

Sans-fil : attaques contre les mécanismes de randomisation d'adresses MAC des terminaux

ESIR 3 - SSD

Valentin Conseil, Matthias Le Yhuelic, Valentin Lion
12 février 2019

Plan

1. Le système de randomisation d'adresses MAC
 - a. Le problème du pistage
 - b. Mécanisme de randomisation d'adresse MAC
2. Contournement des mécanismes de randomisation
 - a. Passif
 - b. Actif



Le système de randomisation d'adresses MAC

L'adresse MAC dans un réseau IEEE 802.x

Adresse unique sur 6 octets : 01:23:45:67:89:ab

Permet d'identifier un appareil sur un réseau

Transmise à chaque trame

Une donnée personnelle selon la RGPD



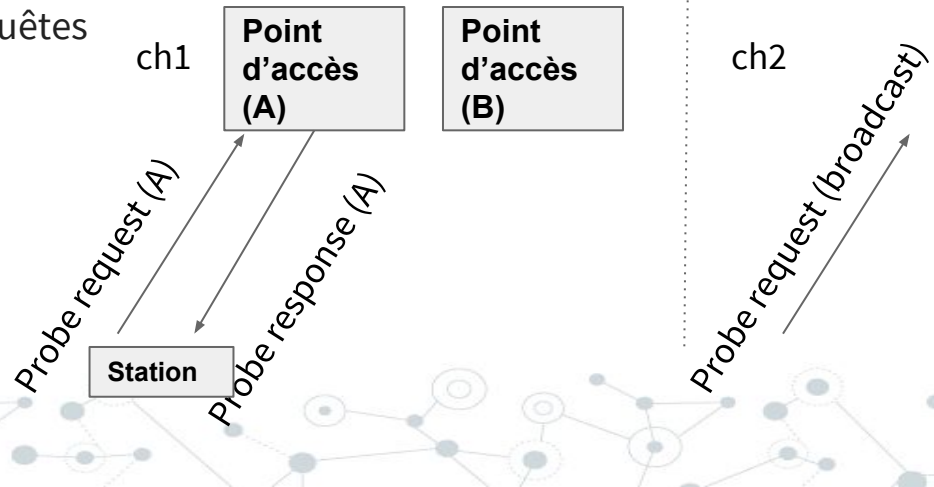
Le système de randomisation d'adresses MAC

Risque de pistage physique

Chaque appareil équipé d'une antenne Wifi émet en continue des probe request

But : signaler la présence de l'appareil et rechercher un réseau pour se connecter

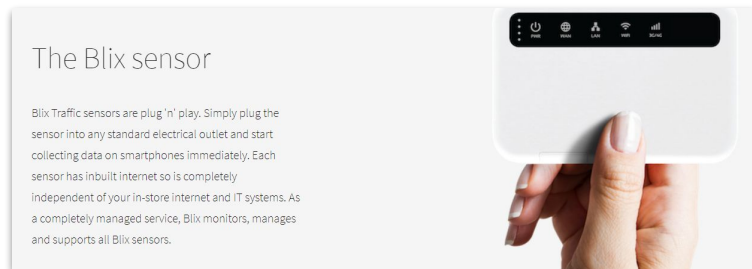
Envoi de l'adresse MAC dans ces requêtes



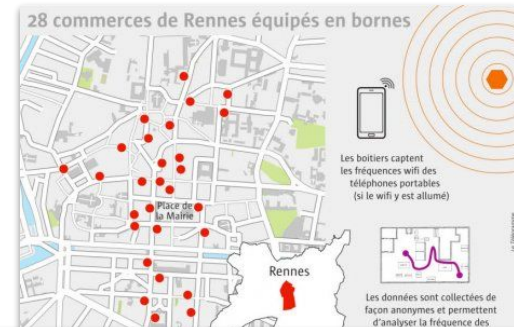
Le système de randomisation d'adresses MAC

Risque de pistage physique

Possibilité de pister les appareils en stockant les adresses MAC
But : Suivre à la trace une personne



Comment s'en protéger ?



