password. The WPS doesn't allow the external registrar to use this method to connect to the AP, so by using this method AP can't be the enrollee [11].

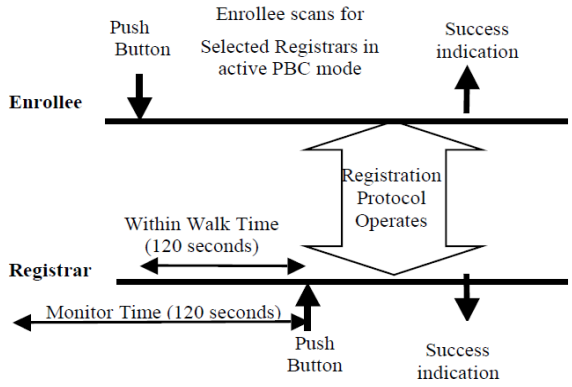

Fig. 2 An example of using PBC method

2.4 PIN code entry method

In this method authentication is based on the registration protocol and an 8-digit PIN code is used for the Device Password. This PIN code could be static and written on a label attached to the device or could change dynamically. In the case of headless devices (such as the AP) the last digit of the PIN code is used as a checksum. The algorithm for calculating this checksum is given below in C code:

```
bool ValidateChecksum(unsigned long int PIN)
{
unsigned long int accum = 0;
accum += 3 * ((PIN / 10000000) % 10);
accum += 1 * ((PIN / 1000000) % 10);
accum += 3 * ((PIN / 100000) % 10);
accum += 1 * ((PIN / 10000) % 10);
accum += 3 * ((PIN / 1000) % 10);
accum += 1 * ((PIN / 100) % 10);
accum += 3 * ((PIN / 10) % 10);
accum += 1 * ((PIN / 1) % 10);
return (0 == (accum % 10));
}
```

3. Previous attacks

3.1 Online brute force attack

The first practical attack against the WPS standard was introduced in 2011 by Stefan Viehböck [13]. The attacker attempts as the registrar to connect to AP which is the enrollee in this case and tries to guess the PIN code by an online brute-force attack. As shown in section 2.2, the registration protocol uses the PIN code in two parts. So the search space is limited to 10^4+10^4 = 10,000+10,000 = 20,000 that is not a large number. Also in the case of static PIN last digit is a checksum, and this decreases this number to 11,000.
The flow chart is shown in Figure 3.

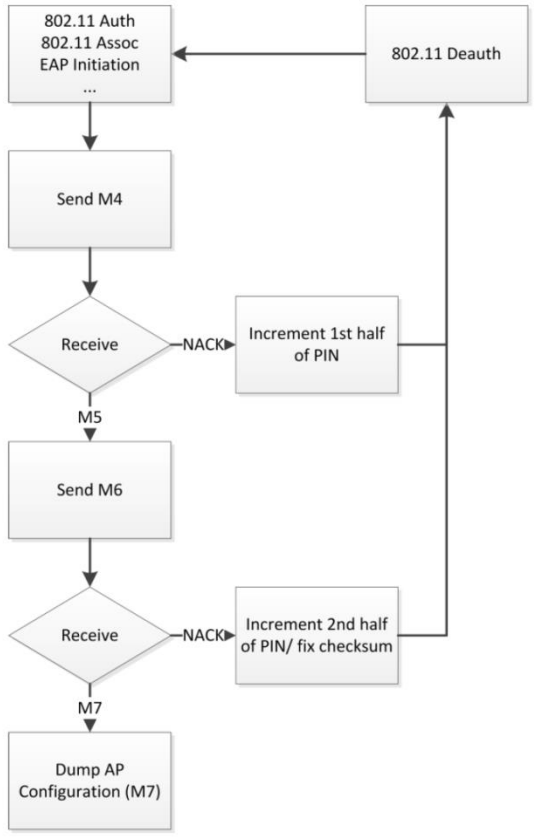

Fig. 3 Flow chart of the online brute force attack [13]

The AP sends EAP-NACK message after receiving invalid packet, and the attacker knows that his guess about the 1st half of the PIN was incorrect. For any guess the attacker should try to connect again and this makes the attack usually to take a long time. Bully [14] and Reaver [15] are implementations of this brute force attack.

