



L'environnement radio, de plus en plus difficile à protéger

JSSI

17 Mars 2014

Renaud Lifchitz

renaud.lifchitz@oppida.fr



Présentation d'Oppida



Présentation d'Oppida

- Cabinet conseil spécialisé dans la sécurité des systèmes d'information fondé en 1998
- Deux établissements : Saint-Quentin en Yvelines, Toulouse
- 25 consultants, 3,1 M€ de CA
- Habilitation de la société, ses locaux et son personnels
- Certification ISO-9001: version 2008
- Accréditation en tant que laboratoire d'essai : ISO17025



Le développement fulgurant des technologies radios



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 (pacemakers, pompes à insuline, ...)
- Dispositifs de navigation (GPS)
- Radiopilotage horaire (GSM NITZ, DCF77, ...)
- Talkies-walkies, radios personnelles, PMR

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

DECT



Autres

- TETRA
- NFC
- RFID



Attaques radio classiques et contre-mesures



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 :
 - mécanisme de chiffrement
 - L'étalement spectral et les sauts de fréquence étaient réputés fiables, ils ne le sont plus

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 spectrum »)
 - Saut de fréquence (« frequency hopping »)
 - Pas de contre-mesure miracle...

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

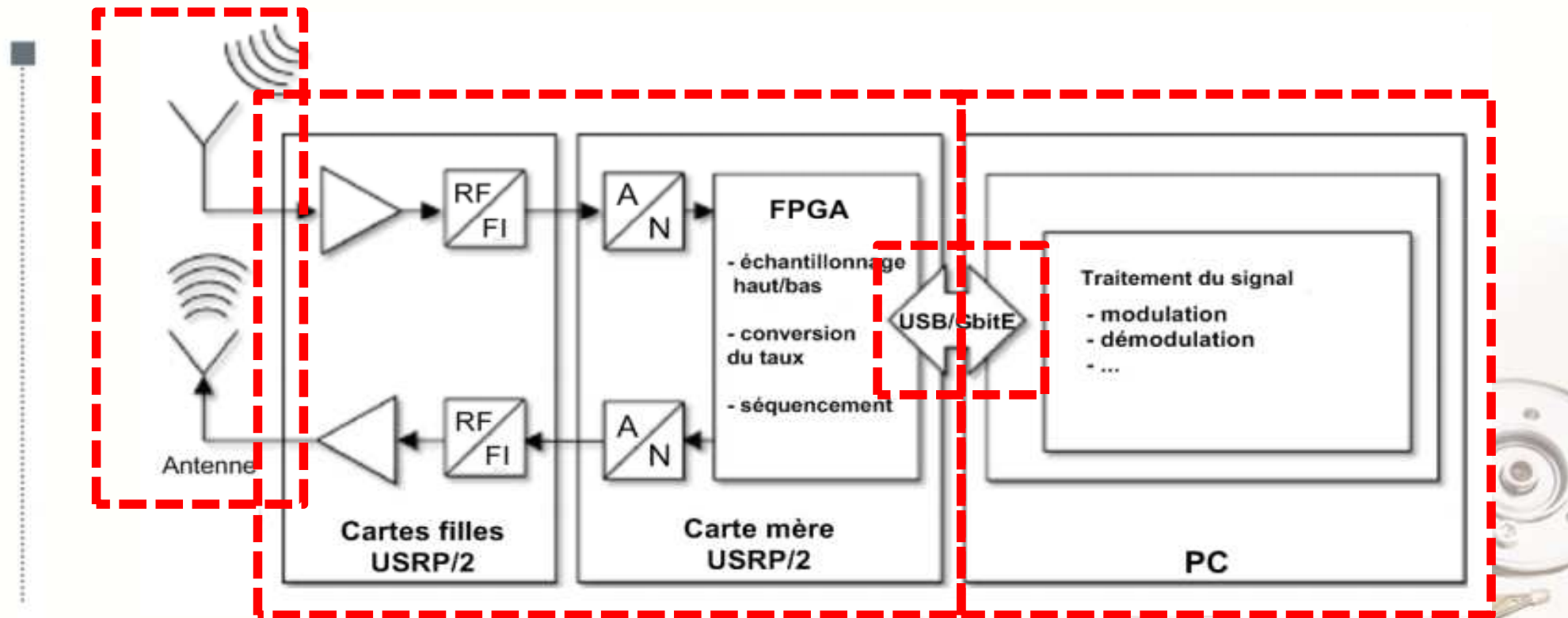
Un nouvel outil d'audit et d'attaque, la radio logicielle



