Interception passive d'informations sur le réseau GSM

Projet tutoré

INSA

Geoffrey Calmet-Sanchez
Damien Cassu
Axel Chauvin
Cécile Duthoit

Encadrants :

- Daniela Dragomirescu
- Damien Roque

Introduction

- 3,6 milliards d'utilisateurs mobiles
- Différentes failles ont été découvertes et exploitées

GSM®
GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

Notre projet

- Écoute, analyse et déchiffrement de communication GSM
- Droits des télécommunications
- Prise en main de logiciels open-source

ETSI

Sommaire

1. Droits des télécommunications
2. Rappels sur les notions nécessaires
    a. Techniques d'accès et canaux logiques
    b. Cryptographie
    c. Réseau GSM
3. Démonstration
4. Bilan

Droit des télécommunications

A-t-on le droit d'intercepter passivement les communications?

Va-t-on finir en prison?

- Le droit a dû s'adapter aux nombreuses évolutions technologiques

- Nécessité d'assurer la confidentialité, l'intégrité et la disponibilité des communications

XVIIIème siècle

XXIème siècle

- Au niveau mondial

  ➢ Régulé par l'UIT (Union internationale des télécoms), sous l'égide des Nations Unies
  ➢ Article 12 de la **Déclaration Universelle des Droits de l'Homme et des Nations Unies** :

« Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »

- Au niveau européen
  - ➢ Article 8 de la **Convention européenne des droits de l'homme relatif au droit et au respect de la vie privée et familiale**

1. *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.*

- Au niveau européen
  - ➢ **Paquet télécom** (2008-2009)
    - ■ Article 5 de la directive 2002/58/CE

1. Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée [...]. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité.

- Au niveau national (France)
  - ➢ Repose historiquement sur le **droit postal** qui garantit le secret de la correspondance
  - ➢ Régulé par l'**ARCEP** (Autorité de Régulation des Communications Electroniques et Postales) depuis 2005. Avant 2005 : **ART** (Autorité de régulation des télécommuncations).

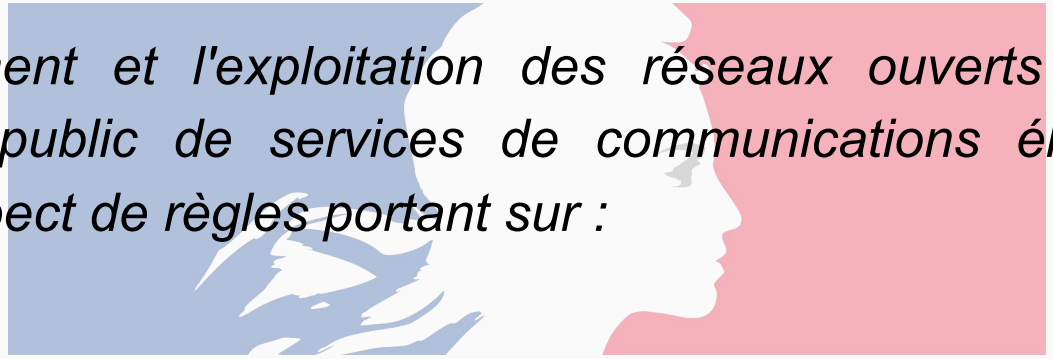
ARCEP

www.arcep.fr

- Au niveau national (France)
  - ➢ **Code des postes et des correspondances**
    - Article D98-5:

« L'opérateur prend toutes les mesures appropriées pour assurer l'intégrité, [...] la sécurité de son réseau et de ses services à un niveau adapté au risque existant. En particulier, des mesures sont prises pour prévenir ou limiter les conséquences des atteintes à la sécurité pour les utilisateurs et les réseaux interconnectés. »

- Au niveau national (France)
  - ➢ **Code des postes et des correspondances**
    - Article L33-1:



« L'établissement et l'exploitation des réseaux ouverts au public et la fourniture au public de services de communications électroniques sont soumis au respect de règles portant sur :

[...]

b) Les conditions de confidentialité et de neutralité au regard des messages transmis et des informations liées aux communications ;»

- Au niveau national (France)
  - ➢ **Code pénal**
    - Article 226-15: 1 an d'emprisonnement et 45000€ d'amande

« Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45 000 euros d'amende. Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie électronique ou de procéder à l'installation d'appareils de nature à permettre la réalisation de telles interceptions.»

