

Sécurité du téléphone: 2 - Traçage par GSM et Wifi

Contenu transféré depuis la base: [Sécurité du téléphone: 2 - Traçage par GSM et Wifi](#)

Sécurité du téléphone. Fiche 2

Dans cette fiche, nous allons voir les risques peu connus liés au traçage d'un téléphone mobile.

Modèle de menace : la police présente sur une action utilise un **IMSI-catcher** pour repérer tous les téléphones présents dans une zone, enregistrant les numéros **IMSI** et les numéros de téléphone. Ces numéros permettent d'identifier les propriétaires de téléphones anonymes en analysant leur déplacement sur le réseau de téléphonie mobile.

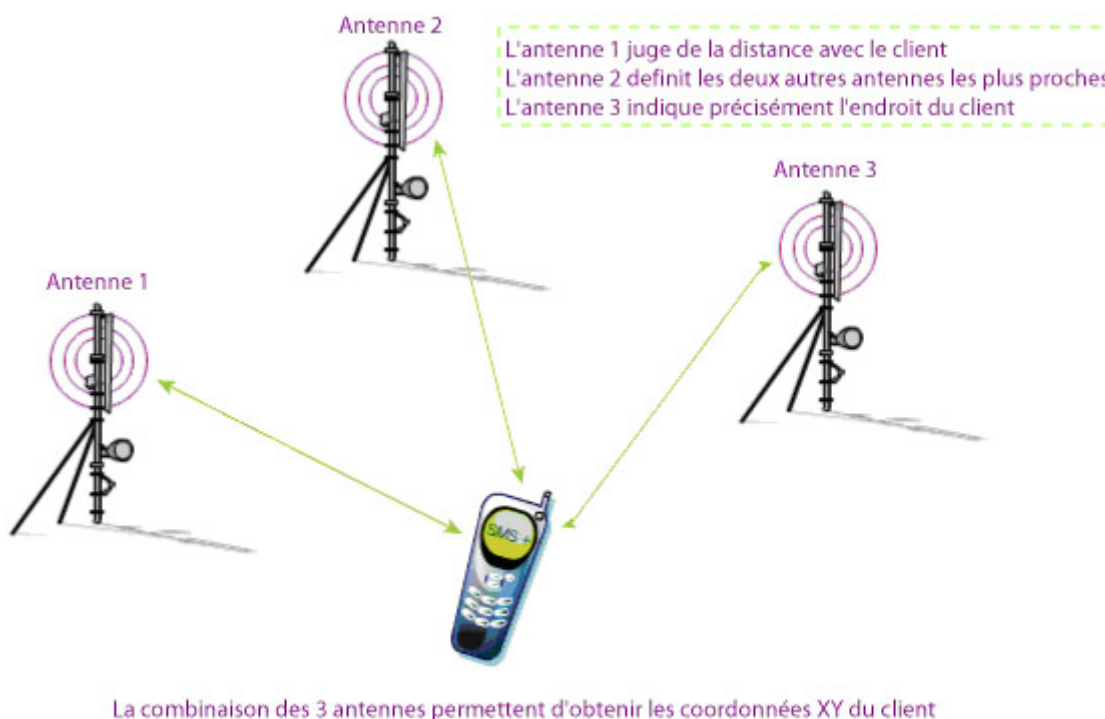
Menace type 1 : la carte SIM
est tracée et le ou la
propriétaire est identifiée

Le suivi par GPS

Contrairement à une idée répandue, nous sommes rarement traqués par le GPS de nos mobiles. Les capteurs GPS sur les téléphones sont des **récepteurs**. Des satellites géostationnaires envoient constamment des données qui permettent aux téléphones de déterminer leur position sur le globe. Cette position est calculée **dans le téléphone** en fonction de la distance connue d'au moins 4 satellites. Les satellites n'ont même pas connaissance des récepteurs GPS utilisant leurs données.

Le traçage GPS peut se produire via des logiciels malveillants présent sur des téléphones, qui transmettent la position calculée par le téléphone à un serveur via internet. Pour introduire un logiciel malveillant sur le téléphone, l'attaquant doit généralement avoir un **accès physique au téléphone (déverrouillé)**, ou que le/la propriétaire ait été victime d'une attaque de *fishing* pour qu'il installe lui/elle-même l'application malveillante. Une fois le logiciel malveillant installé, il faut quand même que le GPS et que les données mobiles soient activés pour qu'il puisse vous suivre et transmettre les données.