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

Radio logicielle : principes de fonctionnement



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>



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/>

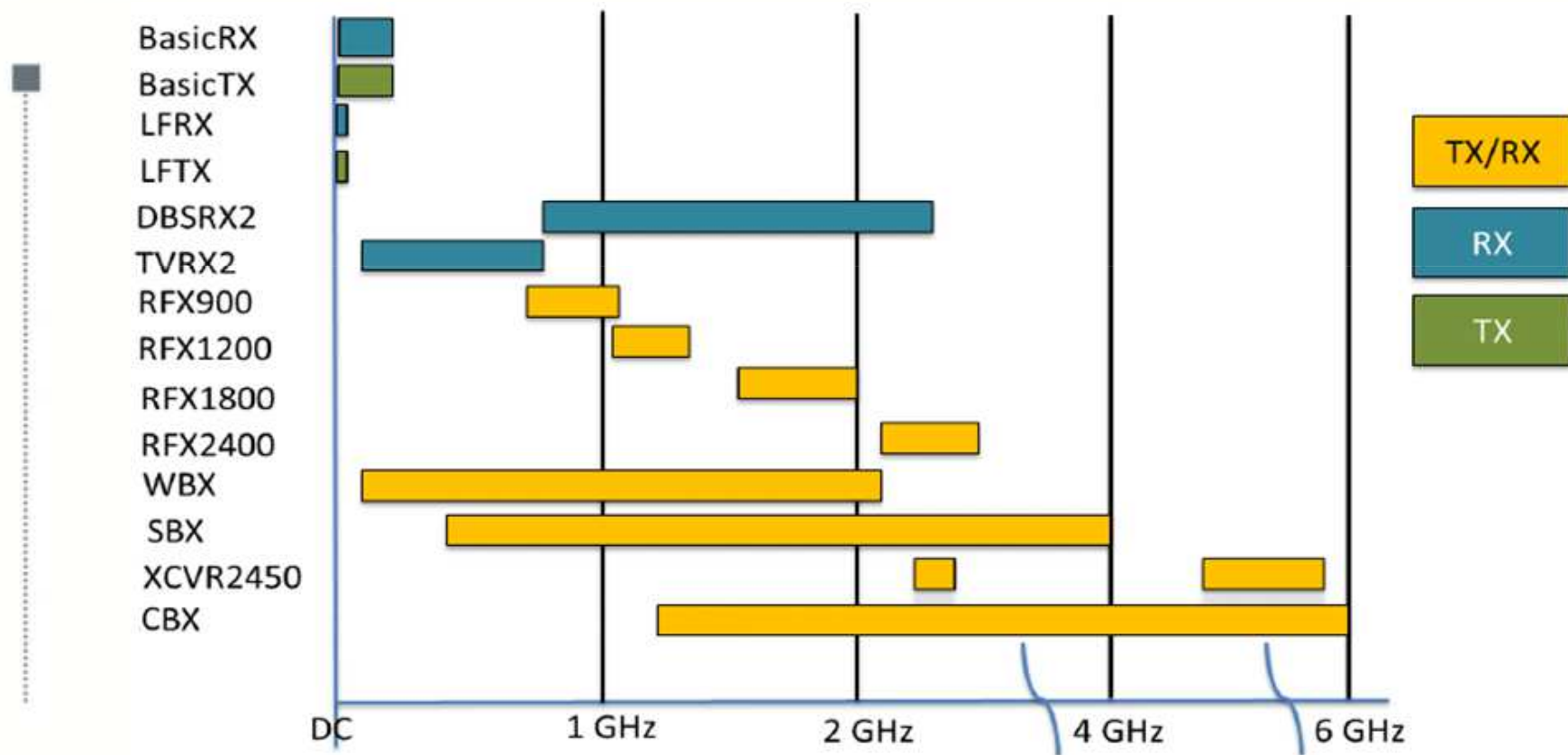


Radio logicielle : plates-formes matérielles USRP

- Boîtiers 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>



Radio logicielle : plates-formes matérielles USRP

