OPPIDA

EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Démonstrations d'attaques radios

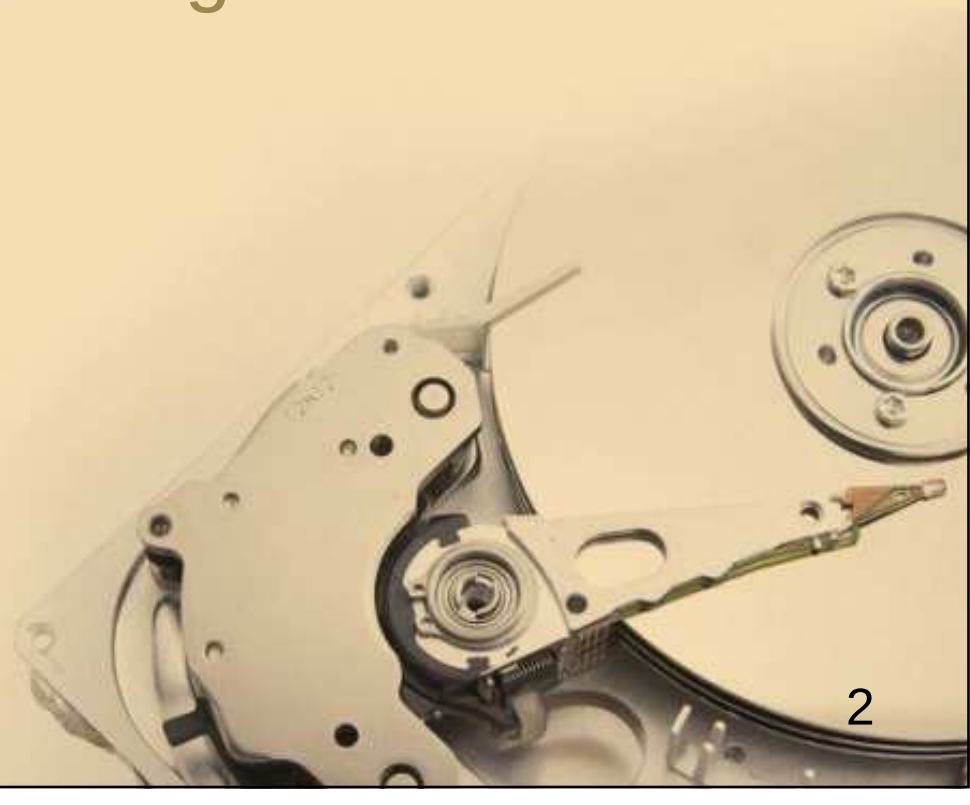
GS Days
18 Mars 2014

Renaud Lifchitz
renaud.lifchitz@oppida.fr

OPPIDA

EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Le développement fulgurant des technologies radios



OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Usages radios grand public & professionnels

- Contrôle d'accès (badges sans contact)
- Ouverture de portes (garage, voiture, …) & interphones
- Alarmes sans fil, capteurs domotiques
- Drones
- Abonnements urbains (cartes Velib', Autolib, Navigo, …)
- Réseaux cellulaires (GSM, téléphonie domestique DECT)
- Bureautique sans fil (souris, clavier, casque)
- Dispositifs médicaux (peacemakers, pompes à insuline, …)
- Dispositifs de navigation (GPS)
- Radiopilotage horaire (GSM NITZ, DCF77, …)
- Talkies-walkies, radios personnelles, PMR

OPPIDA
EXPERT EN SÉCURITÉ DES SYSTÈMES D'INFORMATION

# Principaux standards radios

## Standards IEEE

- 802.11a/b/g/n (WiFi)
- 802.11p (~ DSRC)
- 802.15.1 (Bluetooth)
- 802.15.4 (ZigBee)
- 802.16 (WiMax)

## Réseaux Cellulaires

- GSM900/DCS1800
- DECT
- EDGE
- UMTS
- LTE

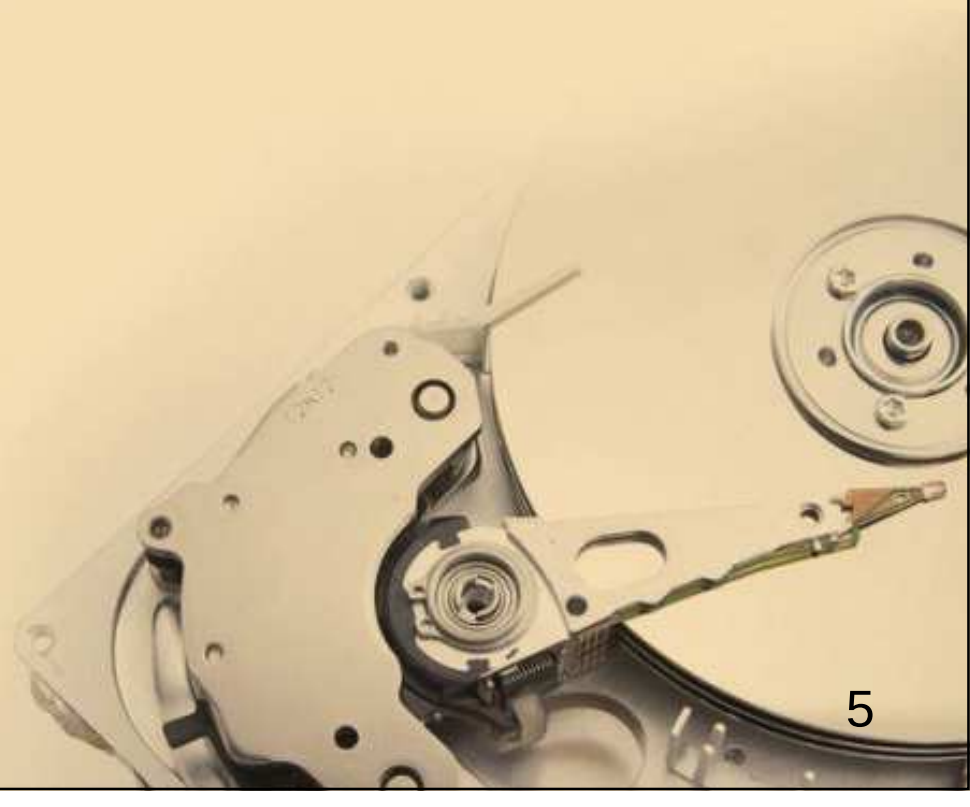
## Autres

- TETRA
- NFC
- RFID

OPPIDA

EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Attaques radio classiques et contre-mesures



OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Ecoute passive

- Simple enregistrement passif à démoduler/décoder pour les protocoles non ou faiblement chiffrés

- Exemples : communications analogiques ou numériques en clair, couche MAC Wi-FI, analyse statistique du trafic chiffré WEP, provisionnement OTA en clair des clés ZigBee …
- Risques : tous !
- Contres-mesures :
  - Mécanismes de chiffrement
  - L'étalement spectral et les sauts de fréquence étaient réputés fiables, ils ne le sont plus

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Brouillage

- Brouillage volontaire :
  - Emission d'un bruit blanc amplifié
- ou brouillage involontaire :
  - Interférences avec d'autres communications radios
  - Obstacles physiques (murs, végétation, …)
- Risques : déni de service, atteinte à l'intégrité
- Contre-mesures :
  - Étalement de spectre (« spread sprectrum »)
  - Saut de fréquence (« frequency hopping »)
  - Pas de contre-mesure miracle…

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

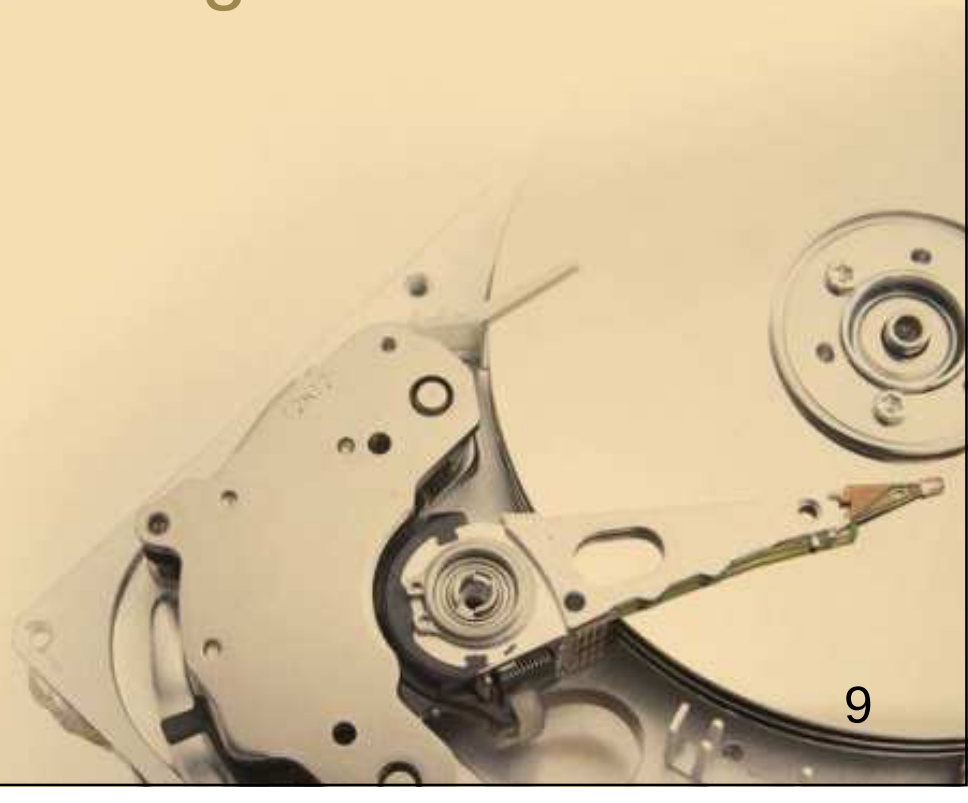
# Usurpation (« spoofing »)

- De nombreux protocoles sont vulnérables à l'usurpation, ne serait-ce parce qu'ils autorisent le rejeu
- Exemples : « bips » d'ouverture de portes de garage, demande d'allocation de canal GSM
- Risques : tous !
- Contre-mesures :
  - Mécanismes anti-rejeu (« nonce » cryptographique)
  - Authentification par challenge

OPPIDA

EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Un nouvel outil d'audit et d'attaque, la radio logicielle



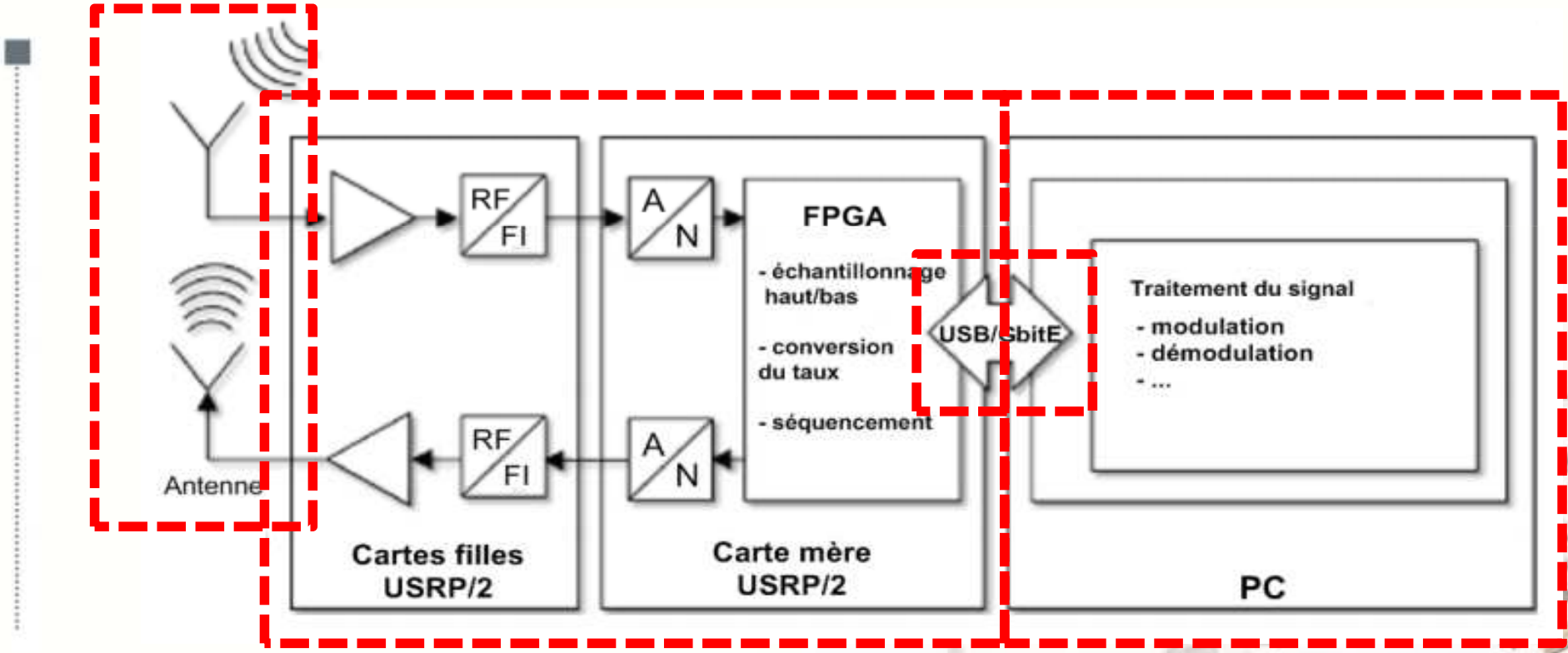
OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Radio logicielle : principes de fonctionnement