Pour repérer un téléphone géographiquement le plus pratique est d'utiliser le réseau téléphonique. Nos téléphones sont toujours connectés à une ou plusieurs bornes/antennes plus ou moins éloignées (les fameuses buchettes qui représentent la qualité de la connexion au réseau). Cela permet de communiquer sans être coupé à chaque changement d'antenne. C'est également très pratique pour suivre un téléphone car l'on peut voir nos appareils sautiller d'antenne en antenne. Les antennes qui sont généralement arrangées en réseaux le long des routes et au sommet des bâtiments, et que l'on appelle souvent des tours ou antennes relais, sont des points de repères connus. Il suffit alors de faire une "triangulation" pour obtenir le point d'émission de votre téléphone avec une bonne précision. C'est la méthode employée, par exemple, par les nazis pour repérer les radio clandestines pendant la Seconde Guerre mondiale.



Identifier le propriétaire d'un téléphone

A chaque carte SIM correspond un numéro de téléphone mais également un numéro unique lui servant à s'identifier avec les antennes relais : le IMSI (International Mobile Subscriber Identity). Puisqu'il sert d'identifiant, il est constamment diffusé lors des échanges avec les antennes. Or il est très simple de capter les numéros IMSI des téléphones avoisinants quelques centaines de mètres autour de soi en utilisant [un récepteur SDR à 15€](#).

Cela a des conséquences importantes :

1. Les cartes SIM sont souvent achetées via des cartes de crédit (votre abonnement mensuel ou l'achat au tabac du coin). Donc l'association utilisateur = SIM est facile à connaître.
2. Même si vous achetez en liquide une carte pré-payée, utiliser ce téléphone à côté de votre téléphone officiel ou celui d'un copain vous identifie. Par exemple : je suis dans un bar, j'allume mon téléphone pré-payé et je suis avec mon téléphone officiel dans la poche. Les deux téléphones sont 'vus' ensemble donc il y a un lien. De même, si vous éteignez votre téléphone officiel mais allumez votre téléphone pré-payé au domicile, l'adresse est connue.
3. Insérer une sim dans un téléphone utilisé officiellement permet à l'opérateur d'associer l'identification de votre terminal (téléphone) avec la nouvelle sim. (l'IMEI est utilisé avec la SIM X appartenant à Harry mais aussi avec la SIM Y.... donc Y = Harry). Ayez un téléphone dédié et si possible jamais utilisé ou acheté d'occasion.

Conséquence : vous êtes localisable avec votre téléphone, prépayé ou non. Si quelqu'un a accès à la fois à votre numéro IMSI et l'accès à la base de données du fournisseur (ce que les autorités obtiennent facilement), il est possible de remonter à l'identité des individus présents dans le rayon d'une antenne, dont la vôtre.

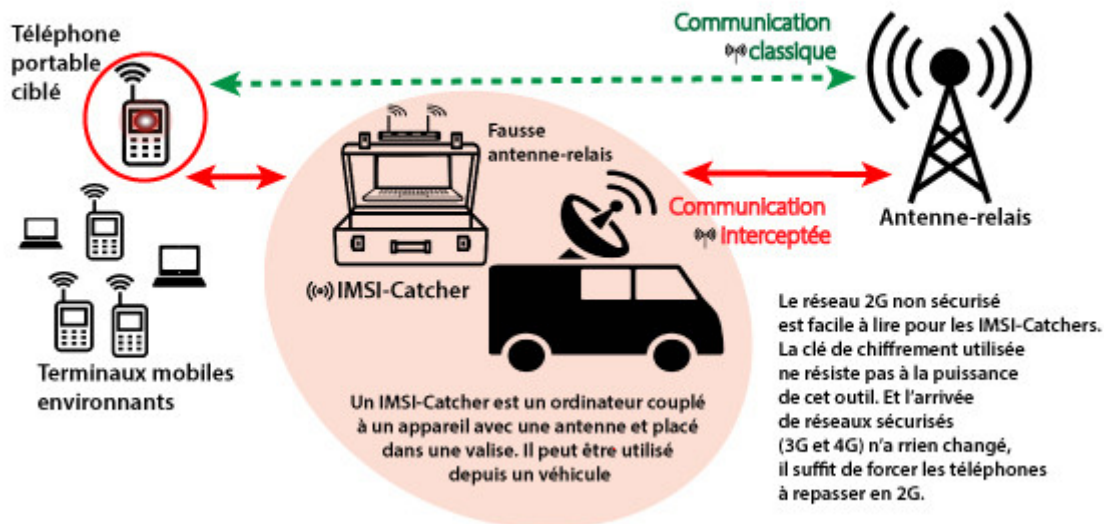
Cela peut être utilisé pour déterminer les identités des individus présents à une manifestation, et peut être utilisé plus tard pour trouver des groupes d'activistes pendant une réunion. Il se pourrait que cette technique ait été utilisée pour découvrir et mettre fin aux *Black Lives Matter* aux USA.