Pour simplifier, nous supposerons que nous sommes de bonne foi...

Rappels sur les notions nécessaires

Un peu de remise à niveau (RT) ou de culture générale (I) !

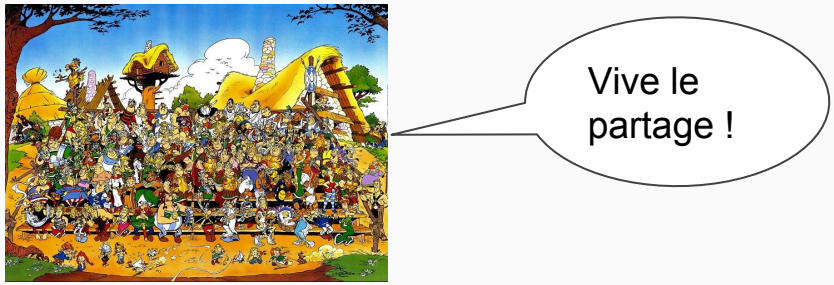
Techniques d’accès et canaux logiques

Comment accéder au spectre radio ?

La bande des 900MHz
(880-960MHz)

FDMA

Chaque part correspond à une fréquence de porteuse identifiée par un numéro ARFCN (Absolute Radio Frequency Channel Number)



Comment augmenter le nombre d'utilisateurs ?

Partager le temps de dégustation !
C'est le TDMA

Panoramix	Astérix	Idéfix	Falbala	Obélix	César	Cléopatre	Bonemine
0	1	2	3	4	5	6	7

Slot
577 µs

Trame TDMA
4,6 ms

Canaux physiques VS Canaux logiques

Canaux logiques
=
?