- Système de radiocommunication reconfigurable logiciellement (fréquence, modulation et protocole)
- En anglais : SDR (« Software Defined Radio »)
- Intérêts : ne plus utiliser différents équipements pour différents usages et pouvoir mettre à jour facilement l'implémentation de protocoles
- « Radio générique »
- En pratique, l'essentiel du traitement du signal se fait sur un PC client (réception de données brutes I/Q)
- Secteurs en pleine expansion : radioamateurisme, radio mobile, NASA, militaire, radar et guerre électronique

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Radio logicielle : principes de fonctionnement



OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Radio logicielle : plates-formes matérielles
# RTL2832U

- Chipset Realtek RTL2832U des clés USB pour recevoir la TNT

- Caractéristiques théoriques :
  - Réception seule
  - 8 bits I/Q
  - Bande passante : 3,2 MHz à 3,2 MSPS
  - Plage de fréquences : 50 MHz à 2,2 GHz (Elonics E4000, variable selon modèle)
- Environ 20€
- Projet RTL-SDR & périphériques compatibles : http://sdr.osmocom.org/trac/wiki/rtl-sdr

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Radio logicielle : plates-formes matérielles
# HackRF

- Projet ouvert de Michael Ossmann (Great Scott Gadgets)

- Caractéristiques théoriques :
  - Réception et émission (half duplex)
  - 8 bits I/Q
  - Bande passante : 20 MHz à 20 MSPS
  - Plage de fréquences : 30 MHz à 6 GHz


- Environ 180€
- http://greatscottgadgets.com/hackrf/

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Radio logicielle : plates-formes matérielles
# USRP

- Boitiers et cartes spécialisés commercialisés par Ettus Research (National Instruments)

- Caractéristiques théoriques (USRP N210) :
  - Réception et émission (full duplex)
  - 14 bits I/Q
  - Bande passante : 25 MHz à 100 MSPS
  - Plage de fréquences : 0 MHz à 6 GHz (selon carte fille)

- Environ 1500€ (sans carte fille), une des solutions la plus complète et mature
- http://www.ettus.com/home

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

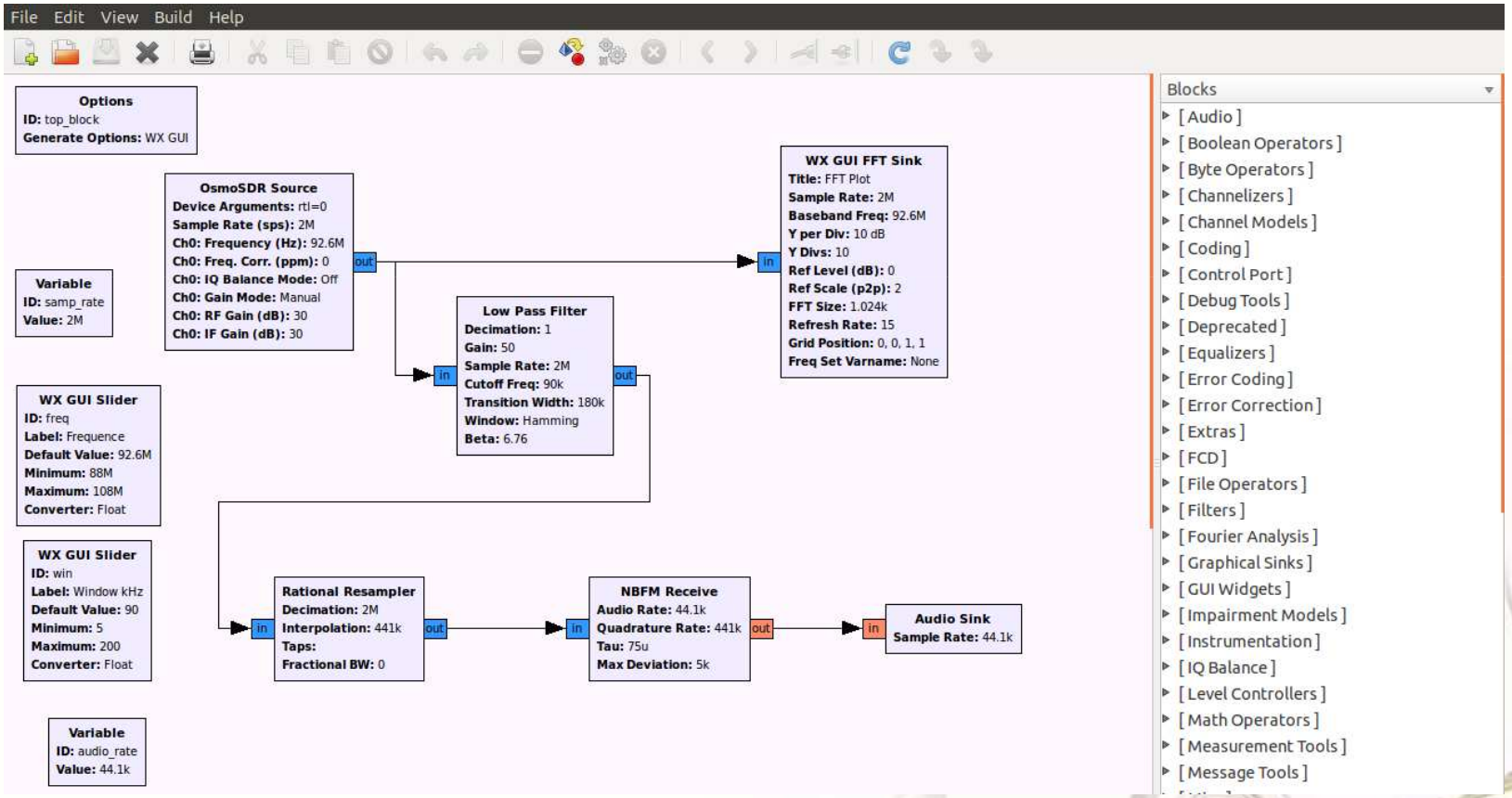
# Radio logicielle : environnement logiciel GNU Radio