“Visiteurs uniques, fréquence des visites, durée, heures d'arrivée et de départ, flux et parcours visiteurs... Le système permet même d'identifier les zones de chaleur dans la boutique”

Mécanisme de randomisation d'adresse MAC

Le principe

Remplacer fréquemment l'adresse MAC par une nouvelle choisie aléatoirement

Mécanisme mis en place depuis 2014 mais pas de standardisation

Complexes à mettre en place pour assurer la compatibilité hardware



Mécanisme de randomisation d'adresse MAC

Android	iOs	Windows	Linux
<p>Depuis Android 6.0</p> <p>Lorsque l'appareil n'est pas associé + possibilité de l'activer lors de la connexion (Android P)</p> <p>DA:A1:19</p> <p>Si le driver et le matériel supporte la randomisation</p> <p>Dépend du constructeur</p>	<p>Depuis iOS 8</p> <p>Complètement random</p> <p>Obscur</p>	<p>Depuis Windows 10</p> <p>Lorsque l'appareil n'est pas associé et lors de la connexion</p> <p>addr = SHA-256(SSID, macaddr, connId, secret)[:6]</p> <p>Si le driver et le matériel supporte la randomisation</p>	<p>Depuis le kernel 3.8</p> <p>Lors du scan wifi</p> <p>Différentes à chaque scan</p> <p>Exemple de Tail, qui choisit une adresse fixe à chaque boot</p>



2 - Contournement des mécanismes de randomisation



Retrouver l'adresse MAC

Randomisation encore peu répandue, support logiciel mais pas matériel

Algorithmes de randomisation parfois inefficace:

- adresses aléatoires réutilisées
- scan avec sa vraie adresse MAC

Protocole WPS : requête contient un UUID généré à partir de l'adresse MAC



Numéros de séquence

Numéros de séquence se suivent et révèlent d'un changement d'adresse MAC

62.303819	d2:cc:8c:c8:94:1a	Broadcast	802.11	131	Probe Request, SN=2609,
62.359162	d2:cc:8c:c8:94:1a	Broadcast	802.11	131	Probe Request, SN=2610,
78.282951	f6:0b:d9:19:9a:eb	Broadcast	802.11	141	Probe Request, SN=2617,
78.284922	f6:0b:d9:19:9a:eb	Broadcast	802.11	142	Probe Request, SN=2618,
78.286251	f6:0b:d9:19:9a:eb	Broadcast	802.11	152	Probe Request, SN=2619,
78.287718	f6:0b:d9:19:9a:eb	Broadcast	802.11	145	Probe Request, SN=2620,



SSID

SSID contenu dans la requête

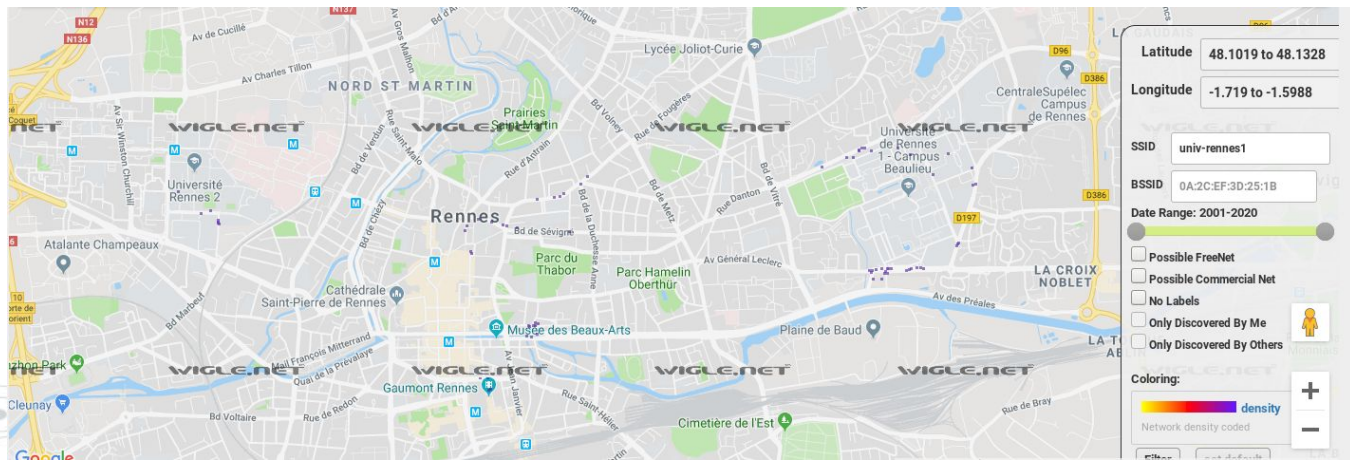
Titre subjectif peut révéler des informations