Une **autre conséquence** est l'identité du téléphone : le IMEI (*International Mobile Equipment Identity*). C'est comme la plaque d'immatriculation de votre téléphone. L'IMEI est également diffusé par le téléphone à chaque interaction avec une antenne de téléphonie mobile (BTS). L'IMEI couplé à l'IMSI peut ajouter une couche supplémentaire de preuves d'identification en cas de saisie, car même si la carte SIM est retirée, l'appareil est identifié.

La surveillance des appels

Une autre menace existe. Au lieu de récolter seulement le numéro IMSI, les téléphones peuvent être facilement trompés en leur faisant croire qu'ils communiquent avec une vraie antenne téléphonique alors qu'en réalité ils sont traqués. Les appels et SMS envoyés peuvent être surveillés (même si cryptage du téléphone) à l'insu du propriétaire du téléphone. Cela a été largement utilisé par les services de polices aux Etats-Unis et ailleurs grâce au déploiement d'un *IMSI Catcheur*.

IMSI-Catcher mode d'emploi



Les systèmes Stingray sont utilisés à la fois pour traquer les téléphones et surveiller leur transmissions. Ces systèmes sont connus pour avoir été largement utilisés contre les activistes. Les services de police des Etats Unis, du Canada, de l'Irlande, du Royaume-Uni, Arabie Saoudite, UAE et Turquie ont reconnu les avoir utilisés.

Ces systèmes appelés IMSI Catcher peuvent aussi être fait maison, avec un budget de 1000€.



Se défendre contre les IMSI Catchers

Utiliser des cartes SIM prépayées

Pour éviter l'identification via l'IMEI, l'identité du téléphone, vous devez utiliser des téléphones achetés uniquement avec du liquide. De plus, même si ça peut paraître irréaliste la plupart du temps, mais pour des action à haut risques, vous devriez acheter un téléphone portable sans abonnement avec une carte SIM prépayée.

i On recommande que tous les coordinateur·rice·s, surtout ceux·elles engagé·e·s dans la planification d'actions et la logistique, utilisent des carte SIM prépayées, et idéalement des téléphone sans abonnements. Le groupe infrastructure devrait considérer avoir un stock de cartes SIM prépayées. Ces dépenses de 7-10€ peuvent être faites avant une action puis les cartes SIM recyclées pour les actions suivantes. Dans le pire des cas, cela peut permettre une confusion dans l'effort de la police utilisant un système de capture de IMSI.

Les téléphones sans abonnement (prépayés) sont des investissements qui peuvent être considérés pour des actions à hauts risques.

⚠ Attention à bien prendre en compte la partie sur l'identification au dessus. Avoir une carte pré-payée permet de freiner l'identification mais de nombreuses erreurs telles que la présence de téléphones "fantômes" à côté de téléphones officiels rends caduques l'anonymisation. Pensez à distribuer les téléphones pré-payés uniquement après avoir éteint tout téléphone officiel.

Installer un détecteur de IMSI Catcher

Des applications ont été développées pour détecter et avertir de la présence de catcher IMSI. Elles utilisent une carte des antennes de téléphonie mobile pour détecter la présence d'antennes inconnues qu'elles considèrent alors comme suspectes. Sans être entièrement fiables, certaines applications sont plus complexes que d'autres et détectent les "SMS silencieux" souvent utilisés par les IMSI catchers. Une de ces applications est [Android IMSI catcher detector](#) pour les services Android. En voici une autre [SnoopSnitch](#) (**Avertissement** : lien Google Play).

Est-ce qu'on est detectable quand on est en mode avion ?

Pour simplifier un peu grossièrement : Il n'est pas totalement exclu que bluetooth, wifi et réseau mobile fonctionnent et dialoguent avec les différents hubs qu'il y a autour MALGRÉ le mode avion : c'est selon les OS et l'honnêteté des marques qui les développent.