- GNU Radio :
  - Framework complet open source de développement en radio logicielle
  - Support de la plupart des périphériques SDR du marché
  - Composants C++ et Python
  - Nombreux filtres de traitement du signal
  - Assistant graphique de conception de circuits SDR :

  GNU Radio Companion
  - Projet : http://gnuradio.org/redmine/projects/gnuradio/wiki

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

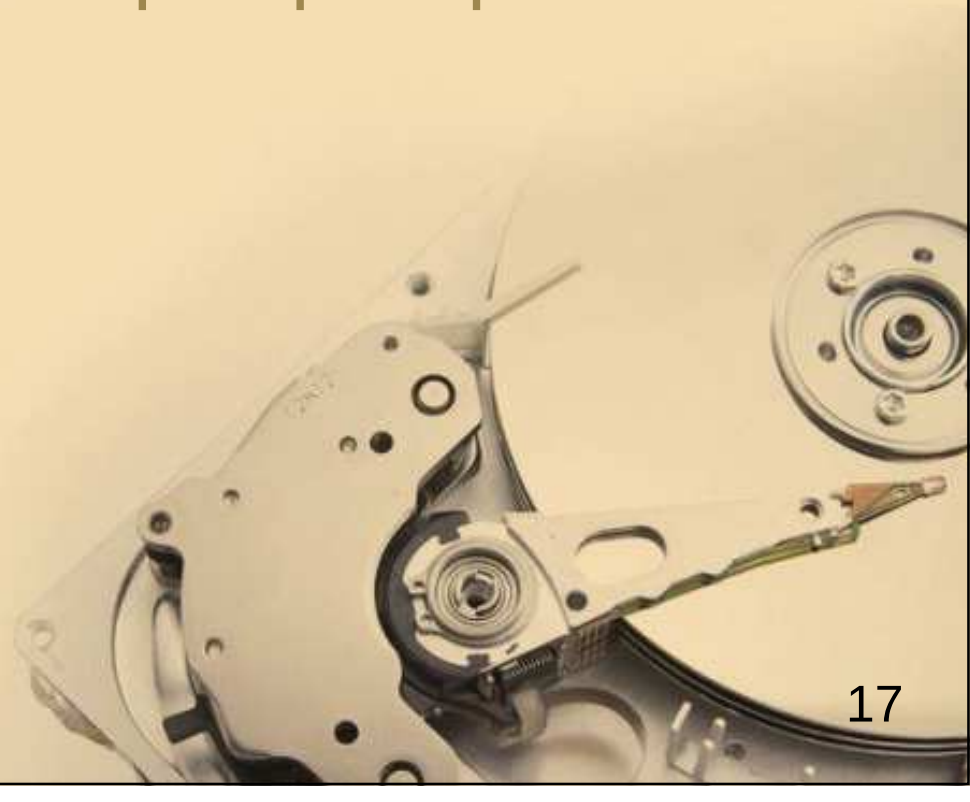
# Radio logicielle : environnement logiciel GNU Radio




**GNU Radio Companion : création d'un récepteur FM logiciel**

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Zoom et démonstrations sur la sécurité de quelques protocoles



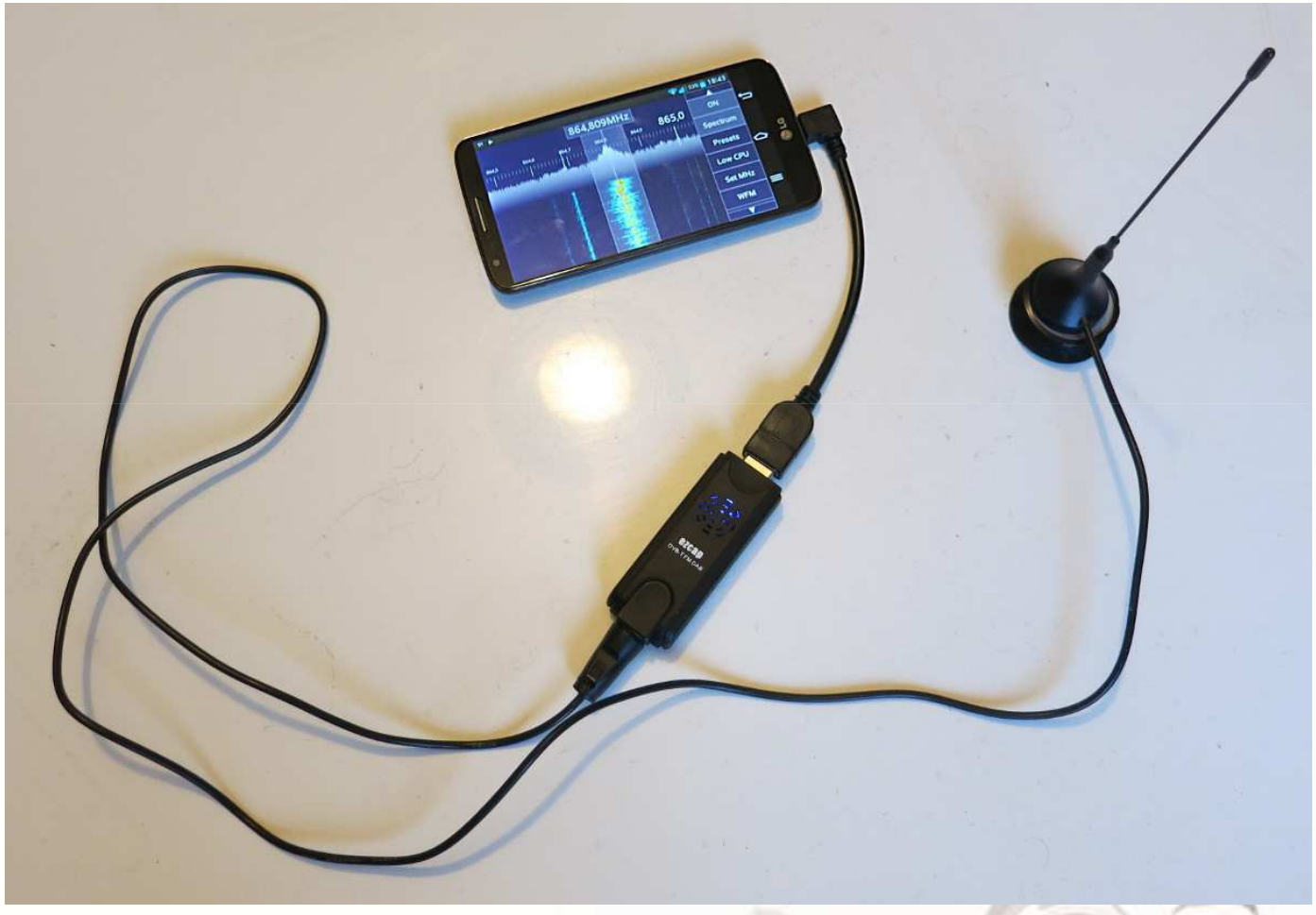
OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Dispositifs radios domestiques