Canaux physiques
=
N° Slot TDMA + N° Trame TDMA + ARFCN

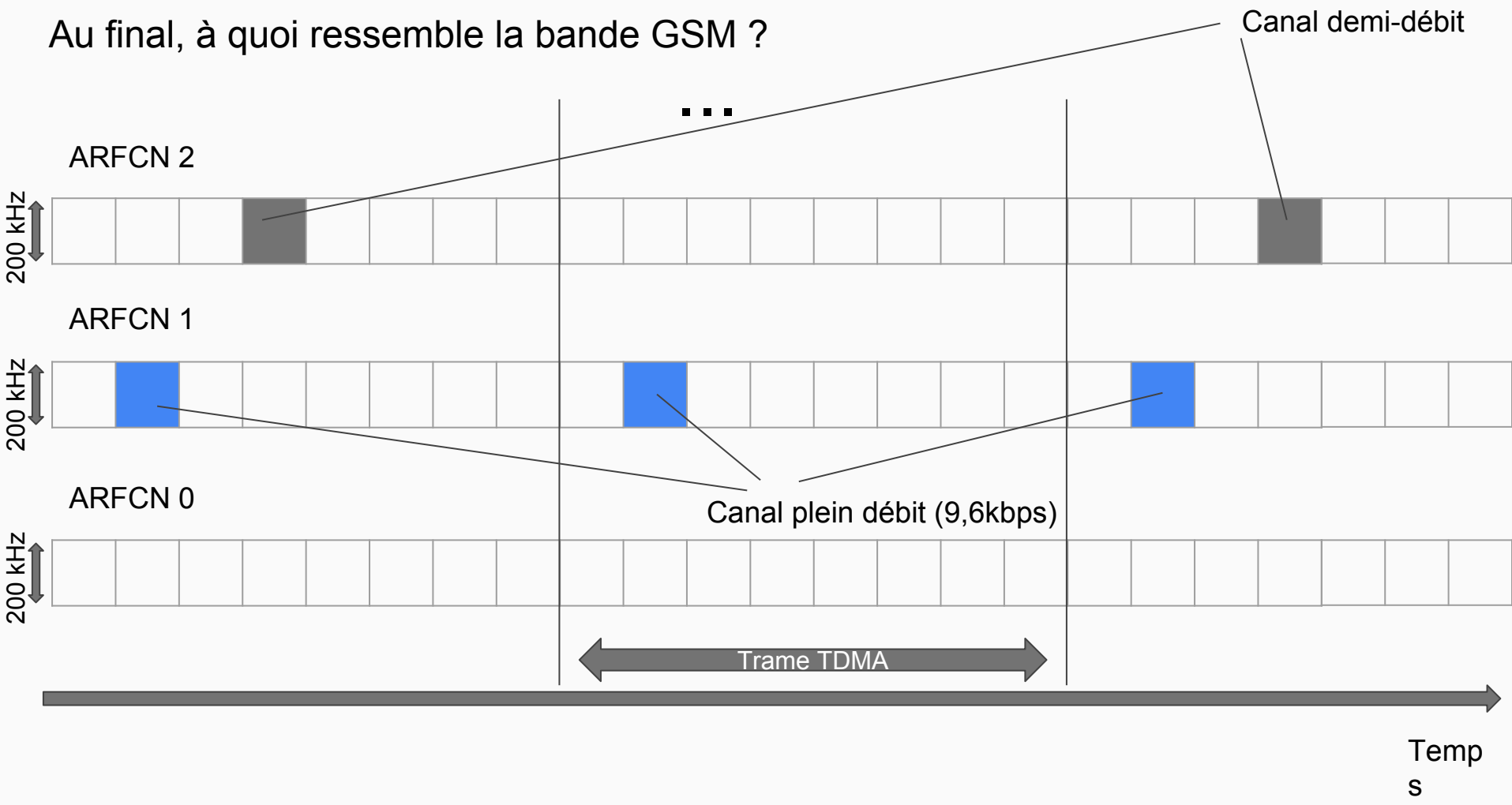
Ressource physique
=
Spectre radio

Canal logique : offre un service aux usagers du système GSM (Mobiles et stations de bases)

- Des canaux logiques communs :
  - BCCH : Identité du réseau, condition d'accès