Néanmoins :

1. Sans carte SIM, l'opérateur ne peut pas faire le lien avec nos noms. L'antenne va avoir une adresse IP, mais pas de numéro client, et l'adresse IP change ofc d'une antenne à l'autre, donc pas possible de faire le lien avec une identité.
2. La seule vraie faille est au niveau de l'adresse MAC de nos smartphones (qui est une adresse statique, sauf sur le réseau mobile). Il est théoriquement possible de la retracer via les boxs wifi de particuliers à côté desquelles on passe : Même si on ne s'y connecte pas, nos smartphones crient en permanence leurs adresses MAC à toutes les boxs wifi qu'ils rencontrent.

Mais (1) c'est très difficile à faire et ça demande des efforts et un temps considérables pour identifier ne serait-ce qu'un appareil, et (2) si les flics peuvent demander à SFR d'accéder aux données de leurs antennes (ce que suggérais l'article), ils ne peuvent pas demander les données des boxs de tous les particuliers d'une rue (juridiquement et logistiquement : un enfer. Les opérateurs n'ont pas intérêt à leur filer les données de boxs de particuliers) En bref : clairement pas intéressant pour eux de s'attaquer à un si gros défi pour des délits aussi mineurs.

3. Le GPS est hors de propos, nos smartphones ne lui parlent pas.

NB : Concernant la prise de photo en revanche, elle peut poser problème, et ce même à postériori parce qu'elles sont souvent liées par défaut à une localisation (ou autres exifs, vous en parliez) et à des comptes personnels sur différents services. Charge à chacun d'aller checker ses réglages si iel veut prendre le risque de photographier des trucs. Sur ce sujet ça dépend des googles & co, pas du fonctionnement des réseaux, du coup ça reste une zone d'ombre.

Menace type 2 : traçage et identification via WiFi

Comme sur le réseau de téléphonie mobile, un téléphone diffuse des informations d'identification aux réseaux WiFi. La partie WiFi d'un téléphone peut également être utilisée pour suivre un appareil lorsqu'il se déplace en ville. L'équivalent du IMSI ou IMEI est une adresse MAC (Media Access Controller) comme par exemple `62:7d:34:c1:04:2b`.

Même si l'on est connecté à aucun réseaux, le téléphone diffuse quand même des demandes de sonde aux points d'accès WiFi qui constituent une cartographie excellente en ville et donc une traçabilité du téléphone.

Les téléphones Apple récents "anonymisent" de telle requête jusqu'à ce que le téléphone soit connecté aux réseaux WiFi. Les Androids ne le font pas. Dans tous les cas, il est important de savoir que cela se produit, tout comme le fait que les points d'accès gardent en mémoire une trace du passage de votre téléphone. De telles traces ont été utilisées comme preuve à plusieurs reprises dans les tribunaux.

⚠ Si vous effectuez des recherches sur le terrain et/ou ailleurs pour aider à une action, réfléchissez à deux fois avant de rejoindre un réseaux public non-fiable et n'activez votre WiFi que lorsque vous en avez besoin.

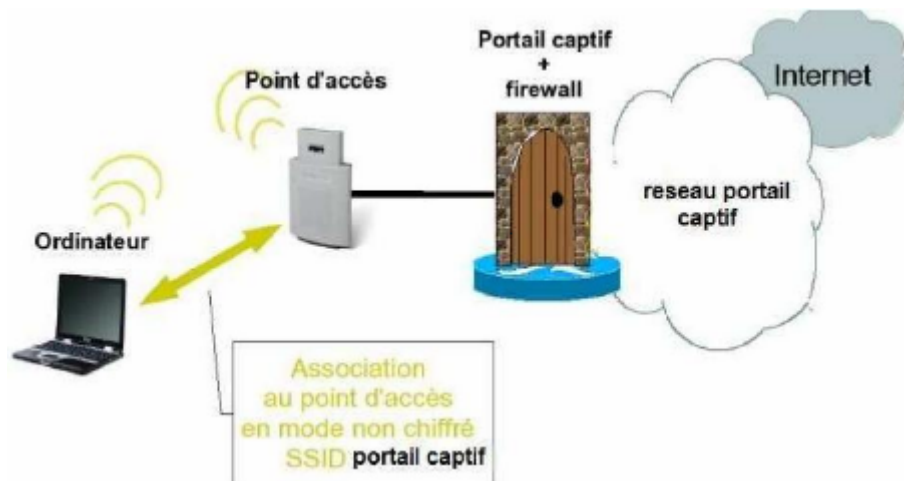
Utiliser un réseau WIFI inconnu

Lorsque vous utilisez un réseau WiFi inconnu vous ne pouvez garantir la confidentialité des données échangées. De nombreux réseaux ouverts officiels (les hôtels par exemple) utilisent des outils de type portail captif. Ces composants servent à garantir la traçabilité des usages des réseaux. En France, un fournisseur d'accès internet (un hôtel devient fournisseur en proposant son wifi) se doit de garder des traces des accès Internet en cas de demande des services d'état dans le cadre d'enquêtes (cf.