3.2 Offline brute force attack

The second attack was announced in 2014 by Dominique Bongard [16]. The attack, like the previous attack is based on exhaustive search and is a brute force attack, with the exception that after obtaining the initial value, the attack is performed as offline. After receiving the message M_3 by the attacker, he knows E-Hash1, E-Hash2, PKE and PKR. If somehow he was able to obtain E-S1 and E-S2, he can launch an offline brute force attack. So this attack must be very faster, since it doesn't need to connect repeatedly to guess PIN value.
But how can obtain the E-S1 and E-S2. Bongard has examined AP's firmware configured by wireless equipment manufacturers and he got the E-S1 and E-S2 calculation method. For example, in most of Ralink products observed that these values are considered zero, or in some of AP's just after the restart, the values of the initial state using in the algorithm for calculating nonces are equal. By knowing this values attacker can launch an offline brute force attack to fine the PIN code easily. There is an implementation of this attack called as PixieWPS [17].

3.3 Countermeasures

Both described attacks have limitations. Given that the first attack needs an attempt to connect for any guess, it may last for hours or days. Besides, Wi-Fi equipment manufacturers in their next productions have tried to fix security problems. For example, in most of today routers, there is a prevention method against online brute force attack. Similarly, securing devices against the offline brute force attack is possible by a firmware update.

4. Proposed attacks

4.1 First attack

Our first attack is based on the imbalance in the registration protocol. In M_3 message, the enrollee sends E-Hash1 and E-Hash2 to the registrar. In the next message M_4, the registrar sends R-S1 alongside R-Hash1 and R-Hash2 to the enrollee. So at this point it's not possible to verify the authenticity by the registrar, because it requires two random values chosen by the enrollee (E-S1 and E-S2), but the enrollee has R-S1 and it's possible to verify registrar's knowledge of the first half of the PIN.
In two previous attacks, the attacker was the registrar and AP was the enrollee. But if the attacker could somehow change his role in this exchange and could be the enrollee, he can use two arbitrary values instead of E-Hash1 and E-Hash2 and sends it as M_3 message. As mentioned before, at this point it's not possible to verify the authenticity of these two values. So the victim accepts the message and sends M_4 message to the attacker. Now the attacker is able to extract R-S1 and now, he can launch an offline brute force attack to find the first 4 digits of the PIN code. To find the next 4 digit this process must be repeated.
In accordance with WPS, both AP and clients can be the enrollee or the registrar. But it seems creators are forced to have this imbalance, because finally one of the parties should verify first. So they tried to fix this vulnerability by authentication based on "Enrollee's Device Password" and the AP always should be the enrollee. This solution was unlike the definition of the enrollee and the registrar, but weaknesses were acceptably resolved. However, this weakness can still be used. We describe a scenario for using this weakness as follows.

4.1.1 The first attack scenario

The attack is in the presence of an AP and a connected client. First the attacker attempts to send de-authentication packets to the client and runs jamming on the radio channel or any other kind of denial-of-service attacks. Then he offers an AP with similar network specification (SSID and security type) and higher signal strength to induce the client to connect to this rogue network. Given that it's impossible to connect to real network, the user likely will try to connect to the fake AP. Thus the attacker can be the enrollee in the registration protocol and force the client to authenticate by PIN code again. Now it's possible to launch an offline brute force attack to find the first 4 digit of the PIN code.

4.2 Second attack

After announcing that WPS is unsecured, most researchers offered not using of the WPS standard. But we will show even with disabling WPS in Wireless equipment, it's possible to penetrate the network using its weaknesses. There is an attack called as *evil twin attack*, and occurs when a client forced to connect to an unsecured rogue AP with the same SSID to the real AP, as described above. The attacker prevents the client from access to real network by launching one of denial-of-service attacks. But the victim can detect the attack, since the rogue AP has *unsecured* security type and it shows, this is a fake AP. Our attack works in the case of using WPA/WPA2-PSK

security type for the fake AP and will not be any difference between the fake and the real AP in view of the victim.