SSID privé sert d'identifiant unique

Nouveau mode de fonctionnement avec SSID nul qui fait que tout les réseaux répondent

25	4.554649818	26:6d:57:1f:e4:0d	Broadcast	802.11	110 Probe Request, SN=3285, FN=0, Flags=.....C, SSID=Wildcard (Broadcast
27	10.218752149	LiteonTe_1f:e4:0d	Broadcast	802.11	118 Probe Request, SN=3292, FN=0, Flags=.....C, SSID=FreeWifi
33	16.577848708	LiteonTe_1f:e4:0d	Broadcast	802.11	118 Probe Request, SN=3346, FN=0, Flags=.....C, SSID=FreeWifi

wigle.net



Démo de pistage par SSID

MAC

```
da:a1:19:f7:92:d1 : ['Livebox-73E7']  
44:6d:57:1f:e4:0d : ['Interstellar ']  
da:a1:19:7d:c5:d3 : ['Livebox-73E7']  
7c:2e:bd:24:93:2f : ['Bbox-FDE0711C']  
da:a1:19:a0:39:62 : ['Livebox-73E7']
```

SSID

```
Interstellar : ['44:6d:57:1f:e4:0d']  
Livebox-73E7 : ['da:a1:19:a0:39:62', 'da:a1:19:f7:92:d1', 'da:a1:19:7d:c5:d3']  
Bbox-FDE0711C : ['7c:2e:bd:24:93:2f']
```

Utilisation de Probequest



Information Elements

IEs tagged parameters

Informant des capacités de l'appareil

- débits supportés
- protocoles acceptés
- ...