  - PCH : Localisation d'un mobile
  - AGCH : Allocation de ressources

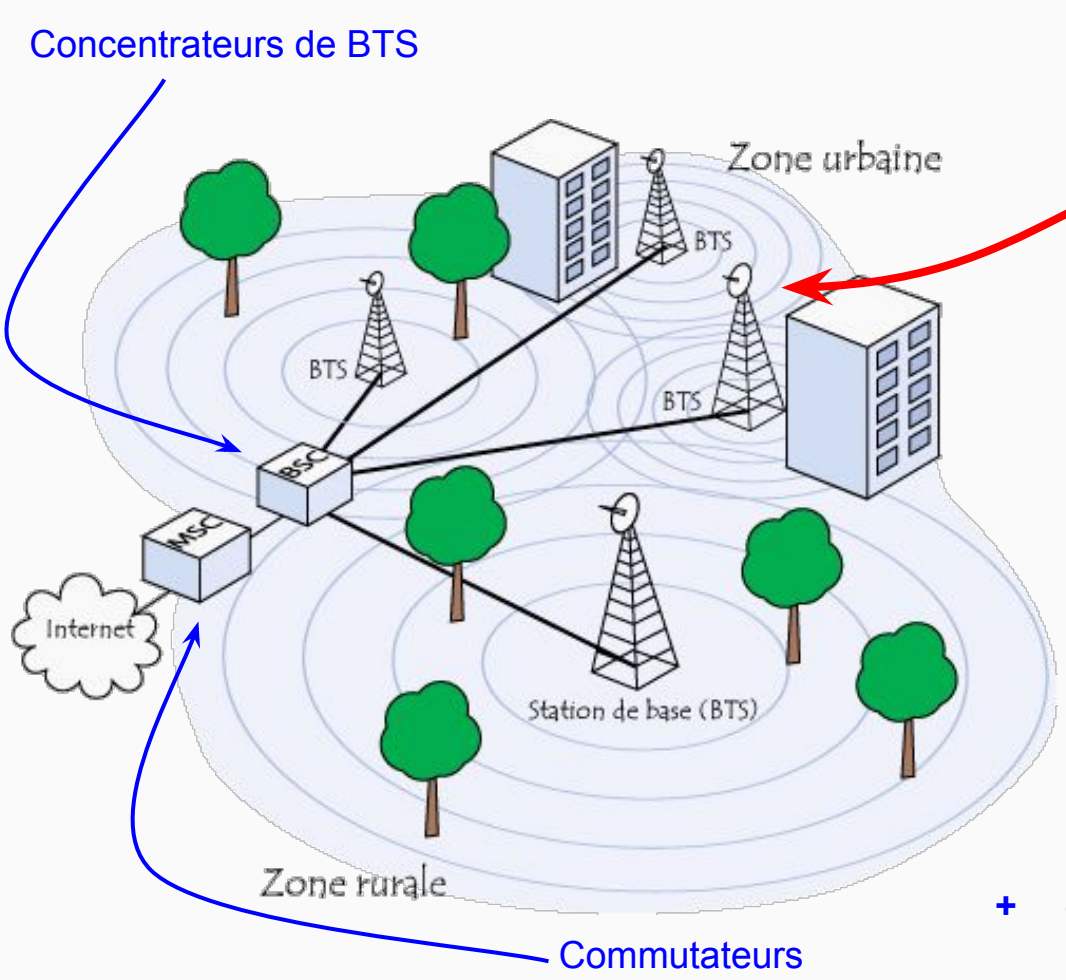
- Des canaux logiques dédiés :
  - TCH : Transmet la voix
  - SDCCH : Signalisation, SMS hors communication
  - SACCH : Contrôle paramètre physique de la liaison, SMS pendant la communication