The attack works in the presence of an AP and a client. The attacker runs jamming on the radio channel and stops the connection and offers a fake AP with the same network specification, similar to the first attack. The difference is that in this attack, it's not important the real AP supports WPS or not and it doesn't need to client use WPS to connect. The attacker sends out 802.11 beacons indicating support for the WPS and also PBC mode. After a while, the user attempts to connect again, but it's not possible to connect to the real network. If he attempts to connect to the fake AP, then he should enter a passphrase to establish 4-way handshake, since our fake AP has WPA/WPA2-PSK security type. The 4-way handshake is a strong mutual authentication method and it's not possible to accept any passphrase by the fake AP, because the client checks authenticity of the other party. But using weaknesses in the implementation of WPS in Windows operating system, it's possible to perform the attack.

Today in all versions of the Microsoft Windows operating system, attempting to connect to such a WPS supported AP, is equal to pushing the WPS button. It means pushing the WPS button in the Microsoft Windows is not optional. Figure 4 illustrates attempting to connect to a WPS supported AP in Microsoft Windows 8.

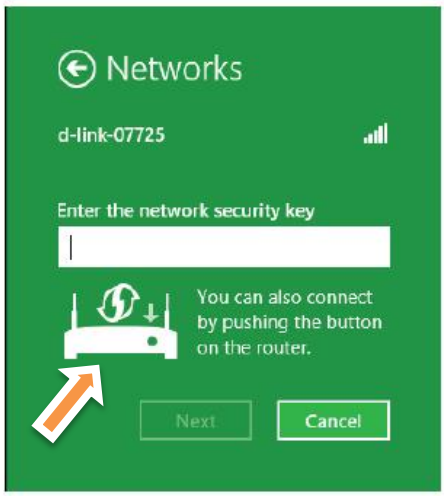

Fig. 4 attempting to connect to a WPS supported AP in Microsoft Windows 8.

So by attempting to connect, the registration protocol operates automatically and the client connects to rogue AP successfully.

5. Conclusions

The WPS standard has several weaknesses. Poor design of the registration protocol and also some mistakes in the implementation of this standard have made it as a threat to the security of Wi-Fi networks. This is a perfect example of the consequences that can make a weak standard. It seems the WPS must be disabled urgently by the users. The wireless equipment manufacturers should modify the firmware on their devices or stop using it completely. Also, all implementations of the standard should be reviewed and modified immediately.

References

[1] http://www.wi-fi.org/who-we-are
[2] https://en.wikipedia.org/wiki/Wi-Fi_positioning_system
[3] IEEE Std 802.11-1997 Information Technology-telecommunications And Information exchange Between Systems-Local And Metropolitan Area Networks-specific Requirements-part 11: Wireless Lan Medium Access Control (MAC) And Physical Layer (PHY) Specifications. 1997.
[4] Fluhrer, Scott, Itsik Mantin, and Adi Shamir. "Weaknesses in the key scheduling algorithm of RC4." Selected areas in cryptography. Springer Berlin Heidelberg, 2001.
[5] Borisov, Nikita. "Ian oldberg, and David Wagner. Intercepting Mobile Communications; The Insecurity of 802.11." Seventh Annual International Conference on Mobile Computing and Networking, Rome, Italy, Tuly. 2001.
[6] Stubblefield, Adam, John Ioannidis, and Aviel D. Rubin. "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP." NDSS. 2002.
[7] IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements available at http://standards.ieee.org/getieee802/download/802.11i-2004.pdf
[8] Tews, Erik, Ralf-Philipp Weinmann, and Andrei Pyshkin. "Breaking 104 bit WEP in less than 60 seconds." Information Security Applications. Springer Berlin Heidelberg, 2007. 188-202.
[9] Bittau, A., Handley, M., Lackey, J.: The Final Nail in WEP's Coffin Security and Privacy. In: IEEE Symposium on, pp. 386–400 (2006)
[10] Tews, Erik, and Martin Beck. "Practical attacks against WEP and WPA." Proceedings of the second ACM conference on Wireless network security. ACM, 2009.
[11] WiFi Protected Setup Specification 1.0h available at http://cfile28.uf.tistory.com/attach/16132E3C50FCFFCB3EC74E
[12]https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange
[13] Viehböck, Stefan. "Brute forcing wi-fi protected setup." Wi-Fi Protected Setup (2011).
[14] https://github.com/Lrs121/bully.git
[15] http://code.google.com/p/reaver-wps/
[16] Bongard, Dominique. "Offline bruteforce attack on WiFi Protected Setup." Presentation at Passwordscon (2014).
[17] https://github.com/wiire/pixiewps.git