Brute forcing Wi-Fi Protected Setup

When poor design meets poor implementation.

26.12.2011
Version 3
Traducción: Chumpy
Para: seguridadwireless.net

Stefan Viehböck
https://twitter.com/sviehb
http://sviehb.wordpress.com/

Introduction

"Wi-Fi Protected Setup™ es un programa de certificación opcional de la Wi-Fi Alliance diseñado para facilitar la tarea de crear y configurar la seguridad de una red inalámbrica de área local. Introducida a principios de 2007, el programa provee un configuración de redes para horgares y pequeñas empresas (SOHO).

Wi-Fi Protected Setup permite a los usuarios que habitualmente tienen reducidos conocimientos en la configuración de redes Wi-Fi la creación de nuevas redas inalámbricas y la instalación de nuevos dispositivos con sus correspondientes medidas de seguridad. Más de 200 productos han sido certificados por Wi-Fi CERTIFIED™ para Wi-Fi Protected Setup desde que el programa se lanzó en enero de 2007.

Wi-Fi Simple Configuration Specification (WSC) es la tecnología bajo Wi-Fi Protected Setup certification.

Practicamente todos los principales fabricantes (incluyendo Cisco/Linksys, Netgear, D-Link, Belkin, Buffalo, ZyXEL y Technicolor) tienen dispositivos WPS-certified, otros fabricantes (ej. TP-Link) tienen dispositivos con WPS-support que no son WPS-certified.

WPS está activado por defecto en todos los dispositivos a los que he accedido.

Aunque WPS está considerado como un sistema seguro para configurar dispositivos inalámbrios hay errores de diseño e implementación que permiten a un atacante obtener acceso a una red que de otra forma sería suficientemente segura.

Opciones de Configuración

WPS soporta la configuración fuera de la red inalámbrica sobre Ethernet/UPnP (también NFC es mencionado en las especificaciones) y la configuración desde la red inalámbrica sobre IEEE 802.11/EAP. Este escrito solo tratará la configuración desde la red inalámbrica.

Terminología[2]

- ***Registrar(Registrador)***: dispositivo con la autoridad de generar o revocar las credenciales en la red. Tanto un AP como cualquier otra estación o PC de la red pueden actuar de *Registrar*. Puede haber más de un *Registrar* en una red.
- ***Enrollee (cliente o afiliado)***: dispositivo que solicita el acceso a la red WLAN.
- ***Authenticator(Autentificador o Punto de Acceso)***: AP funcionando de proxy entre el *Registrar* y el *Enrollee*.

[1] http://www.wi-fi.org/wifi-protected-setup/
[2] http://download.microsoft.com/download/a/f/7/af7777e5-7dcd-4800-8a0a-b18336565f5b/WCN-Netspec.doc
N.t.: SOHO del ingles Small Ofices, Home Ofices, puede ser traducido como "microempresas" el termino PYMES (Pequeñas Y Medianas EmpresaS) hace referencia a empresas algo más grandes que las SOHO.

Push-Button-Connect ("PBC")

Los usuarios tienen que pulsar un boton, que puede ser físico o virtual, tanto en el AP como en el nuevo dispositivo cliente. PBC estará activado únicamente hasta que se complete la autentificación o pasen dos minutos.

This Option is called **wps_pbc** in wpa_cli[3] (text-based frontend program for interacting with wpa_supplicant).

Firgura 1: activado "virtual Push Button" (Windows actúa como "enrollee") (Windows 7)

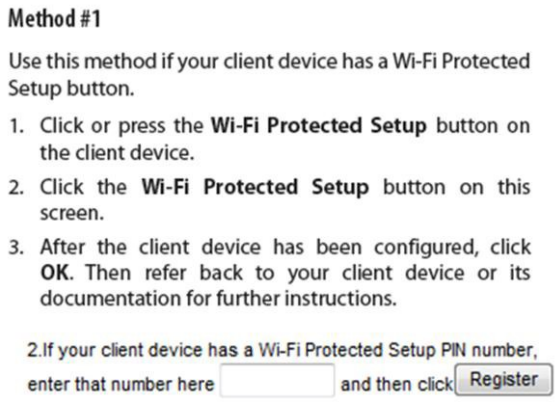

Figura 2: Descripión de un PBC (Linksys WRT320N User Manual)

PIN

Internal Registrar

El usuario tiene que introducer el PIN del adaptador Wi-FI en la interfaz web del AP. El PIN puede estar impreso en la etiqueta del adaptador o ser generado por software.
Está opción se llama **wps_pin** en wpa_cli.