- Beaucoup de dispositifs radios domestiques ne sont pas protégés
- Parmi les équipements voix :
  - Téléphones sans fil domestiques (DECT) faiblement chiffrés ou vulnérables à des attaques de type Man-In-The-Middle : project Dedected
  - Casques sans fil (téléphonie, TV, radio) rarement chiffrés et utilisant la modulation classique WFM sur une bande ISM (ex.: ~ 860 MHz)

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Dispositifs radios domestiques




**Ecoute d'un casque sans fil avec…**
**un smartphone Android (SDR Touch)**

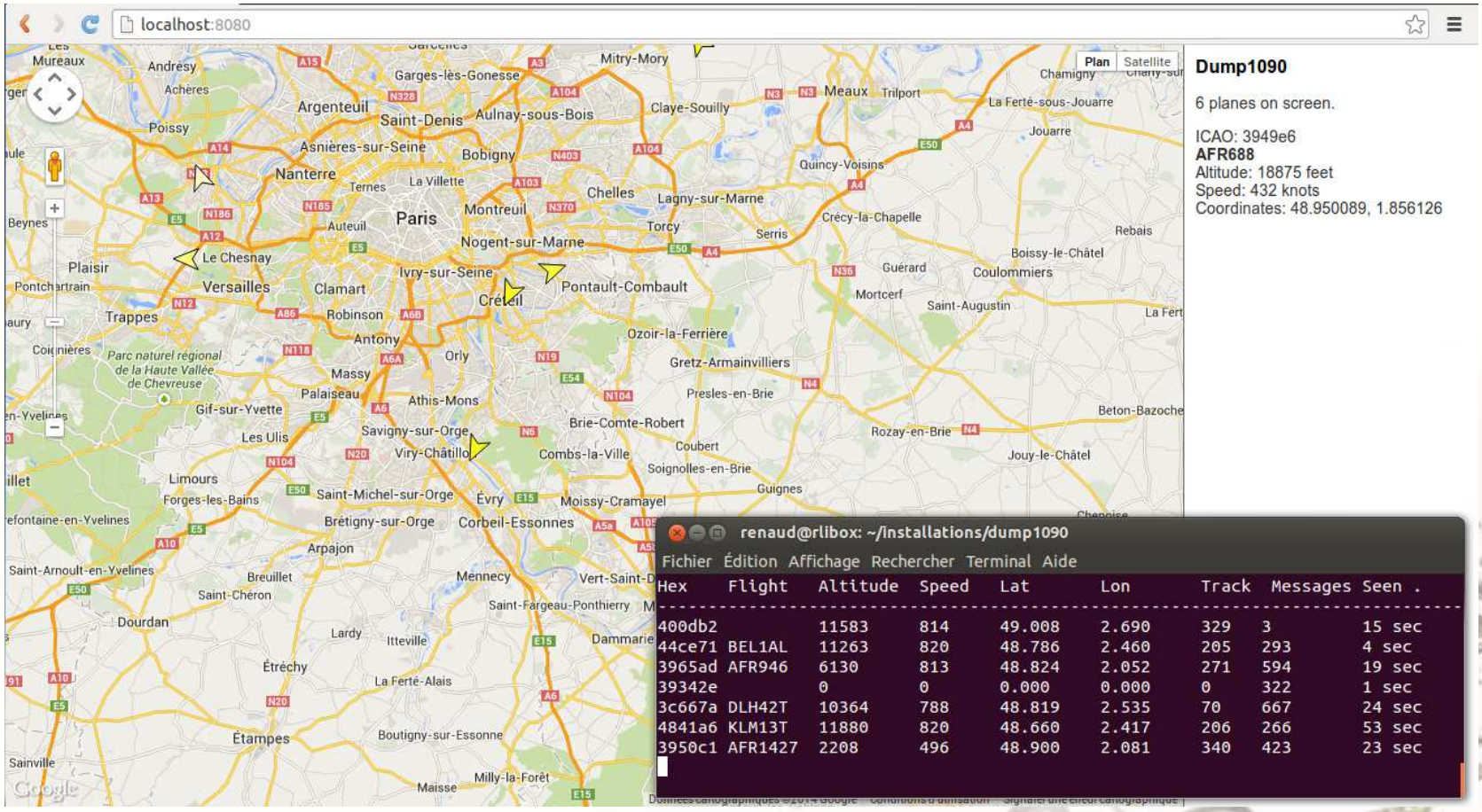
OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Géolocalisation et identification d'avions

- Système américain : les avions sont localisés par les tours de contrôle (radars au sol)
- Système européen : chaque avion se géolocalise seul et envoie sa position au sol par radio
- Protocole ADS-B (Automatic Dependent Surveillance-Broadcast)
- Système de diffusion de la position (latitude/longitude), de l'altitude, de la vitesse et du numéro de vol aux stations au sol
- Protocole simple sans sécurité, non chiffré

