ECOLE SUPERIEURE
D'INGENIEURS DE RENNES

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

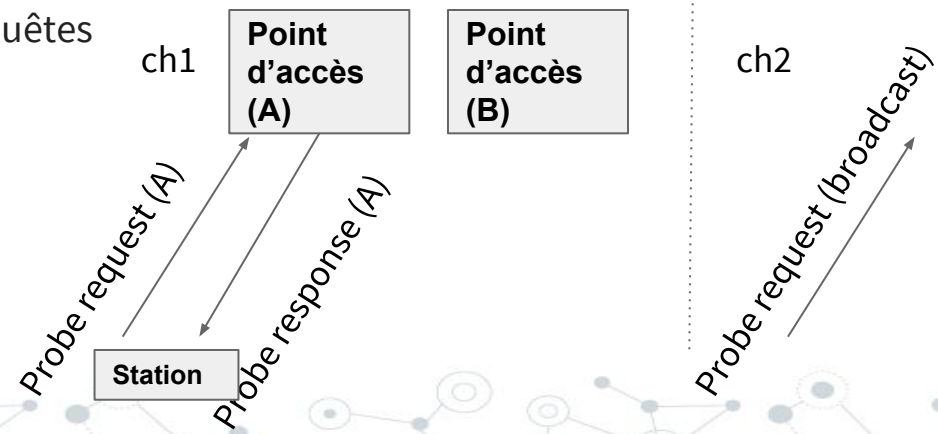
Le système de randomisation d'adresses MAC

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

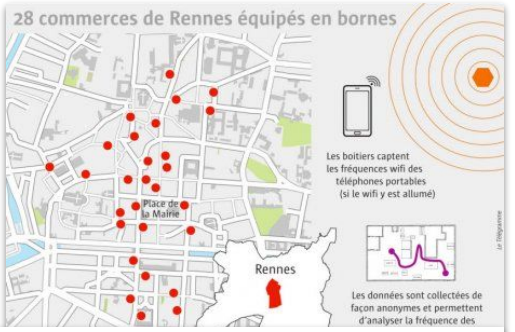
Envoi de l'adresse MAC dans ces requêtes



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

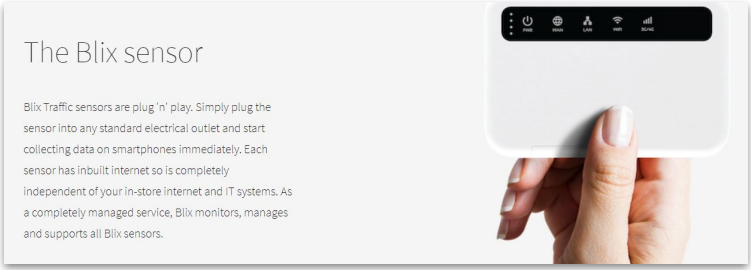


ACCUEIL › RENNES

Rennes : Des capteurs wifi pour suivre les clients du centre-ville

La CNIL s'oppose au traçage des piétons par Wi-Fi à La Défense

20 minutes



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

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

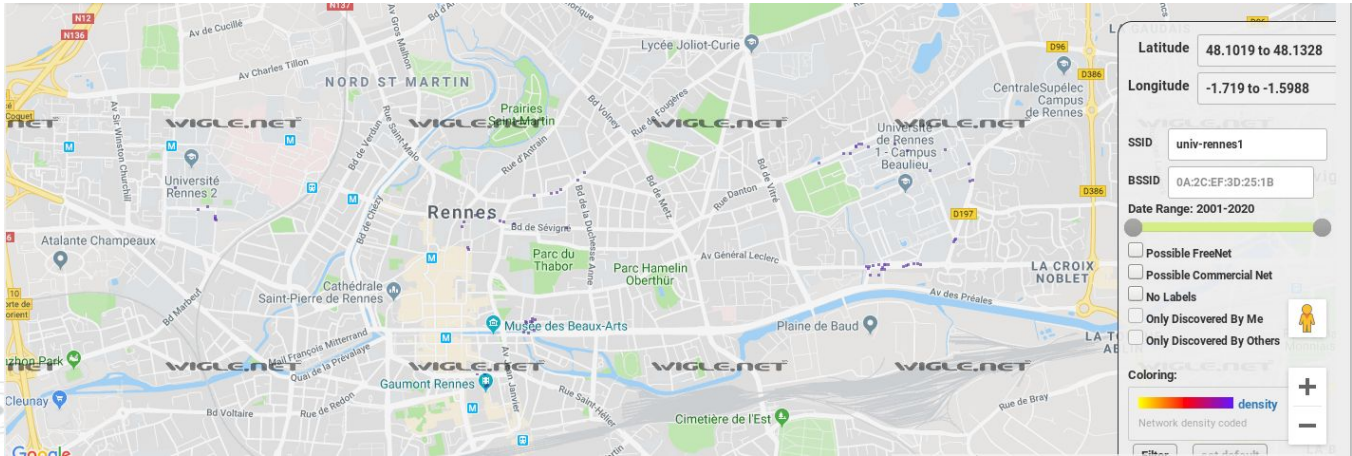
Titre subjectif peut révéler des informations