Au final, à quoi ressemble la bande GSM ?



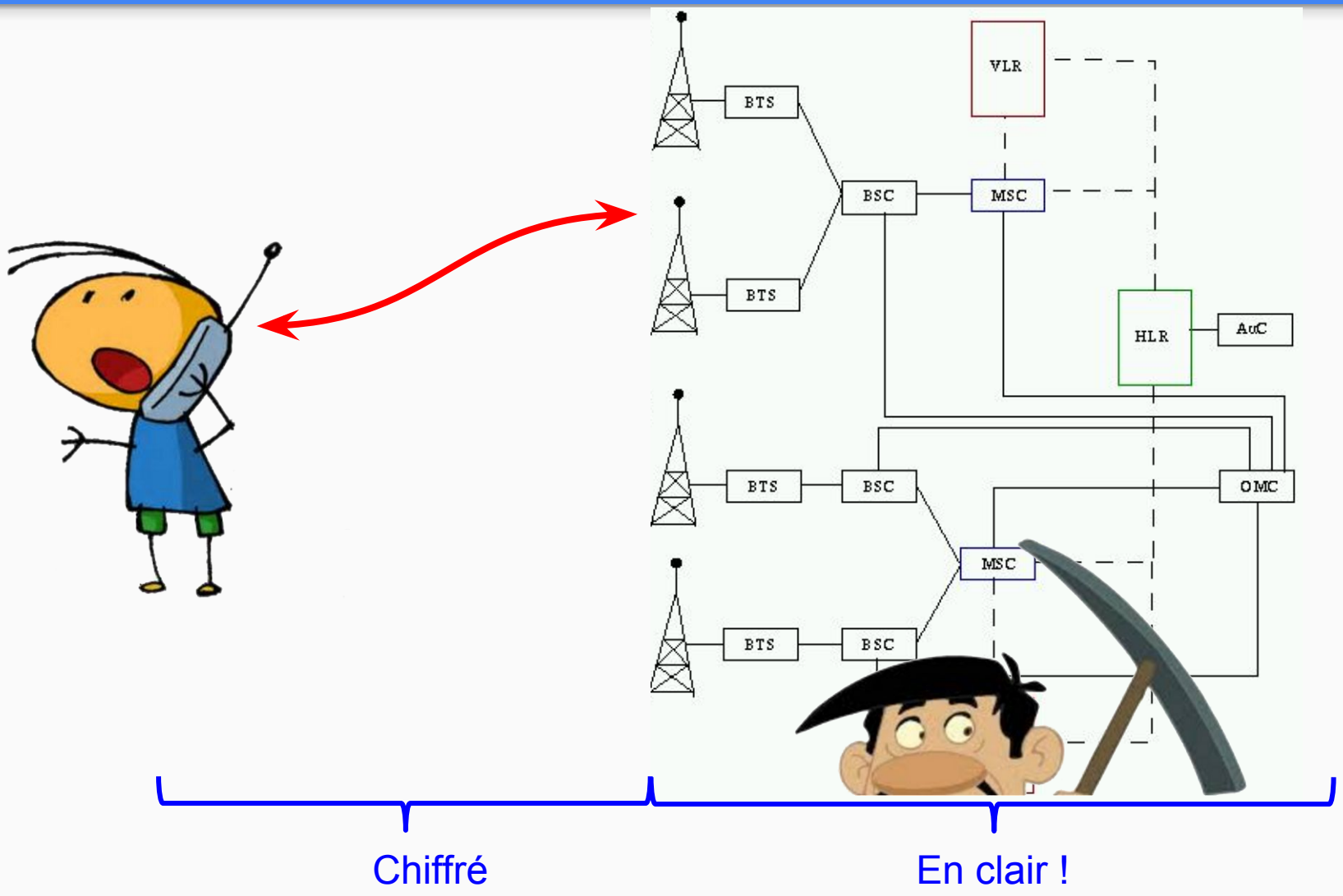
Sécurité :