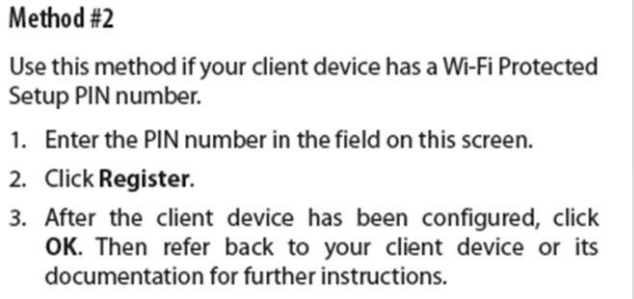

Figura 3: Descripión de "PIN internal Registrar" (Linksys WRT320N User Manual)

Figura 4: campo PIN – Router es "Registrar" (Linksys WRT320N Web Interface)

[3] http://hostap.epitest.fi/wpa_supplicant/

External Registrar

El usuario tiene que introducir el PIN del AP a petición del dispositivo cliente (ej. Ordenador)
Esta opción se llama **wps_reg** en wpa_cli.

Method #3

Use this method if your client device asks for the Router's PIN number.

1. Enter the PIN number listed on this screen. (It is also listed on the label on the bottom of the Router.)
2. After the client device has been configured, click **OK**. Then refer back to your client device or its documentation for further instructions.

Figura 5: Descripción de "PIN external Registrar" (Linksys WRT320N User Manual)

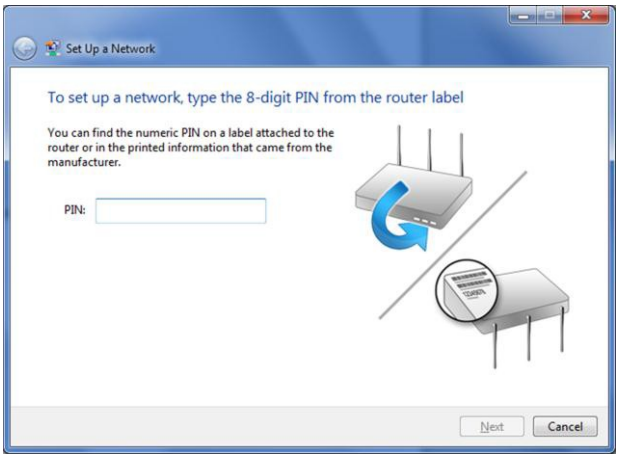

Figura 6: "Windows Connect Now Wizard" actuando como "Registrar" (Windows 7)

Figura 7: Etiqueta con WPS PIN bajo un router D-Link

Error de Diseño #1

Option / Authentication	Physical Access	Web Interface	PIN
Push-button-connect	X		
PIN – Internal Registrar		X	
PIN – External Registrar			X

Opción WPS y que timo de autentificación utilize.

Como "External Registrar" no require ningún tipo de autentificación además de proveer el PIN es potencialmente vulnerable a ataque de fuerza bruta.

Authentication (PIN – External Registrar)[4]

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)

1	2	3	4	5	6	7	0
1st half of PIN				checksum 2nd half of PIN			

Si la autentificación WPS falla en algún momento el AP enviará un mensaje EAP-NACK.

[4] basado en http://download.microsoft.com/download/a/f/7/af7777e5-7dcd-4800-8a0a-b18336565f5b/WCN-Netspec.doc

Error de Diseño #2

Un atacante puede extraer información de las corrección de las partes del PIN a partir de las repuestas del AP.

- Si el atacante recibe un mensaje EAP-NACK después de enviar M4, sabe que la primera parte del PIN (1st half) era incorrecta.
- Si el atacante recibe un mensaje EAP-NACK después de enviar M6, sabe que la primera parte del PIN (2nd half) era incorrecta.

Esta forma de autentificación reduce dramaticamente los posibles intentos de autentificación necesarios de 10^8 (=100.000.000) a $10^4 + 10^4$ (=20.000).

Como el 8º digito del PIN es siempre un checksum de los dígitos del primero al séptimo son como máximo necesarios $10^4 + 10^3$ (=11.000) intentos para encontra el PIN correcto.

