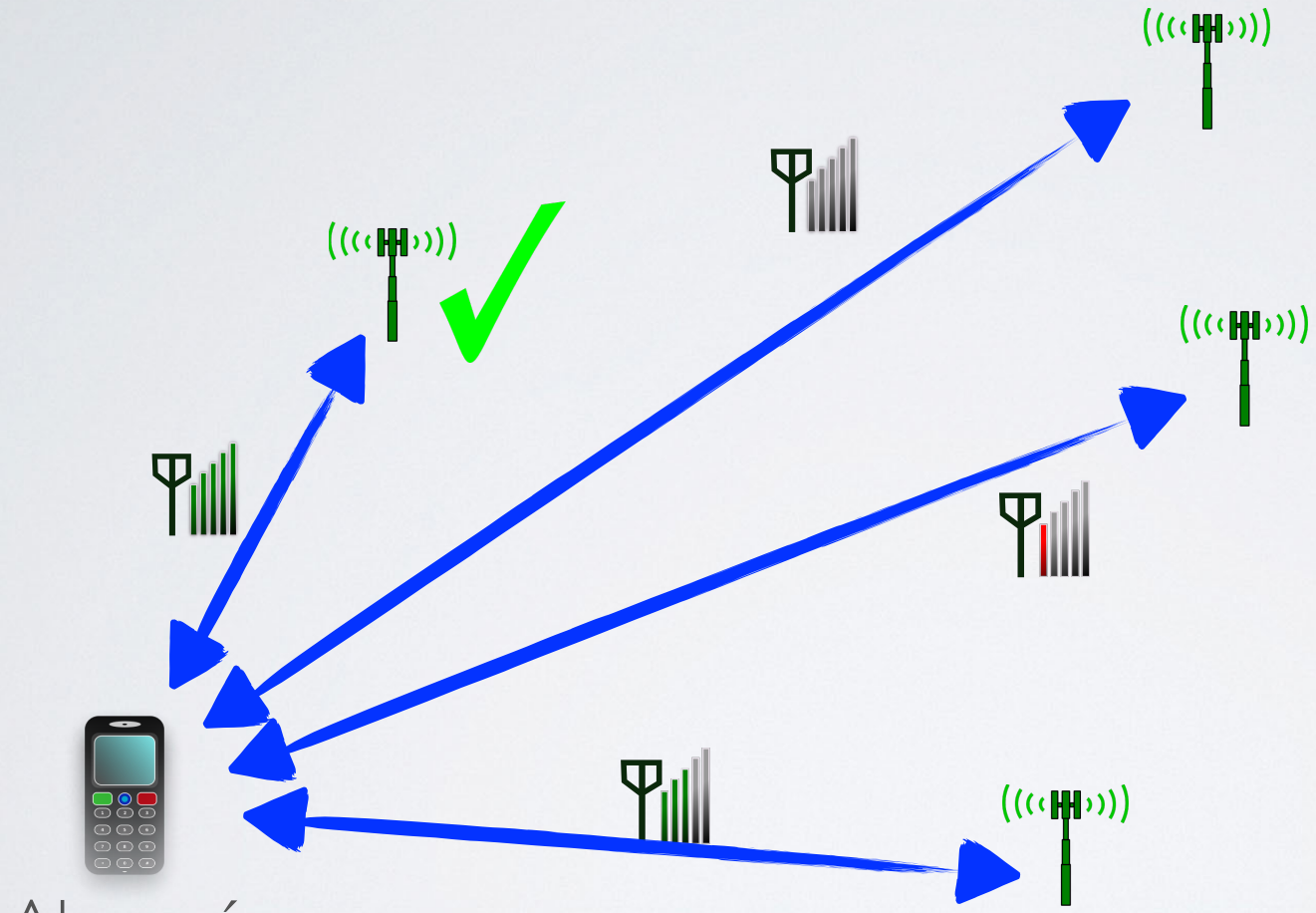
PSES 2015

LES IMSI-CATCHERS

ou comment devenir parano

Yves Rougy — twitter: @yrougy
email: yves@rougy.net

LE GSM



Abonné
(IMSI)

L'abonné de PSES télécom capte plusieurs antennes et choisit celle qu'il reçoit le plus fort.

