Enhancing WPS Security

Dimitris Zisiadis, Spyros Kopsidas, Argyris Varalis, Leandros Tassiulas
Centre for Research & Technology Hellas (CERTH) & University of Thessaly
Volos, Greece
{dzisiadis, kopsidas, avaralis, leandros}@iti.gr

***Abstract*—The main concern on the use of wireless technologies is security, due to the nature of the medium. User awareness in order to implement efficient security configurations is an important requirement raised by the technology, undermining its use. Wireless Protected Setup (WPS) was introduced as a viable solution to the problem, offering automatic network setup and device configuration. WPS itself suffers from a security flaw; the feature has to be disabled on the devices and user confidence is subverted. In this work we propose to enhance WPS security through the Visual Device Pairing Security (ViDPSec) method to address this problem. ViDPSec is a user-based, lightweight device pairing protocol that establishes secure communication channels between devices, encrypting data with a one time symmetric key that is securely exchanged per session. Enhanced WPS alleviates the WPS security issues and enables the user to have full control over the procedure, raising user confidence.**

Wi-Fi; WPS; ViDPSec; wireless security

I. INTRODUCTION

Due to the nature of wireless technology, security is raised as the main barrier against their use, requiring special skills from the end user. On the other hand, users are accustomed to preconfigured devices that work right away as they get them of the shelf, without going into the bits and bytes of the provided service or the enabling technology. Wireless Protected Setup (WPS) was introduced to overcome this problem and make use of Wi-Fi technology easy to use for the end users, hiding the technology plane from the user plane [1]. Although promising, WPS itself suffers from security vulnerabilities, as proved recently in [2]. In the present work we propose the enhancement of WPS with the ViDPSec security handshake mechanism [3]. ViDPSec is a user-based device pairing protocol, enabling the establishment of a session symmetric key over unsecured wireless environments. ViDPSec enhancement alleviates the security flaw hampering WPS, enabling even inexperienced users to have full control over the exchange procedure, increasing user confidence on the use of the specific technology. This paper is organized as follows: an overview of In section 2 WPS fundamentals are described and its security flaw is explained while in section 3 Enhanced WPS is unveiled. Performance evaluation parameters are outlined in section 4 and finally concluding remarks are provided in section 5.

II. WIRELESS PROTECTED SETUP

The most common wireless security standards are Wired Equivalent Privacy (WEP) [4] and Wireless Protected Access (WPA) [5]. WPA2 [6], the successor of WPA, introduces CCMP [6], a new AES-based encryption mode with strong security [7]. WPA2 supports WPA but cannot support WEP. WPA2 is the current certification by the Wi-Fi Alliance and it is adopted in most WLANs today.

Wireless protected Setup (WPS) automatically configures the network's SSID and WPA2 security key, relieving users from having to understand the underlying technology of wireless security. There are two in-band configuration methods supported by WPS: Push Button Configuration (PBC) method and Personal Identification Number (PIN) method. Three descriptive roles are defined for these methods in order to illustrate the setup procedure: (a) **Enrollee** is the device seeking access to a WLAN, (b) **Registrar** is the device with the authority to issue and revoke access credentials to members of a WLAN, which may be integrated in an AP or it can run on another device and (c) **AP**, an Access Point that provides wireless connectivity between the Registrar and the Enrollee.

In the PBC method, users initiate the setup and configuration procedure by pressing buttons on both the AP and the client device. The buttons could be physical, located on the device, or virtual, displayed onscreen during setup. In the PIN method, WPS enabled devices have a factory installed PIN attached on the device or the PIN is dynamically generated and displayed onscreen. In the Internal Registrar PIN method the PIN has to be read from the Enrollee device, then entered at the web interface of the AP via the Registrar's device; upon successful PIN validation the WLAN is automatically configured and the Enrollee is enabled to access the WLAN. In the External Registrar PIN method the 8-digit PIN is read from the AP sticker, then entered to the client's-side via an onscreen interface; after PIN validation WLAN is properly setup with the relevant SSID and WPA2 key.

A. WPS Security Flaw

In December 2011 Stefan Viehbock presented an implementation flaw on the PIN method with External Registrar, where the 8-digit PIN of the AP is revealed after a brute-force type of attack. Fig. 1 outlines the protocol message exchange as illustrated in Stefan Viehbock's paper, following Microsoft's WCN specification [8]. The attack exploits the WPS authentication scheme, which is based on the PIN alone and therefore is prone to brute force attacks. When WPS authentication fails, as is the case when the AP's PIN keyed in the device's screen doesn't match the actual PIN on the AP sticker, a negative acknowledgement on PIN validity is sent from the AP (EAP-NACK).