<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164> Article 6). Tout accès vers internet est enregistré dans des journaux (logs) et souvent les flux chiffrés sont

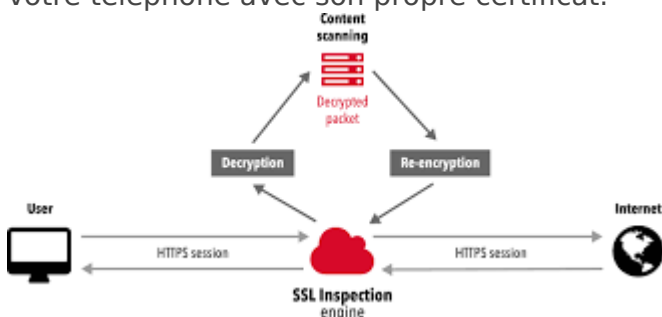
décryptés. C'est facilement repérable sur un pc, un peu moins sur un téléphone. Dans ce cas, lors de l'utilisation du WiFi, vous êtes redirigés vers une page d'authentification qui demande à connaître :

- N° de chambre,
- Numéro de téléphone pour recevoir un code par SMS. Le pire. Vous êtes automatiquement relié a votre identifiant téléphonique, voir ci-dessus les impacts.
- Votre nom
- Votre email
- Tout autre type d'information.

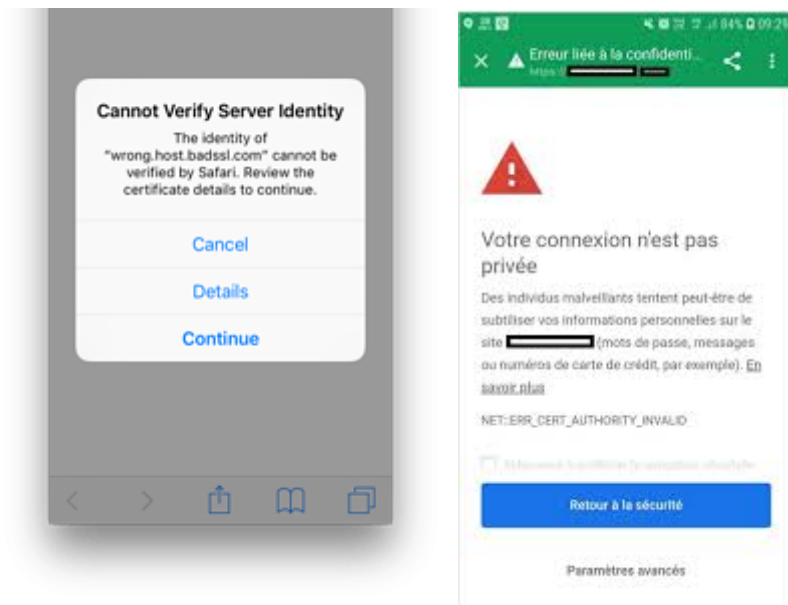


Dès que vous avez ce type de page vous pouvez être certain que vous n'aurez pas un accès direct à Internet comme avec votre box, mais que tout va être enregistré dans un journal (log).

De plus, même si vous naviguez en chiffrant vos communications, cela est très souvent insuffisant. Les Portails ou les routeurs du restaurant, hôtel... peuvent faire de l'inspection SSL. Ils déchiffrent vos communications pour voir l'intérieur des messages. C'est également repérable car vous devez avoir une alerte de sécurité sur votre client de mail, navigateur web etc... Le routeur va se substituer à vous lors de la connexion avec le site internet et vous renvoyer les informations sur votre téléphone avec son propre certificat.



Votre téléphone ne reconnaissant pas le certificat d'origine doit vous alerter.



Dans tous les cas, vous devez vous déconnecter et supprimer le réseau de vos paramètres WiFi de votre téléphone sinon il essaiera de nouveau de s'y connecter.

Références :

- (fr) [Wikipedia sur le système IMSI-catcher](#)
- (en) [Wikipedia page on the Stingray system.](#)
- (en) [Article in The Intercept on Stingray systems](#)

► [Suivant : Sécurité du téléphone, fiche 3](#)

Révision #1

Créé 8 septembre 2023 18:16:24 par mollusque

Mis à jour 8 septembre 2023 18:16:24 par mollusque