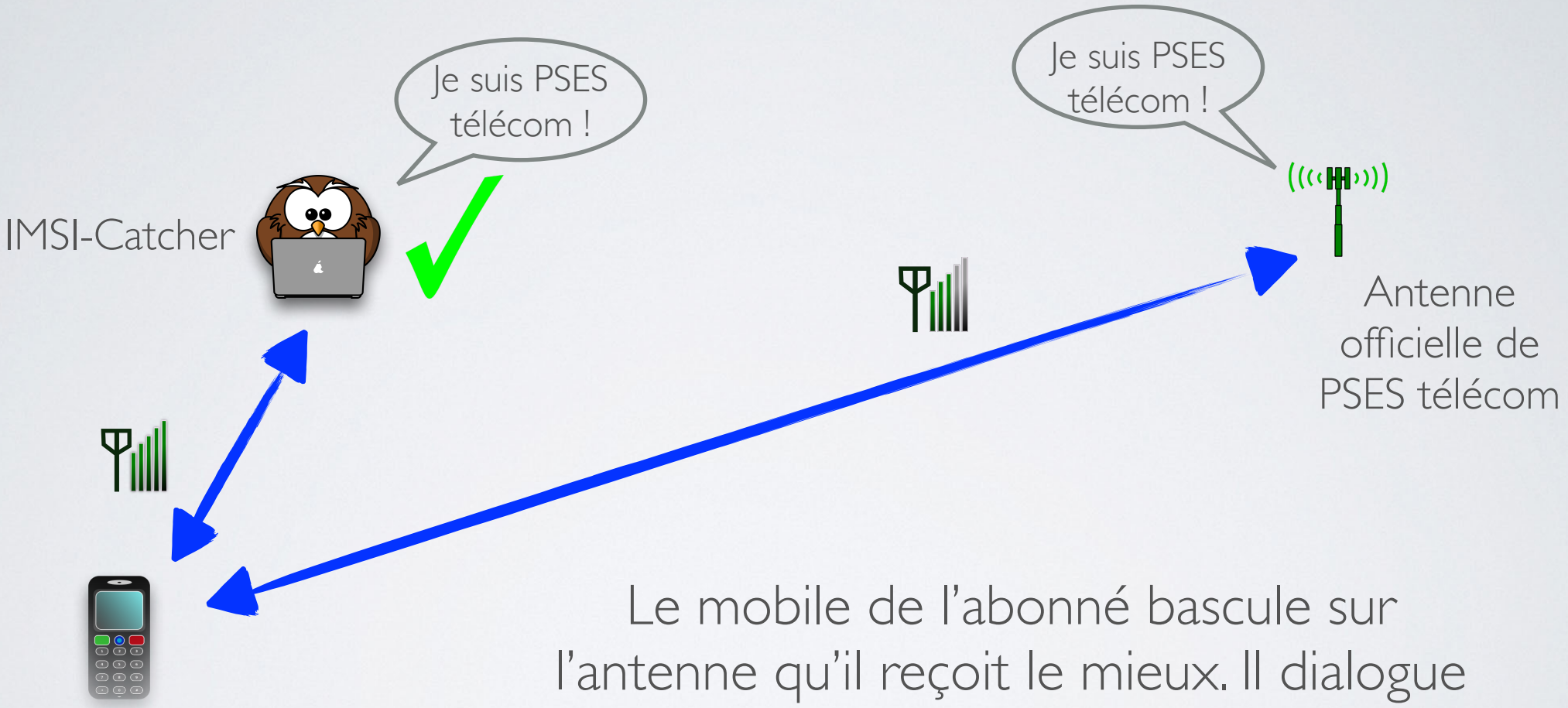
LE GSM

- Le téléphone est identifié par IMEI.
- Les appels et SMS sont chiffrés.