Metodología de la Fuerza Bruta

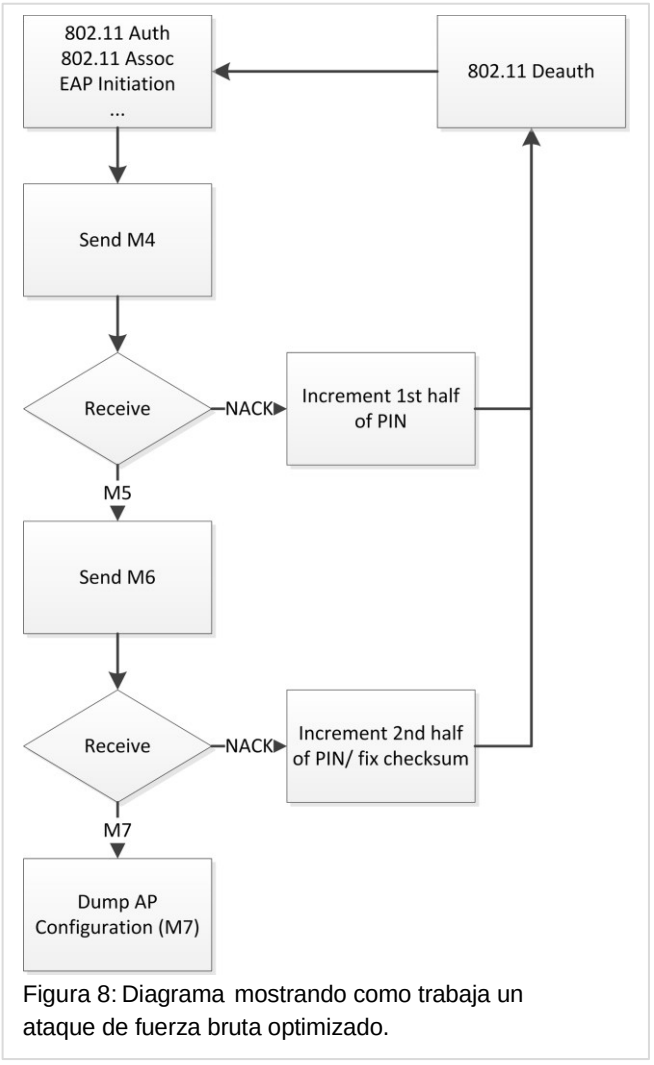

Figura 8: Diagrama mostrando como trabaja un ataque de fuerza bruta optimizado.

Implementación del Ataque de Fuerza Bruta

Una prueba de concepto de una herramienta de fuerza bruta fue implementada en Pyton. Utiliza la librería Scapy[5] para la decodificación, generación, envío y recepción de los paquetes. Esta herramienta fue usada en varios routers de diferentes fabricantes.

Sample output

```
sniffer started

trying 00000000
attempt took 0.95 seconds
trying 00010009
attempt took 1.28 seconds
trying 00020008
attempt took 1.03 seconds

<snip>

trying 18660005
attempt took 1.08 seconds
trying 18670004              # found 1st half of PIN
attempt took 1.09 seconds
trying 18670011
attempt took 1.08 seconds
trying 18670028
attempt took 1.17 seconds
trying 18670035
attempt took 1.12 seconds

<snip>

trying 18674071
attempt took 1.15 seconds
trying 18674088
attempt took 1.11 seconds

trying 18674095              # found 2nd half of PIN
E-S2:
0000   16 F6 82 CA A8 24 7E 98  85 4C BD A6 BE D9 14 50   .....$~..L.....P
SSID:
0000   74 70 2D 74 65 73 74                              tp-test
MAC:
0000   F4 EC 38 CF AC 2C                                 ..8.,
Auth Type:
0000   00 20                                             .
Encryption Type:
0000   00 08                                             ..
Network Key:
0000   72 65 61 6C 6C 79 5F 72  65 61 6C 6C 79 5F 6C 6F   really_really_lo
0010   6E 67 5F 77 70 61 5F 70  61 73 73 70 68 72 61 73   ng_wpa_passphras
0020   65 5F 67 6F 6F 64 5F 6C  75 63 6B 5F 63 72 61 63   e_good_luck_crac
0030   6B 69 6E 67 5F 74 68 69  73 5F 6F 6E 65            king_this_one
Key Wrap Algorithm:
0000   76 3C 7A 87 0A 7D F7 E5                           v<z..}..
```

[5] http://www.secdev.org/projects/scapy/

Resultados

Duración de los intentos de Autentificación

Un intento de autentificación llevó normalmente entre 0.5 y 3 segundos para completarse. Se observe que el cálculo de la "Diffie-Hellman Shared Key" (que necesita ser realizado antes de la generación de M3) en el AP lleva una buena parte del tiempo de autentificación. Esto puede ser acelerado eligiendo una Clave Pública DH muy pequeña y hacienda el cálculo de la Clave Compartida, en el lado del AP, más sencillo.