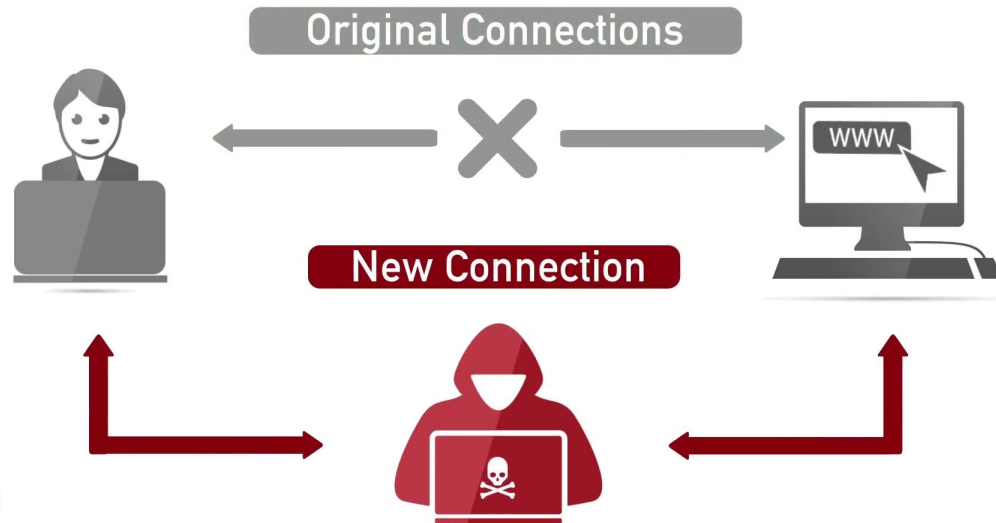
```
▼ IEEE 802.11 wireless LAN
  ▼ Fixed parameters (12 bytes)
  ▼ Tagged parameters (367 bytes)
    ▶ Tag: SSID parameter set: SFR-8fb8
    ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
    ▶ Tag: DS Parameter set: Current Channel: 11
    ▶ Tag: ERP Information
    ▶ Tag: ERP Information
    ▶ Tag: RSN Information
    ▶ Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
    ▶ Tag: QSS Load Element 802.11e CCA version
  ▼ Tag: HT Capabilities (802.11n D1.10)
    Tag Number: HT Capabilities (802.11n D1.10) (45)
    Tag length: 26
    ▼ HT Capabilities Info: 0x19ad
      .....1 = HT LDPC coding capability: Transmitter supports receiving LDPC coded packets
      .....0 = HT Support channel width: Transmitter only supports 20MHz operation
      .....11.. = HT SM Power Save: SM Power Save disabled (0x3)
      .....0.... = HT Green Field: Transmitter is not able to receive PPDU with Green Field (GF) preamble
      .....1.... = HT Short GI for 20MHz: Supported
      .....0.... = HT Short GI for 40MHz: Not supported
      .....1.... = HT Tx STBC: Supported
      .....01.... = HT Rx STBC: Rx support of one spatial stream (0x1)
      .....0.... = HT Delayed Block ACK: Transmitter does not support HT-Delayed BlockAck
      .....1.... = HT Max A-MSDU length: 7935 bytes
      .....1.... = HT DSSS/CKK mode in 40MHz: Will/Can use DSSS/CKK in 40 MHz
      .....0.... = HT PSMP Support: Won't/Can't support PSMP operation
      .....0.... = HT Forty MHz Intolerant: Use of 40 MHz transmissions unrestricted/allowed
      .....0.... = HT L-SIG TXOP Protection support: Not supported
    ▶ A-MPDU Parameters: 0x17
    ▶ Rx Supported Modulation and Coding Scheme Set: MCS Set
    ▶ HT Extended Capabilities: 0x0000
    ▶ Transmit Beam Forming (TxBF) Capabilities: 0x00000000
    ▶ Antenna Selection (ASEL) Capabilities: 0x00
  ▶ Tag: HT Information (802.11n D1.10)
  ▶ Tag: Extended Capabilities (8 octets)
  ▶ Tag: Vendor Specific: Microsoft Corp.: WPS
  ▶ Tag: Vendor Specific: Broadcom
  ▶ Tag: Vendor Specific: Microsoft Corp.: WPA Information Element
  ▶ Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
  ▶ Tag: RM Enabled Capabilities (5 octets)
  ▶ Tag: Vendor Specific: Epigram, Inc.
```

```
▼ IEEE 802.11 wireless LAN
  ▼ Tagged parameters (54 bytes)
    ▶ Tag: SSID parameter set: FreeWifi
    ▶ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
    ▶ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
  ▼ Tag: HT Capabilities (802.11n D1.10)
    Tag Number: HT Capabilities (802.11n D1.10) (45)
    Tag length: 26
    ▼ HT Capabilities Info: 0x01ef
      .....1 = HT LDPC coding capability: Transmitter supports receiving LDPC coded packets
      .....1.. = HT Support channel width: Transmitter supports 20MHz and 40MHz operation
      .....11.. = HT SM Power Save: SM Power Save disabled (0x3)
      .....0.... = HT Green Field: Transmitter is not able to receive PPDU with Green Field (GF) preamble
      .....1.... = HT Short GI for 20MHz: Supported
      .....1.... = HT Short GI for 40MHz: Supported
      .....1.... = HT Tx STBC: Supported
      .....01.... = HT Rx STBC: Rx support of one spatial stream (0x1)
      .....0.... = HT Delayed Block ACK: Transmitter does not support HT-Delayed BlockAck
      .....0.... = HT Max A-MSDU length: 3839 bytes
      .....0.... = HT DSSS/CKK mode in 40MHz: Won't/Can't use of DSSS/CKK in 40 MHz
      .....0.... = HT PSMP Support: Won't/Can't support PSMP operation
      .....0.... = HT Forty MHz Intolerant: Use of 40 MHz transmissions unrestricted/allowed
      .....0.... = HT L-SIG TXOP Protection support: Not supported
    ▶ A-MPDU Parameters: 0x03
    ▶ Rx Supported Modulation and Coding Scheme Set: MCS Set
    ▶ HT Extended Capabilities: 0x0000
    ▶ Transmit Beam Forming (TxBF) Capabilities: 0x00000000
    ▶ Antenna Selection (ASEL) Capabilities: 0x00
```