IEEE 802.11			
	Supplicant → AP	Authentication Request	802.11 Authentication
	Supplicant ← AP	Authentication Response	
	Supplicant → AP	Association Request	802.11 Association
	Supplicant ← AP	Association Response	
IEEE 802.11/EAP			
	Supplicant → AP	EAPOL-Start	EAP Initiation
	Supplicant ← AP	EAP-Request Identity	
	Supplicant → AP	EAP-Response Identity (Identity: "WFA-SimpleConfig-Registrar-1-0")	
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	
M4	Enrollee ← Registrar	N1 || R-Hash1 || R-Hash2 || $E_{KeyWrapKey}$(R-S1) || Authenticator	proove posession of 1st half of PIN
M5	Enrollee → Registrar	N2 || $E_{KeyWrapKey}$(E-S1) || Authenticator	proove posession of 1st half of PIN
M6	Enrollee ← Registrar	N1 || $E_{KeyWrapKey}$(R-S2) || Authenticator	proove posession of 2nd half of PIN
M7	Enrollee → Registrar	N2 || $E_{KeyWrapKey}$(E-S2 ||ConfigData) || Authenticator	proove posession of 2nd half of PIN, send AP configuration
M8	Enrollee ← Registrar	N1 || $E_{KeyWrapKey}$(ConfigData) || Authenticator	set AP configuration

Enrollee = AP
Registrar = Supplicant = Client/Attacker

PK_E = Diffie-Hellman Public Key Enrollee
PK_R = Diffie-Hellman Public Key Registrar
Authkey and KeyWrapKey are derived from the Diffie-Hellman shared key.

Authenticator = $HMAC_{AuthKey}$(last message || current message)

$E_{KeyWrapKey}$ = Stuff encrypted with KeyWrapKey (AES-CBC)

PSK1 = first 128 bits of $HMAC_{AuthKey}$(1st half of PIN)
PSK2 = first 128 bits of $HMAC_{AuthKey}$(2nd half of PIN)

E-S1 = 128 random bits
E-S2 = 128 random bits
E-Hash1 = $HMAC_{AuthKey}$(E-S1 || PSK1 || PK_E || PK_R)
E-Hash2 = $HMAC_{AuthKey}$(E-S2 || PSK2 || PK_E || PK_R)

R-S1 = 128 random bits
R-S2 = 128 random bits
R-Hash1 = $HMAC_{AuthKey}$(R-S1 || PSK1 || PK_E || PK_R)
R-Hash2 = $HMAC_{AuthKey}$(R-S2 || PSK2 || PK_E || PK_R)

Figure 1. External Registrar message sequence.

Moreover, the PIN is verified in halves, sized at four bits each, where the last digit of the second half is the checksum of the first seven bits. Thus, it only takes eleven thousands (10^4+10^3) attempts to figure out the AP's PIN instead of the expected one hundred millions (10^8) based on the PIN's length. As stated by the author, the attack exploits poor design in PIN verification and the EAP-NACK messages sent from the AP after steps M4 and M6, when an invalid PIN is provided.

III. ENHANCED WPS

ViDPSec [4] can be used to enhance WPS security. ViDPSec is a user-based device pairing protocol for the establishment of secure data exchange over unsecure channels. It is both lightweight and sophisticated yet easy to us, relying on human visual out-of-band verification to establish a Session Symmetric Key (SSK) that encrypts all exchanged data between the devices. For the SSK, any available symmetric algorithm can be used (3DES, AES, etc.); in this case a 256 AES based key is considered safe for the moment. One-time public cryptography keys are used to securely exchange the SSK over the unsecure channel. The aforementioned procedure ensures that no attack has taken place, ensuring channel security. Fig. 2 outlines the operation of the protocol. ViDPSec can be used to address the security breach discovered by Stefan Viehbock and enhance WPS security overall. The External Registrar PIN method as defined in WPS has a number of flaws:

1) Diffie–Hellman vulnerability: Diffie-Hellman is proven to be a weak security handshake method [9].

2) Physical PIN theft: The static PIN attached on the AP is problematic, as anyone with one time physical proximity to the AP can copy the PIN and therefore take ownership of the WLAN settings then after.