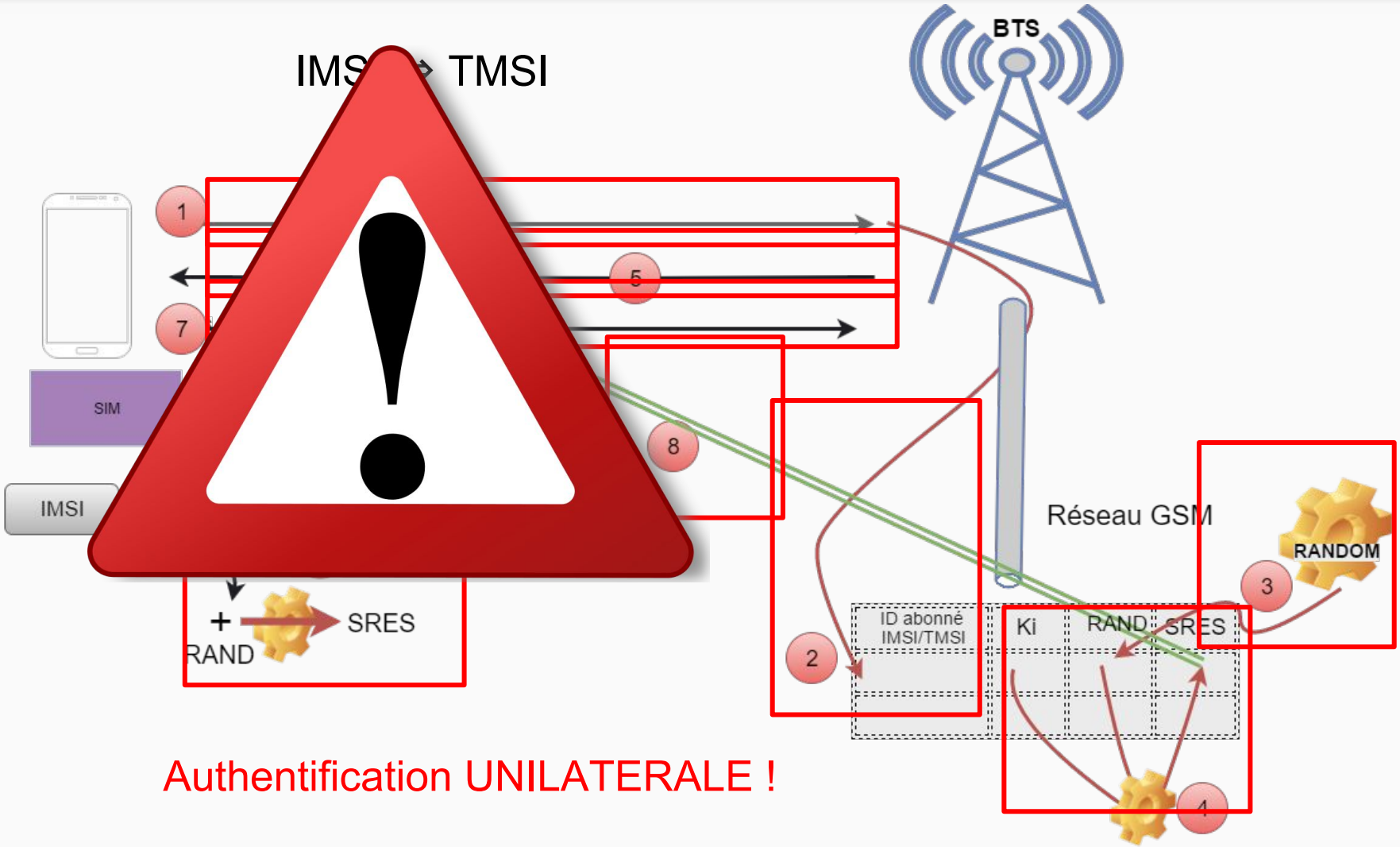
Authentification & Chiffrement



+ des bases de données (HLR, VLR)

Déchiffrer, oui mais quoi ?





Authentification UNILATERALE !

Hey ! Je veux t'envoyer des données chiffrées, je connais ces algos :

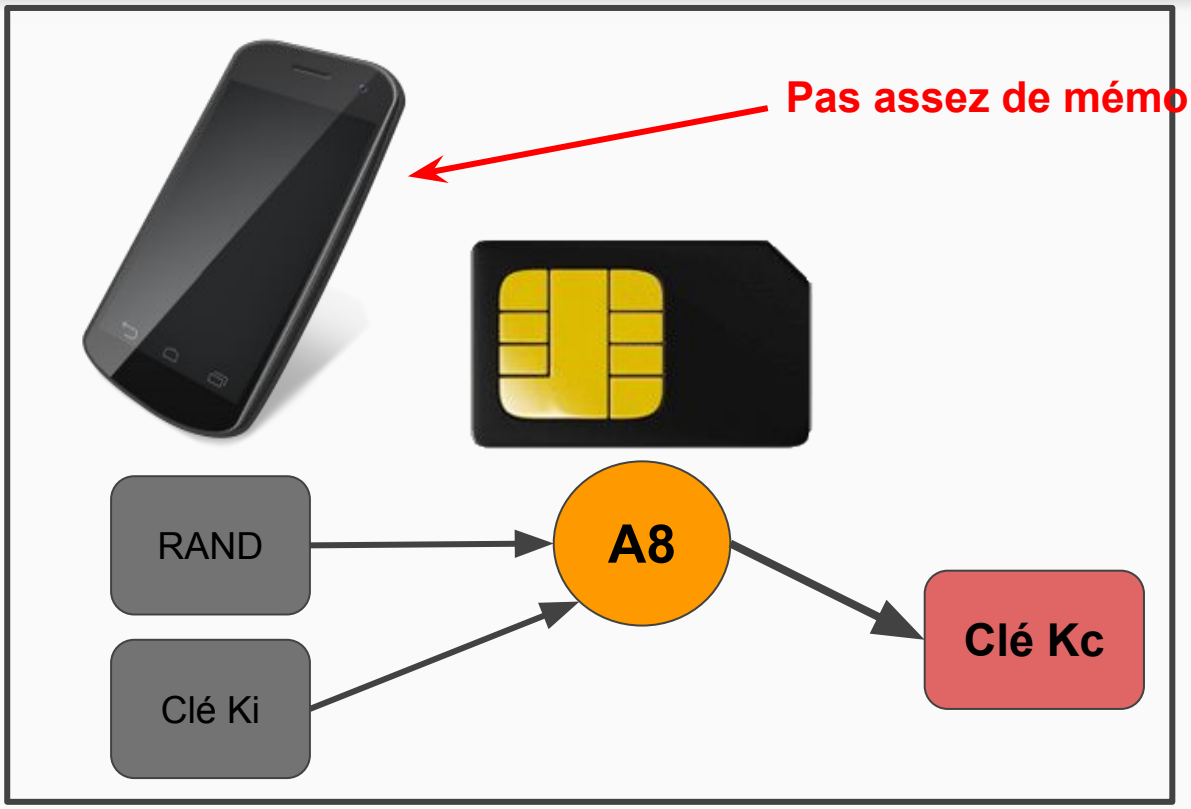
A5/1 A5/3

OK, je connais aussi ces algos !

A5/1 A5/3

Super, on prend le plus fort !