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']
```

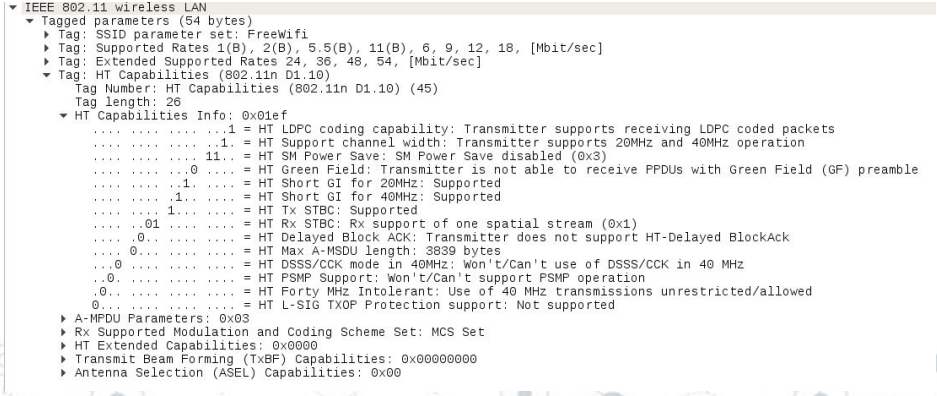
Utilisation de Probequest

Information Elements

IEs tagged parameters

Informent des capacités de l'appareil

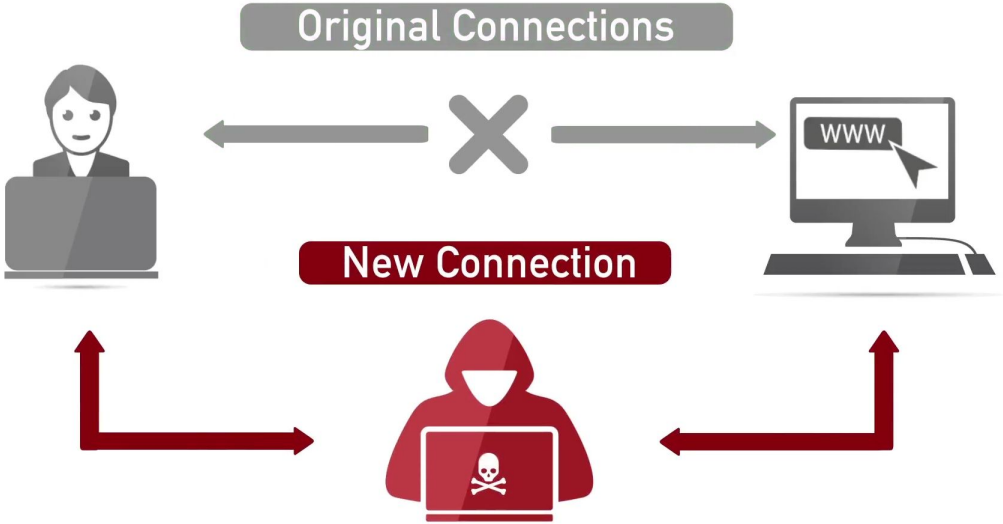
- débits supportés
- protocoles acceptés
- …



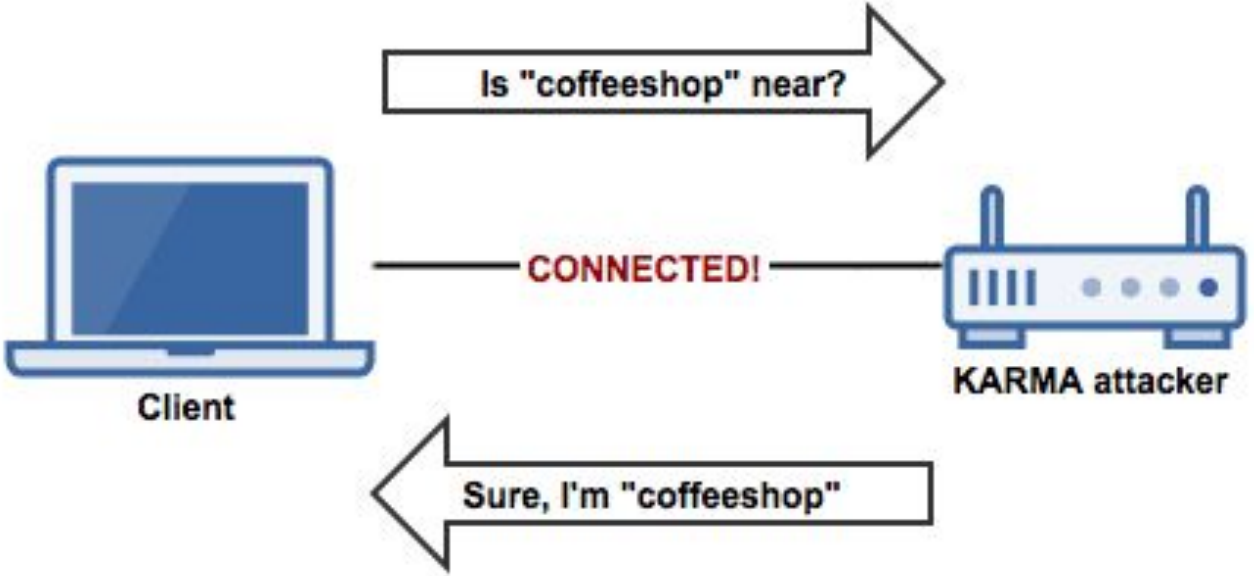
Attaque de type Karma

Karma Attacks Radio Machines Automatically

Man-in-the-middle



Attaque de type Karma



Contremesures

Suppression des réseaux dans les paramètres de connection 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