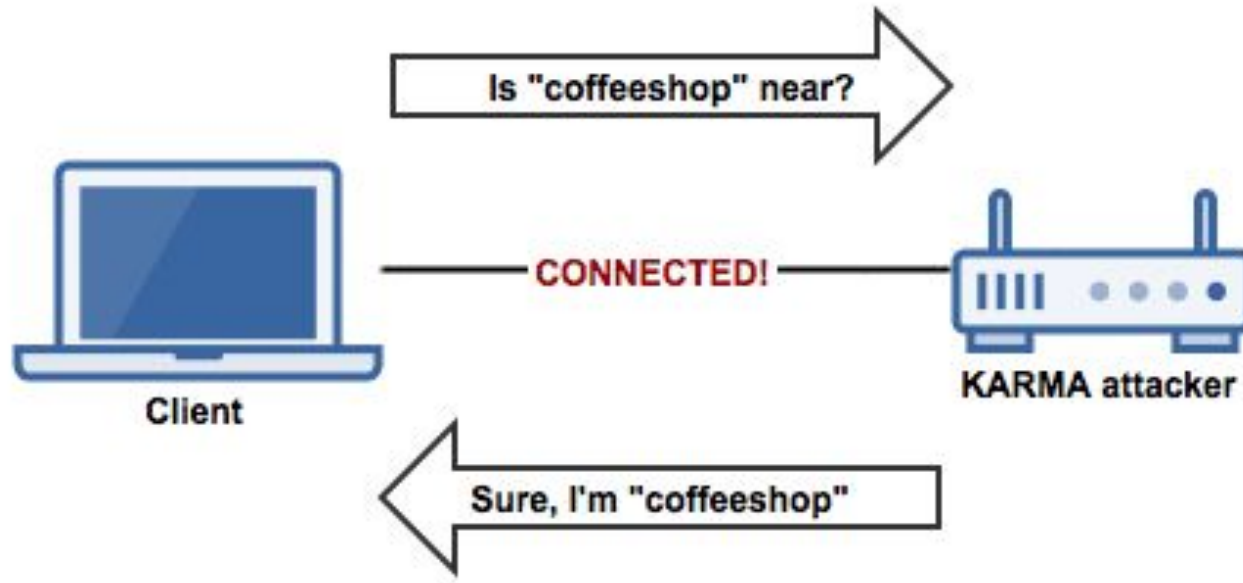
Attaque de type Karma

Karma Attacks Radio Machines Automatically

Man-in-the-middle



Attaque de type Karma



Contremesures

Suppression des réseaux dans les paramètres de connexion sans fil

PiKarma, outil open source, capable de détecter les attaques Karma



Conclusion

Adresse MAC identifiant unique

Mécanisme de randomisation

Contourner en :

- récupérant l'adresse
- trouvant d'autres identifiants uniques
- attaquant avec Man-in-the-Middle