A5/3

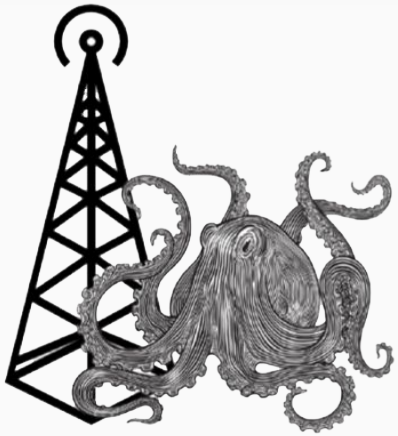


Nouvelle authentication ⇒ Génération d'une nouvelle clé Kc

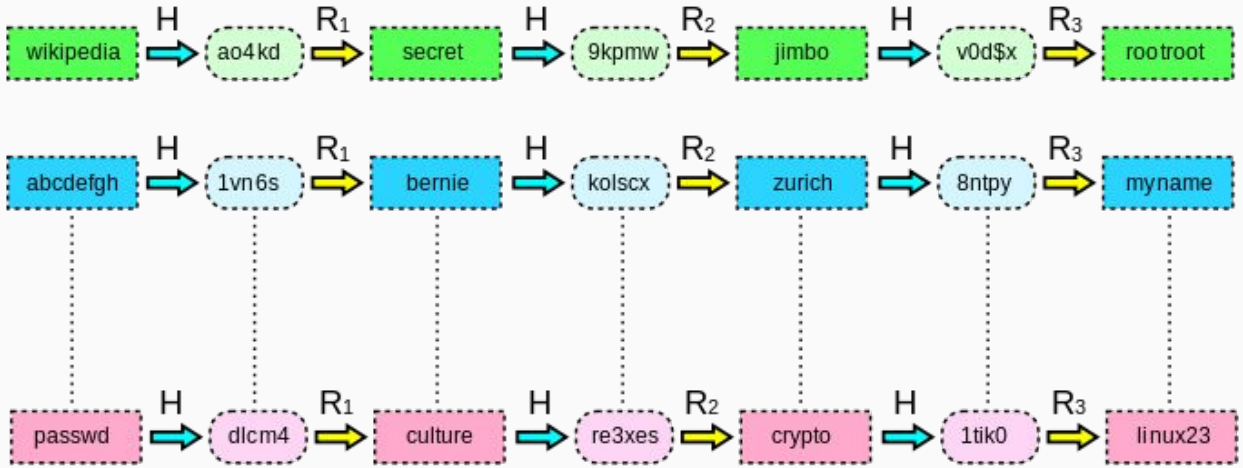
A3 + A5 + A8 = algorithme COMP128 (confidentiel)

Kraken

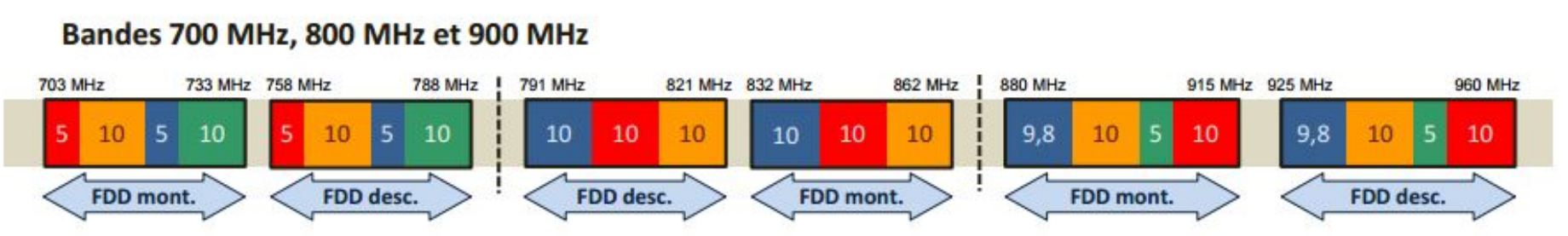
- Projet publié en 2010
- Casse le chiffrement de l'algorithme A5/1
- Configuration matériel facile
- Utilisation de "rainbow tables"