Device 1		Device 2
Start pairing procedure Produce P_1, C_1, N_1 Produce DSS_1		Start pairing procedure Produce P_2, C_2, N_2 Produce DSS_2
Receive DSS_2	Hello (DSS_2) ←	Send DSS_2
Send DSS_1	Hello (DSS_1) →	Receive DSS_1
Receive C_2 Extract N2 Calculate $SUM_1=N_1+N_2$	SENDKEY (C_2) ←	Send C_2
Send C_1	SENDKEY (C_1) →	Receive C_1 Extract N_1 Calculate $SUM_2=N_2+N_1$
Send encrypted SSK (SSK * C_2)	SEND_SYMMETRIC (Encrypted SSK) →	Receive Encrypted SSK Calculate SSK
Prompt User: SUM_1		Prompt User: SUM_2
User Verification: SUM_1 ==SUM_2		
User selects "OK" Encrypt Data with SSK	↔	User selects "OK" Encrypt Data with SSK

N = A 4-digit random number
DSS = N * P
SUM = N1+N2

P = Private Key.
C: Public (Common) Key.
SSK = Symmetric Session Key.

Figure 2. ViDPSec pairing procedure.

3) Typo sensitive: PIN entry typing errors are common and quite onerous, especially for novice users.

4) Brute Force attack vulnerability: The External Registrar PIN method is known to be vulnerable to brute force attack.

We propose the Enhanced WPS PIN method by introducing a ViDPSec security handshake phase with dynamic PIN and user acknowledgement. The requirement posed by our solution is a (relatively low cost) small LED display on the AP side along with the SUM verification button. The LED is used to display the dynamic PIN and the perceived sum on the AP side. Fig. 3 illustrates graphically the operational scenario. The WPS External Registrar PIN method is revised as follows:

1) Step 1 – Random number on device: A four-digit number is generated on the Enrollee, displayed on the relevant user screen. The Enrollee computes its signature DSS_E and sends it over to the AP.

2) Step 2 - Dynamic AP PIN: Upon DSS_E receipt, a dynamic four-digit PIN is generated on the AP (Enrollee), displayed on the LED. The PIN has a session lifetime and it is regenerated for every other session. DSS_{AP} is computed and sent to Registrar.

3) Step 3 - Pubic key exchange: The Enrollee and the AP exchange their one time Public Keys for this session (C_E and C_{AP} respectively).

4) Step 4 - SSK exchange: AP sends the Session Symmetric Key (SSK) to the Enrollee, encrypted with Enrollee's Publik Key (SSK * C_E).

5) Step 5 - Sum verification: The perceived sum is calculated on both ends, displayed on the AP LED and on the user screen. Users only have to acknowledge sum equality to complete pairing. Upon acknowledgement, the Session Symmetric Key (SSK) is established.

6) Step 6 - WLAN configuration: WLAN settings are exchanged over the secure channel established above. AP configuration (SSID and WPA2 key) is securely communicated between the parties, encrypted with the SSK.

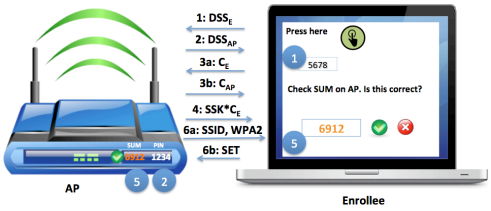

Figure 3. Enhanced WPS External Registrar.

The solution as presented requires from the AP to be equipped with a small LED to display the PIN and SUM values and a button for SUM acknowledgement. A more generic form of the application, lifting any hardware requirements is illustrated in Fig. 5, where the Registrar connects to both the AP and the Enrollee and two views are open simultaneously for the AP and the Enrollee respectively. The user is prompted to initiate Enhanced WPS by pressing the relative buttons, next the two random PINs (N_i) are automatically generated and the perceived sums are calculated and displayed in the views. The user is prompted to verify equality of the perceived sums. In case of disparity the channel is insecure and the pairing procedure fails whereas equal sums indicate that the pairing procedure succeeded and all WPS credentials can be securely exchanged. Static AP PINs are also supported, where SUM computation is based on the Enrollee random number and the static AP PIN.

IV. Performance Evaluation

The main difference to the original WPS approach is the human intervention for creation/verification of the perspective values (random, sum). The performance data of our solution indicate that it is feasible to employ it without performance degradation as: (1) the number of steps is actually reduced (by one), (2) we do not use time-consuming hashing, (3) SSK generation time is approximately 1 msec, and (4) asymmetric key generation time is approximately 150 msec.