- La carte SIM (l'abonné) est identifié par IMSI.
- Dans la plupart des échanges, un IMSI temporaire (TMSI) est utilisé (pour la confidentialité).
- La clé permettant le chiffrement des appels est dans la SIM.

- L'antenne s'annonce en disant simplement à quel opérateur elle est reliée.
- L'antenne demande quels TMSI sont à sa portée pour acheminer un appel ou un SMS (paging).

IMSI-CATCHER



Le mobile de l'abonné bascule sur l'antenne qu'il reçoit le mieux. Il dialogue maintenant avec l'IMSI-Catcher.

IMSI-CATCHER

Abonné

IMSI-Catcher

Re-authentifie-toi

Voilà mon IMSI

Ne cherche pas de meilleure antenne

Tiens, voilà une nouvelle configuration

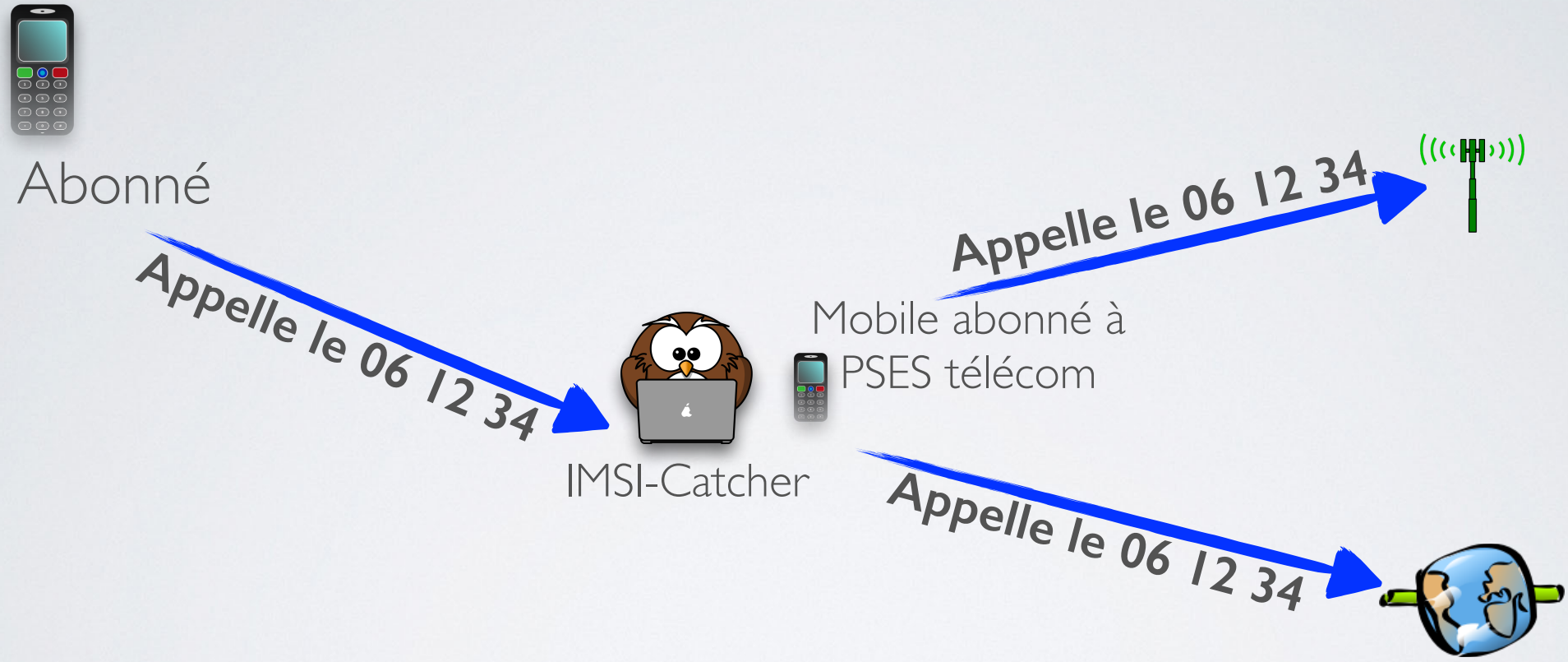
Mets toi à jour avec ce firmware

IMSI-CATCHER

- L'IMSI-Catcher se fait passer pour l'antenne.
- L'IMSI-Catcher ne possède pas la clé de chiffrement des appels.