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

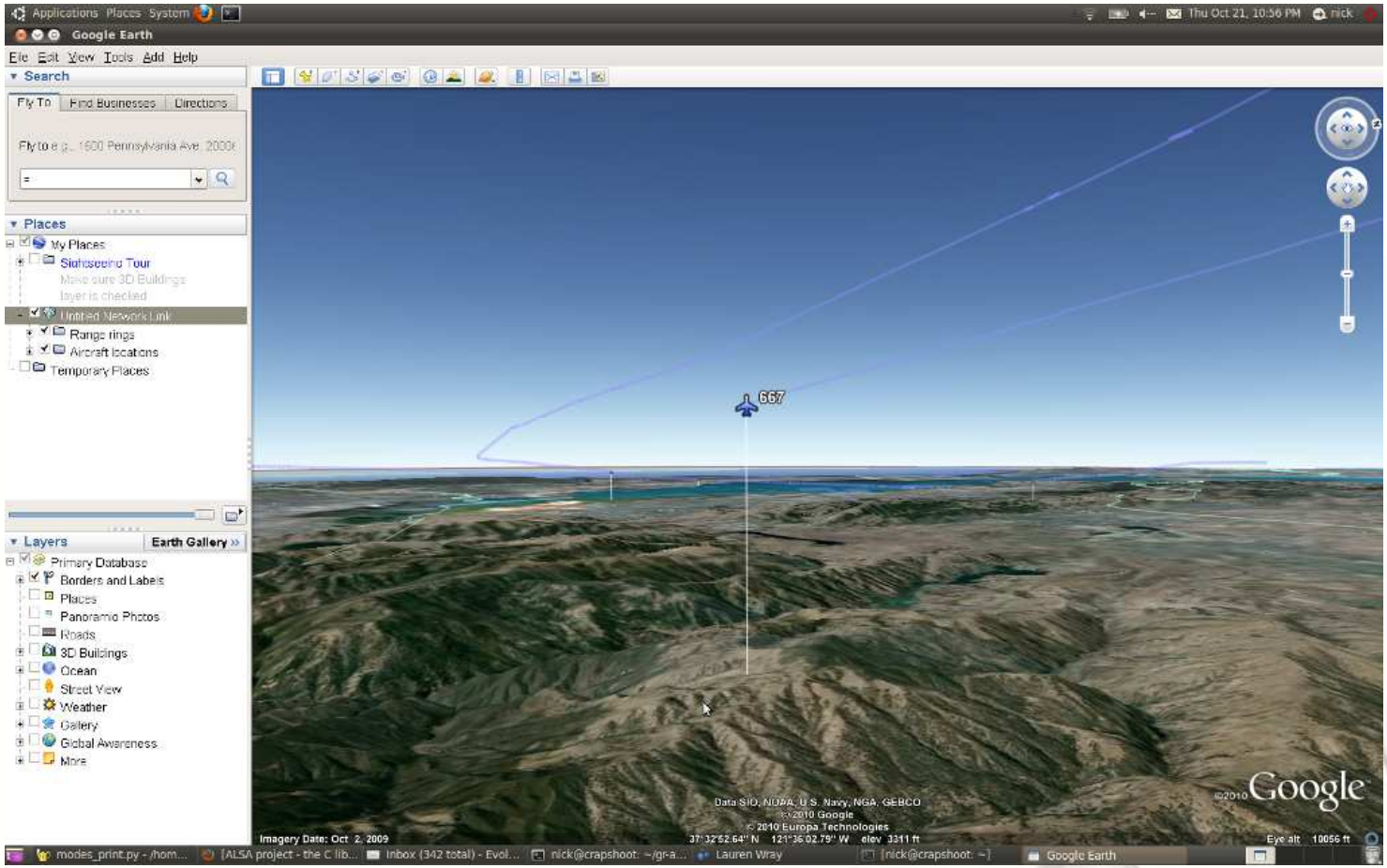
# Géolocalisation et identification d'avions




**Logiciel dump1090 (https://github.com/antirez/dump1090)**

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Géolocalisation et identification d'avions




**Exportation des données géomatiques en KML et visualisation des trajectoires en 3D avec Google Earth**

**(https://github.com/bistromath/gr-air-modes)**

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Géolocalisation d'antennes GSM et d'utilisateurs

- Parcours et écoute sur les 4 bandes GSM (~ 850, 900, 1800, 1900 MHz)
- Chaque cellule GSM (BTS) est identifiée par 4 nombres :
  - MCC: Mobile Country Code
  - MNC: Mobile Network Code
  - LAC: Location Area Code
  - CID: Cell ID
- Recensement des ARFCN utilisées
  (détection d'un pic de fréquence = présence d'une BTS)
- Démodulation et décodage des trames de broadcast d'annonce de BTS
  (numéro de zone LAC et numéro de cellule Cel ID)
- Géolocalisation des antennes
  (par exemple avec Google Maps Geolocation API)

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Géolocalisation d'antennes GSM et d'utilisateurs

- Quelques moyens d'identifier un utilisateur GSM :
  - Numéro de téléphone (MSISDN)
  - IMSI (« International Mobile Subscriber Identity ») : numéro d'abonné international unique = MCC (pays) + MNC (réseau) + HLR (h1 h2) + MSIN
  - CCID : numéro de série de la carte SIM
  - IMEI : numéro de série du téléphone (*#06#)