IEEE 802.11			
	Enrollee → AP	Authentication Request	802.11 Authentication
	Enrollee ← AP	Authentication Response	
	Enrollee → AP	Association Request	802.11 Association
	Enrollee ← AP	Association Response	
IEEE 802.11/EAP			
	Enrollee → AP	EAPOL-Start	EAP Initiation
	Enrollee ← AP	EAP-Request Identity	
	Enrollee → AP	EAP-Response Identity (Identity: "WFA-SimpleConfig-Registrar-1-0")	
IEEE 802.11/EAP Expanded Type			
M1	AP ← Enrollee	N_1 || Description || DSS_E	DSS signature exchange
M2	AP → Enrollee	N1 || N_2 || Description || DSS_{AP} || Authenticator	
M3	AP ← Enrollee	N_2 || C_E || Authenticator	Extract N_E Calculate $SUM_{AP} = N_{AP} + N_E$
M4	AP → Enrollee	N_1 || C_{AP} || Authenticator	Extract N_{AP} Calculate $SUM_E = N_E + N_{AP}$
User verification $SUM_E == SUM_{AP}$			
M5	AP → Enrollee	N_1 || ($SSK*C_E$) || Authenticator	SSK exchange
M6	AP → Enrollee	N_1 || (ConfigData*SSK) || Authenticator	Send AP configuration
M7	AP ← Enrollee	N_2 || (ConfigData*SSK) || Authenticator	Set AP configuration

N_E = Random 4-digit number Enrollee. N_{AP} = Random 4-digit number AP.
$DSS_E = N_E * P_E$ $DSS_{AP} = N_{AP} * P_{AP}$
C_E = Asymmetric Public key Enrollee. C_{AP} = Asymmetric Public key AP.
SUM_E, SUM_{AP} = Perceived sums of N_E and N_{AP}. SSK = Symmetric Session Key.

Figure 4. Enhanced WPS message exchange.

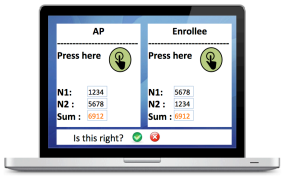

Figure 5. Enhanced WPS External Registrar, generic.

This delay can be avoided, by having the keys pre-generated, in which case, apart from the human interaction delay, our solution is lighter than the original.

V. Conclusions

In the present work we propose the use of ViDPSec as a security handshake method to overcome the security flaw identified recently on WPS External Registrar method and to enhance the WPS PIN method overall. The method is effective and user friendly. It requires from users to acknowledge a small number through the visual channel, alleviating the need for typing, where mistakes are quite often, especially from novice or elder users. The use of dynamic PINs makes the use of WPS resistant to PIN theft attempts, where an attacker needs to have physical presence only once in order to breach security then after. Dynamic PINs also ensure security from eavesdropping when the same PIN is frequently used. Finally, it raises user confidence, as the procedure is user controlled with physical presence of the initiator for SUM acknowledgement. Our solution requires from the AP to have a small LED for PIN and SUM display along with the SUM acknowledgement button. A more generic software solution is also provided, lifting any hardware requirement and conforming to backward compatibility with existing APs.

Acknowledgements

This work is part of the project "Network of Excellence in Internet Science" ICT-FP7- 288021 NoE EINS, funded by the European Commission.

References

[1] WiFi Alliance, "Wi-Fi Simple Configuration Technical Specification v2.0.2"

[2] S. Viehböck, "Brute forcing Wi-Fi Protected Setup," Dec. 26, 2012.

[3] D. Zisiadis, S. Kopsidas and L. Tassiulas, "ViDPSec: Visual Device Pairing Security Protocol," CSE '09, Aug. 2009, pp. 359-364.

[4] ANSI/IEEE Std 802.11, 1999 Edition, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," USA 1999.

[5] "Wi-Fi_Protected_Access", Wi-Fi Alliance, http://www.wi-fi.org/knowledge_center/wpa/

[6] IEEE, "IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements," IEEE, Piscataway, USA 2004.

[7] 7 Federal Information Processing Standards Publication 197 nnouncing the ADVANCED ENCRYPTION STANDARD (AES)," Nov. 26, 2001.

[8] Microsoft Connect Now Net, Dec.8, 2006 http://download.microsoft.com/download/a/f/7/af7777e5-7dcd-4800-8a0a-b18336565f5b/WCN-Netspec.doc

[9] J-F. Raymond and A. Stiglic," Security Issues in the Diffie-Hellman Key Agreement Protocol," IEEE Trans. on Information Theory 2000, pp. 1-17.