- Pour acheminer les appels, les premières versions des IMSI-Catcher désactivaient le chiffrement de la communication.
- Les IMSI-Catcher modernes calculent la clé en quasi-temps réel. Ils peuvent laisser le chiffrement en place si le chiffrement est vulnérable à ce calcul (A5/1 et A5/2).
- L'IMSI-Catcher peut contrôler tout ce que l'opérateur contrôle sur le mobile (Serveurs MMS ou SMS, numéro de la messagerie, …).

IMSI-CATCHER



Comme l'IMSI-Catcher n'est pas connecté au réseau de l'opérateur, il va se faire passer pour un mobile pour transférer l'appel, avec son abonnement propre. Ou passer par une connexion VoIP.

IMSI-CATCHER

Pour quoi faire ?

- Faire une liste des IMSI dans une zone donnée.
- Corréler cette liste avec d'autres captures pour identifier les propriétaires.
- Écouter les conversations et recevoir les SMS d'une cible en particulier.
- Empêcher la communication GSM dans une zone donnée.
- Se passer de la coopération de l'opérateur.
- Techniquement réalisable par n'importe quelle entité.

IMSI-CATCHER

Les problèmes !

- Aucun contrôle sur qui écoute, quand, et ce qu'il fait des données récupérées. Le choix est à la discretion de l'opérateur de l'IMSI-Catcher.
- Seuls les mobiles ciblés peuvent passer des appels.
  - Certains IMSI-Catcher peuvent acheminer plus d'appels à l'aide d'une connexion données, via la VoIP.
  - Potentiellement problématique pour appels d'urgence.
- Les mobiles enregistrés sur l'IMSI-Catcher sont hors réseau, et donc non joignables en appels entrants.

IMSI-CATCHER

Par extension.

Avec le temps, le nom IMSI-Catcher s'est associé avec l'usage « tout ce qui permet d'intercepter sauvagement les communications de mobiles ».

- Écoutes passives,
- Compromission d'antennes,
- Autres technologies.

EN 3G

Pas à l'abris !

- La 3G nécessite que l'antenne s'authentifie également.
- Un intrus ne peut plus se faire passer pour l'antenne.

Mais

- Si le mobile utilise le GSM en repli de la 3G, il va accepter que l'antenne ne s'authentifie pas.
- Il est possible de brouiller le signal 3G pour forcer le repli en GSM.
- Même sans repli, il est possible de demander qu'un mobile envoie son IMSI.

EN 3G/4G

Le problème des femtocells

Pour intercepter des communications, il suffirait de compromettre une antenne « officielle ».

- En 2012, un modèle déployé de femtocell 3G a pu être modifiée par un abonné pour en prendre le contrôle.
- Le réseau fonctionne normalement, l'antenne est officielle.
- Toutes les communications qui y passent peuvent être interceptées.
- Et la 4G ?

EN 4G

VoLTE

La 4G (LTE) résout la plupart des problèmes rencontrés.
Cependant, LTE ne prévoie pas de mode *circuit*.
Les réseaux des opérateurs ne sont pas encore prêts pour la VoLTE (VoIP).

- À la réception d'un appel, le mobile passe en 3G ou en 2G.
- À l'émission d'un appel aussi.

L'ÉCOUTE PASSIVE

Indétectable !

À l'aide d'un *récepteur* et la technologie de radio logicielle, il est possible de déchiffrer et suivre les communications.