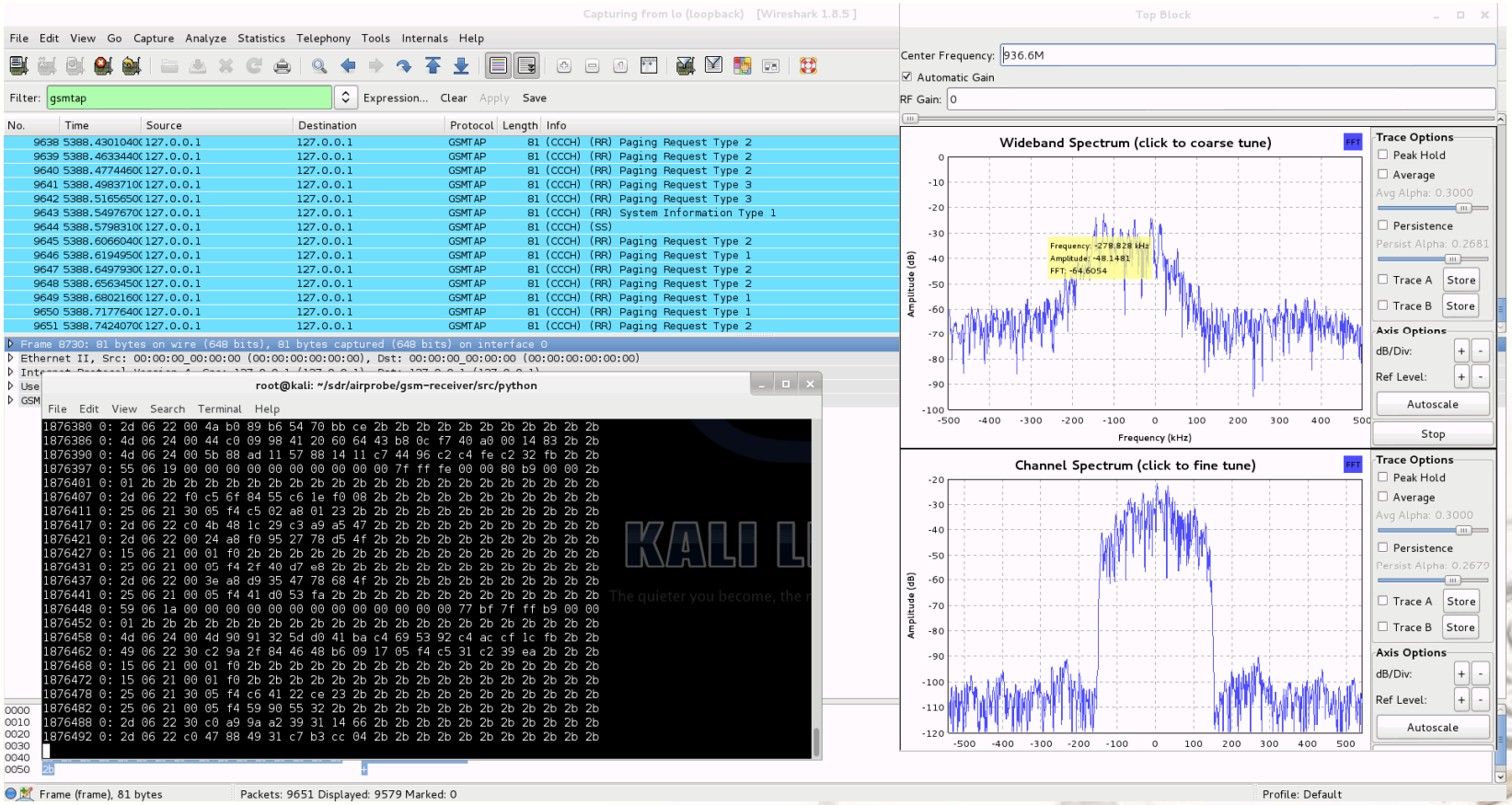
OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Géolocalisation d'antennes GSM et d'utilisateurs

- Normalement, les IMSI utilisateurs ne doivent peu ou pas transiter en clair sur le réseau : utilisation d'identifiants temporaires (TMSI)
- En pratique, les IMSI en clair sont fréquents et nombreux (implémentation du protocole GSM imparfaite, charge importante des équipements, reconnexions fréquentes au réseau, …)
- Il est donc facile d'avoir des statistiques précises sur :
  - Les pays d'origine des utilisateurs
  - Leur opérateur GSM d'origine
  - Les réseaux sur lesquels ils sont
  - Les BTS à lesquelles ils se rattachent
  - L'activité de signalisation qu'ils engendrent (SMS, appels, …)

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Géolocalisation d'antennes GSM et d'utilisateurs