Errores de Implementación

Algunos fabricantes no han implementado ningún tipo de mecanismo de bloqueo para prevenir ataques de fuerza bruta. Esto permite a un atacante probar todas las posibles combinaciones de PIN en menos de cuatro horas (a 1.3 segundos/intento).

En promedio un ataque se completará en la mitad del tiempo.

Los dispositivos Netgear tienen implementado un bloqueo, sin embargo las fases de bloque no son lo suficientemente largas para hacer el ataque inviable. En este caso el ataque será completado, en promedio, en menos de un día (una tabla de tiempo se puede encontrar en la siguiente página).

Vendor	Device Name	HW-Version	FW-Version	Lock down	WPS-certified
D-Link	DIR-655	A4 (Web Interface) A5 (Label)	1.35	No	Yes
Linksys	WRT320	1.0	1.0.04	?[6]	Yes
Netgear	WGR614v10	?	1.0.2.26	Yes	Yes
TP-Link	TL-WR1043ND	1.8	V1_110429	No	No

Versiones de Firmware actualizadas a la fecha de 18.10.2011.

Excepcionalmente algunos dispositivos empezaron a enviar mensajes malformados o sus interfaces web y enrutamientos dejaron de funcionar correctamente. Fue necesario reiniciarlos para resolver el problema. Esto puede ser evidencia de algún tipo de corrupción, pero no ha sido investigado.

[6] WPS-functionality siempre se detenía en algún moento entre 2 y 150 intentos de autentificación fallidos. La funcionalidad no ser recuperaba incluso después de varias horas. Considero esto un bug en el firmware que causa un DoS más que una funcionalidad de bloqueo.

Mitigaciones

Usuarios Finales

Desactivar WPS. Puede no ser siempre posible.

Fabricantes

Introducir periodos de bloqueos suficientemente largos para hacer un ataque inviable. Por supuesto esto require publicar un Nuevo firmware.

Intentos antes del bloqueo	Tiempo de bloqueo	Intentos por minuto	Maximo tiempo de ataque	Maximo tiempo de ataque	Comentarios
11000	0 minutes	46.15	3.97 hours	0.17 days	Sin bloqueo
?[7]		4.20	43,65 hours	1,82 days	Netgear WGR614v10
3	1 minutes	2.82	65.08 hours	2.71 days	Requerimiento para WSC 2.0
15	60 minutes	0.25	737.31 hours	30.72 days	Configuración de bloqueo haciendo el ataque inviable
10	60 minutes	0.17	1103.97	46.00 days	
5	60 minutes	0.08	2203.97	91.83 days	

Tiempo asumido por ataque: 1.3 seconds

Considerando que un AP normalmente trabaja durante varios meses, un determinado atacante podría completar con éxito un ataque a un AP con WPS activado. Este ataque es de bajo coste y tiene una alta garantía de éxito comparado con crakear una clave WPA/WPA2-PSK.

Conclusión

Como practicamente todos los fabricantes de routers/AP tiene dispositivos WPS-certified y WPS – PIN (External Registrar) es obligatorio para la certificación, podemos esperar que muchos dispositivos son vulnerable a este tipo de ataque.

Tener un tiempo de bloque no es practicamente un requerimiento para la certificación. Sin embargo puede ser un requerimiento en la (nueva) WSC Specification Version 2[8]. He contactado con la Wi-Fi Alliance sobre esto - aún no me han respondido.

Será necesaria la colaboración con los fabricantes para identificar todos los dispositivos vulnerable. Está en manos de los fabricantes el implementar mitigaciones y la publicación de un nuevo firmware.

Los usuarios finales afectados tendrán que ser informados sobre esta vulnerabilidad y ser recomendados que desactiven WPS o actualicen su firmware a una vesión más segura (si está disponible).

[7] No se encontró un patrón de bloqueo consistente. Sin embargo una media de 4.20 intentos de autentificación por minuto fueron posibles.

[8] http://www.wi-fi.org/files/20110421_China_Symposia_full_merge.pdf