- Assez peu fiable,
- Très dépendant de l'environnement radioélectrique,
- Totalement indétectable.

LA DÉTECTION

Logiciels de détection

Snoopsnitch

Détecte les anomalies sur le réseau.

- Les anomalies existent dans un réseau en production,
- La détection se base sur un score, comme pour le spam,
- Gros risque de faux positifs (sortie de métro, itinérance nationale, optimisations,…)
- Approche intéressante.

AIMSICD

Détecte essentiellement des cellules inconnues. Se base sur OpenCellID, très peu rempli pour la France.
Beaucoup de faux positifs, peu fiable pour le moment.

LA DÉTECTION

Les appels entrants

Dans le cas d'un IMSI-Catcher, le téléphone n'est pas connecté sur l'opérateur.

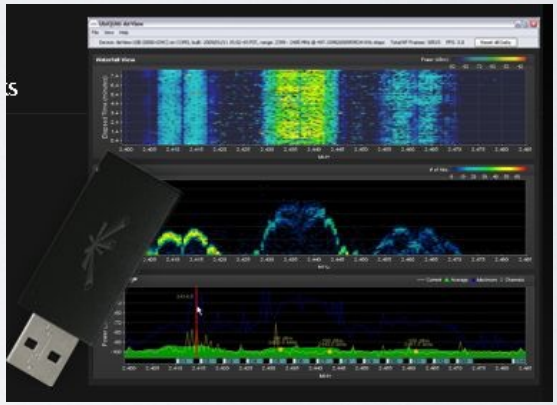
Les appels entrants ne passent donc pas.

- Appeler et se faire appeler régulièrement,
- Utiliser un service de call-back.

LA DÉTECTION

Sur les lieux fixes

Si on connait l'environnement radio habituel, on peut détecter des changements suspects:



- Nouvelle fréquence utilisée,
- Nouvel identifiant de cellule (Cell-ID),
- Cellules à durées de vie courtes,
- Brouillages radios,
- Fréquences incohérentes (utilisation d'une fréquence attribuée à un autre opérateur),
- …

LA DÉTECTION

De façon mobile

Beaucoup plus complexe.

- Faire un mapping des cellules habituelles du lieu,
- Détecter tout changement,
- Rechercher les incohérences sur les fréquences,
- Dégradation des fonctionnalités d'une cellule (pas de data, pas de chiffrement,…)
- …

LES CONTRE-MESURES

De façon générale

- Éviter la 2G (la désactiver dans le téléphone).
- Utiliser le chiffrement:
  - Genre TextSecure pour les messages, (ou équivalent qui fasse les SMS),
- Ne pas parler de sujets confidentiels/privés/secrets au téléphone (!).

LES CONTRE-MESURES

En cas de suspicion d'IMSI-Catcher

- Éteindre son téléphone.
- Se faire rappeler, ne pas appeler.
- Passer en 4G exclusivement pour faire de la VoIP (RedPhone ou autre).
- Utiliser des moyens de communication alternatifs (signaux de fumée…)

MERCI !

Des questions ?

Merci à @_GaLaK_, @Skhaen, @UnGarage, et tous les autres !

ANNEXES

C'est gros un IMSI-Catcher ?

Source: Verfassungsschutz (via DuD 26, 2006)
ISBN 6220-2845-4832-5932-9228

Source: Gamma Group

ANNEXES

Un peu de lecture

- *Digital Self-Defense in Mobile Networks* par Adrian Dabrowski
- *IMSI-Catch Me If You Can: IMSI-Catcher-Catchers* par A. Dabrowski and al.
- *Femtocells: A Poisonous Needle in the Operator's Hay Stack* par Ravishankar Borgaonkar, Nico Golde and Kevin Redon.
- *Hacking Femtocells* par Ravishankar Borgaonkar.
- *IMSI-Catcher and Man-in-the-Middle attacks* par Julian Dammann.
- *Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunication* par Nico Golde, Kévin Redon, Ravishankar Borgaonkar.