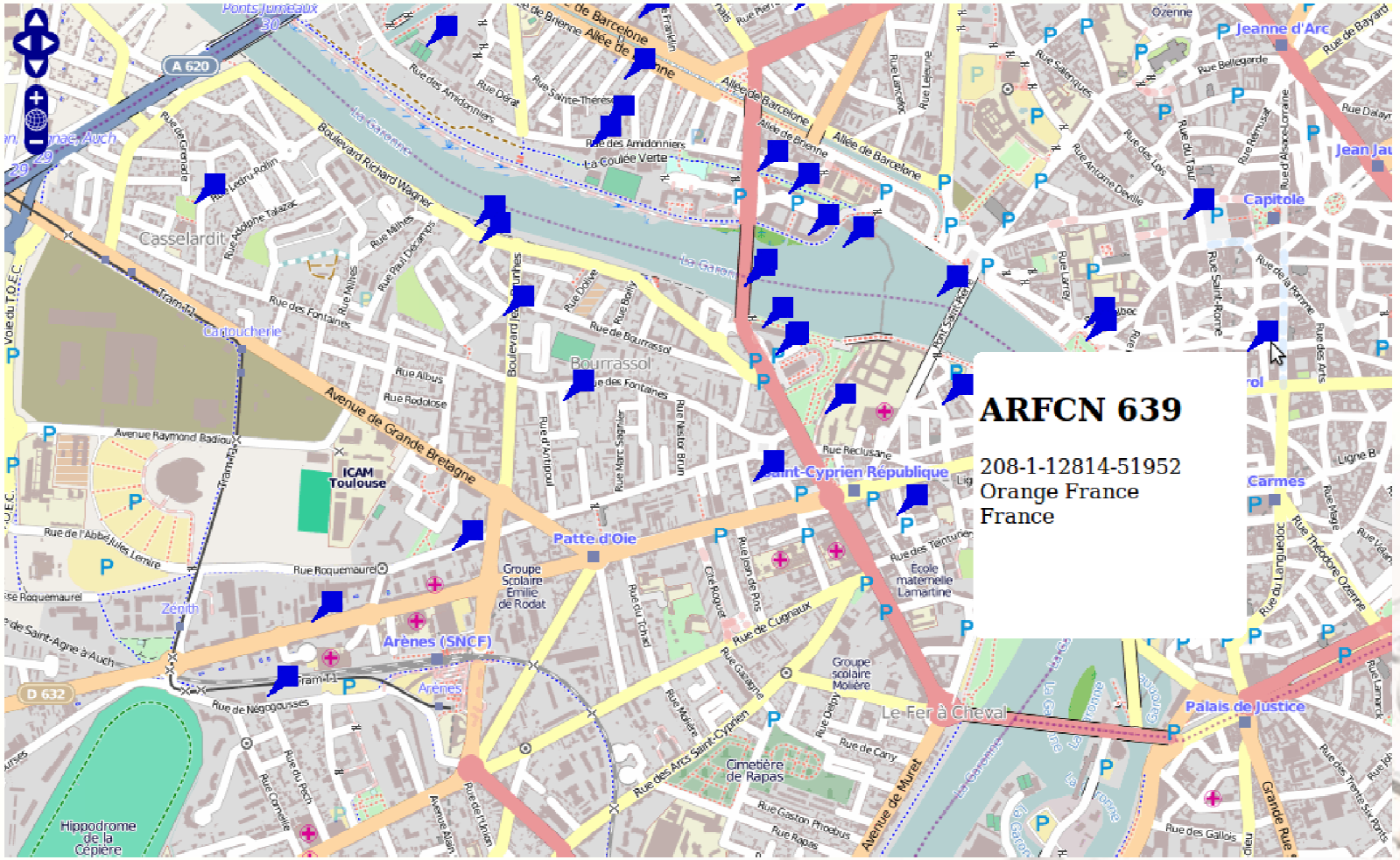



**Projet AirProbe**

**(https://svn.berlin.ccc.de/projects/airprobe/)**

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Géolocalisation d'antennes GSM et d'utilisateurs




**Projet OsmoGeo de l'auteur (utilise OsmocomBB) :**

**http://code.google.com/p/osmogeo/**

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Géolocalisation d'antennes GSM et d'utilisateurs

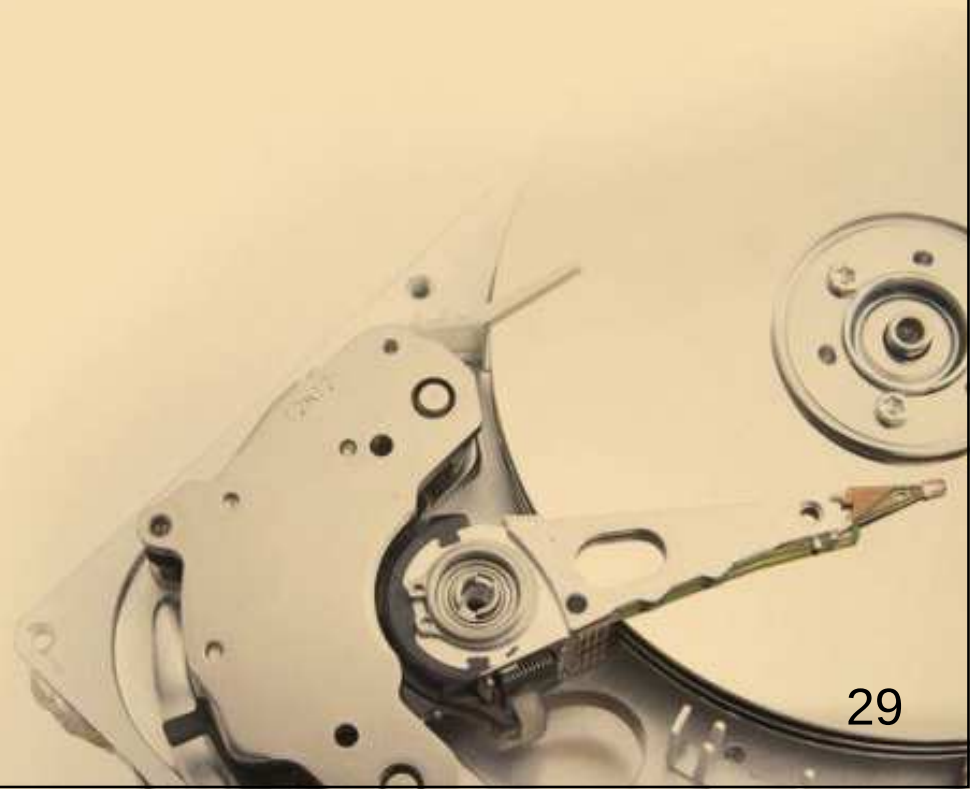
```
renaud@primelt:~/documents/confs/thsf2012/osmogeo$ ./osmogeo.py
Launching Layer1...
Launching Layer23...
Launching TrafficMonitor...
Launching OsmoController...
[26/05/2012 10:57:11] 208103590627461 (208, 100, 'France', 'S.F.R.') ('79', 'Downlink')
[26/05/2012 10:57:13] 208107586434930 (208, 100, 'France', 'S.F.R.') ('82', 'Downlink')
[26/05/2012 10:57:14] 208101055287003 (208, 100, 'France', 'S.F.R.') ('720', 'Downlink')
[26/05/2012 10:57:15] 208103689603143 (208, 100, 'France', 'S.F.R.') ('720', 'Downlink')
5 mapped BTS!
[26/05/2012 10:57:17] 206102300442033 (206, 100, 'Belgium', 'Mobistar') ('755', 'Downlink')
Immediate Paging for Call ARFCN=36
Immediate Paging for Call ARFCN=5
[26/05/2012 10:57:20] 208104084360583 (208, 100, 'France', 'S.F.R.') ('666', 'Downlink')
[26/05/2012 10:57:24] 208200850892724 (208, 200, 'France', 'Bouygues Telecom') ('880', 'Downlink')
[26/05/2012 10:57:24] 208201903151915 (208, 200, 'France', 'Bouygues Telecom') ('880', 'Downlink')
11 mapped BTS!
```

**Projet OsmoGeo de l'auteur (utilise OsmocomBB) :**

**http://code.google.com/p/osmogeo/**

OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Perspectives



OPPIDA
EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

# Perspectives

- La plupart des protocole radios souffre d'une mauvaise conception : absence de chiffrement, d'authentification, de signature, de mécanismes anti-rejeu et anti-brouillage
- Dans l'embarqué, de nombreuses implémentations radios sont vulnérables au fuzzing (déni de service, exécution de code arbitraire !)
- Penser à la sécurité dès la conception du protocole, pas après son implémentation !
- Oublier le « time-to-market » et considérer la sécurité comme un réel besoin
- La sécurisation du périmètre physique est parfois la seule alternative à l'heure actuelle…

OPPIDA

EXPERT EN SÉCURITÉ
DES SYSTÈMES D'INFORMATION

Merci !

Des questions ?