

Wi-Fi Protected Setup

Úvod

Wi-Fi Protected Setup (ďalej už len WPS) je bezpečnostný štandard zavedený v roku 2006. Jeho cieľom bolo uľahčiť laickej verejnosti proces správy a zabezpečenia domácej bezdrôtovej siete. V roku 2011 sa ukázalo, že disponuje veľkou trhlínou, nakoľko umožňuje potenciálnemu útočníkovi získať WPS PIN v priebehu pár hodín, a to za pomoci brute-force. Po uhádnutí PINu zariadenie posiela konfiguračný packet aj s WPA/WPA2 pre-shared key. V dnešnej dobe je bohužiaľ na väčšine zariadení WPS defaultne zapnuté a na niektorých dokonca ani nie je možné vypnúť ho.

Metódy pripojenia

Access-pointy certifikované WPS musia umožňovať minimálne dva spôsoby pripojenia:

1. wps_pin/wps_reg - prečítaním PINu na štítku/displeji registrátora a jeho zadaním u zapisovaného zariadenia alebo vice-versa,
2. wps_pbc - stlačením tlačidla v jeden moment ako na access-pointe, tak na klientovi (stlačenie môže byť aj virtuálne).

Útok technikou brute-force

Dĺžka PINu je daná štandardom takisto ako spôsob jeho overovania. Poslednú číslicu osemmiestneho PINu tvorí checksum, čím sa počet možných kombinácií ustáľuje na 10^7 . Pri overovaní tohto kódu však registrátor osobitne odpovedá na správnosť hornej polovice a osobitne spodnej polovice číslic. Tým sa počet nutných kombinácií na vyskúšanie znižuje na 11.000 a možný čas na prelomenie pod štyri hodiny. Príslušné programy demonštrujúce túto slabinu je možné nájsť pod názvami WPSCrack či Reaver-WPS. Pri využití Diffie-Hellmana a optimalizovaného algoritmu trvá jedna autentifikácia 0,5 až 3 sekundy.

Riešenie

Aj napriek tomu, že o probléme sa verejne vie a postihuje väčšinu dnes používaných zariadení, neprišlo sa ešte na jeho praktické riešenie. Súčasťou nových špecifikácií by malo byť zavedenie lock-down doby, ktorá by skúšanie kódu urobila časovo nevýhodným. To by so sebou však obnášalo aktualizáciu firmware, ktorá je u bežných užívateľov nevyužívaná. Poslednou možnosťou teda ostáva osвета koncových užívateľov s radou, aby si WPS pri prvej konfigurácii access-pointu hneď vypínali.

Algoritmus

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	prove posession of 1 st half of PIN
M5	Enrollee → Registrar	N2 E _{KeyWrapKey} (E-S1) Authenticator	prove posession of 1 st half of PIN
M6	Enrollee ← Registrar	N1 E _{KeyWrapKey} (R-S2) Authenticator	prove posession of 2 nd half of PIN
M7	Enrollee → Registrar	N2 E _{KeyWrapKey} (E-S2 ConfigData) Authenticator	prove posession of 2 nd half of PIN, send AP configuration
M8	Enrollee ← Registrar	N1 E _{KeyWrapKey} (ConfigData) Authenticator	set AP configuration

<p>Enrollee = AP Registrar = Supplicant = Client/Attacker</p> <p>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.</p> <p>Authenticator = HMAC_{Authkey}(last message current message)</p> <p>E_{KeyWrapKey} = Stuff encrypted with KeyWrapKey (AES-CBC)</p>	<p>PSK1 = first 128 bits of HMAC_{AuthKey}(1st half of PIN) PSK2 = first 128 bits of HMAC_{AuthKey}(2nd half of PIN)</p> <p>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)</p> <p>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)</p>
---	--

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

If the WPS-authentication fails at some point, the AP will send an EAP-NACK message.