➢ 40 tables
➢ 2 To




I HAVE NO
IDEA WHAT
I'M DOING



Orange | SFR | Bouygues | Free

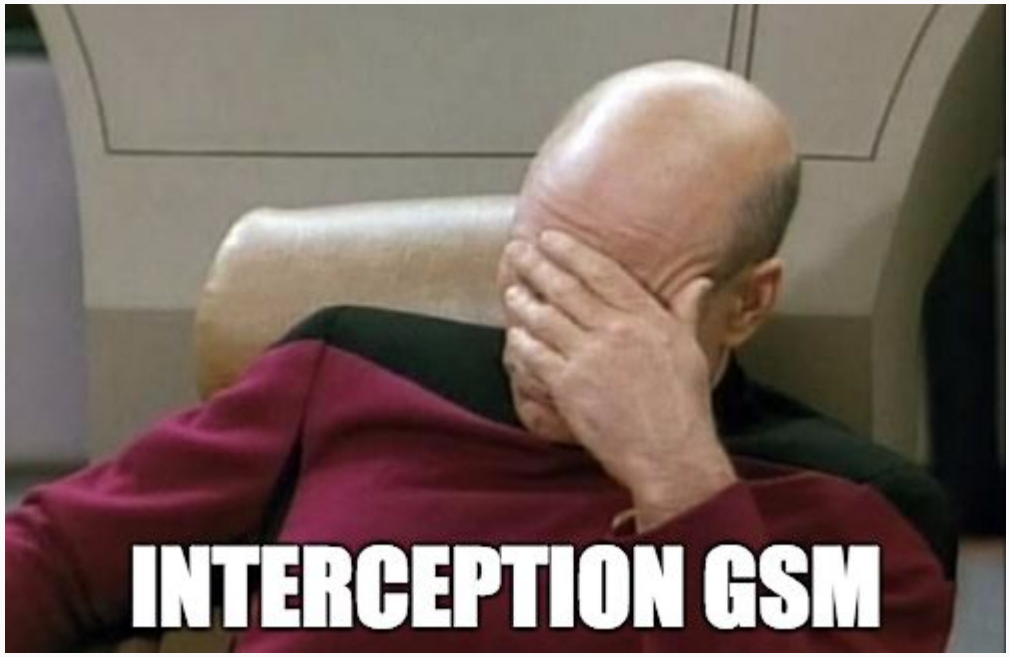
- Ce que nous avons fait :
- Etat de l'art des technologies GSM
- Etude de l'environnement logiciel GNU Radio, GR-GSM et Kraken
- Ecoute du réseau gsm sans fil
- Analyse des trames interceptées

- Applications (plus ou moins légales…) :
- Man-in-the-middle (usurper l'identité d'une BTS pour récupérer des infos sur une station mobile)
- Cartographie du réseau GSM alentour
- Brouillage

- Difficultés rencontrées :

- Installation de logiciels libres
- Conversion laborieuse des Rainbow Tables

Merci de ne pas poser de questions.
(ou alors juste une petite ?)



Bibliographie

[1] "Secret de la correspondance", *Wikipedia*, 2016. [Online]. Available: https://fr.wikipedia.org/wiki/Secret_de_la_correspondance. [Consulté: 29- Apr- 2016].

[2] “Attacking phone privacy”, Karsten Nohl, Security Research Labs, BlackHat 2010 Lecture Notes. [Online] Available: Berlinhttps://srlabs.de/blog/wp-content/uploads/2010/07/Attacking.Phone_.Privacy_Karsten.Nohl_1.pdf

[3] Table of ARFCN values, Telecom ABC. [Online] Available: http://www.telecomabc.com/a/arfcn.html [Consulté : 16-May-2017]

[4] “GSM Layer 3 Messages”, Syed Masroor Ali. [Online] Available: https://fr.scribd.com/doc/97169532/GSM-Layer-3-Messages [Consulté: 17-May-2017]

[5] “Réseaux Mobiles Terrestres”, Daniela Dragomirescu Reyna, LAAS-CNRS, support de cours pour 4ème année RT à l’INSA Toulouse.

[6] “URSP”, site web du fabricant National Instruments. [Online] Available: http://www.ni.com/sdr/usrp/f/

[7] Site officiel de GNU Radio. [Online] Available: http://gnuradio.org/redmine/projects/gnuradio/wiki