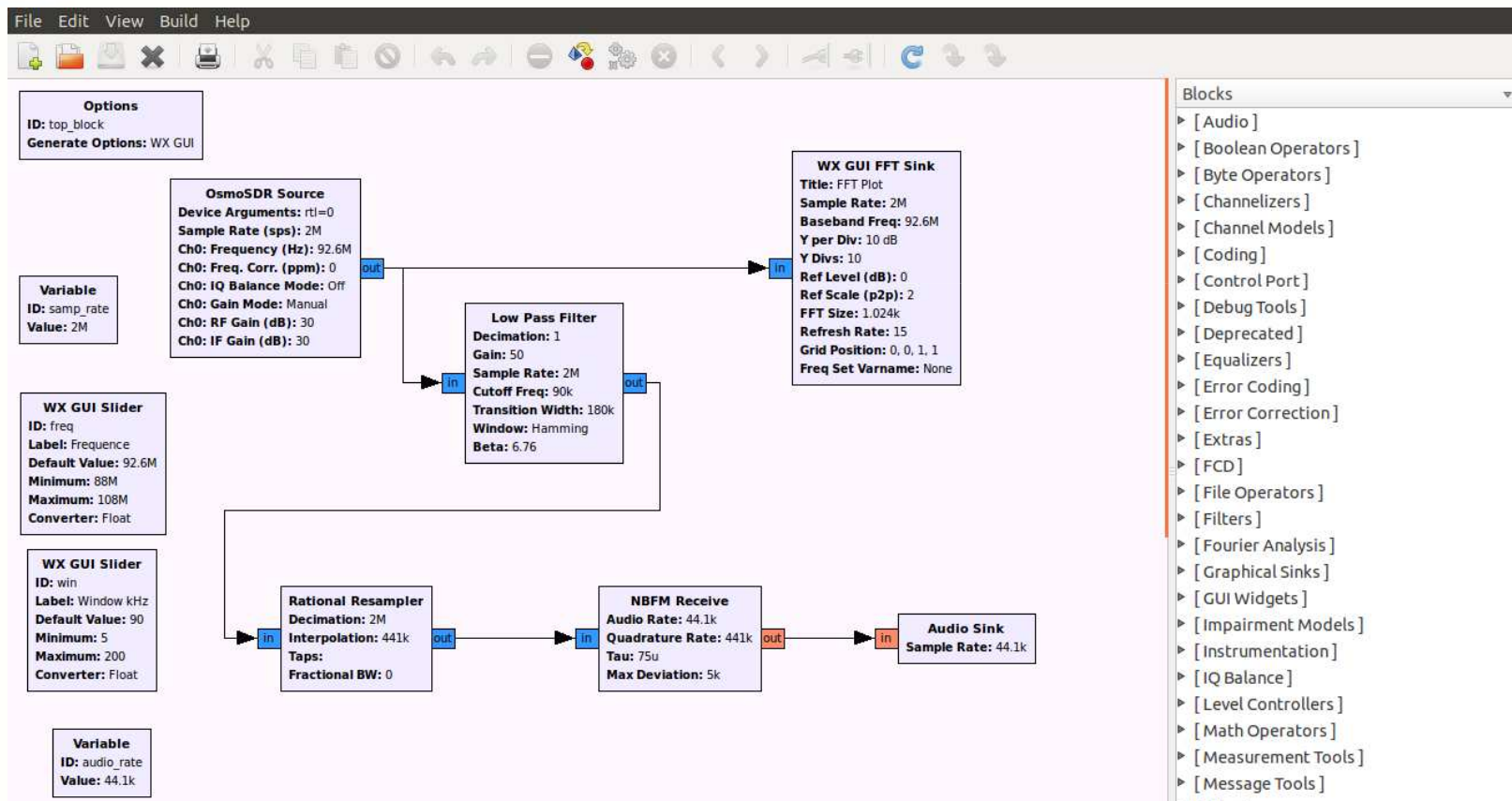


Couverture des cartes filles USRP Ettus

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>

Radio logicielle : environnement logiciel GNU Radio



GNU Radio Companion : création d'un récepteur FM logiciel

Zoom et démonstrations sur la sécurité de quelques protocoles



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)

Dispositifs radios domestiques

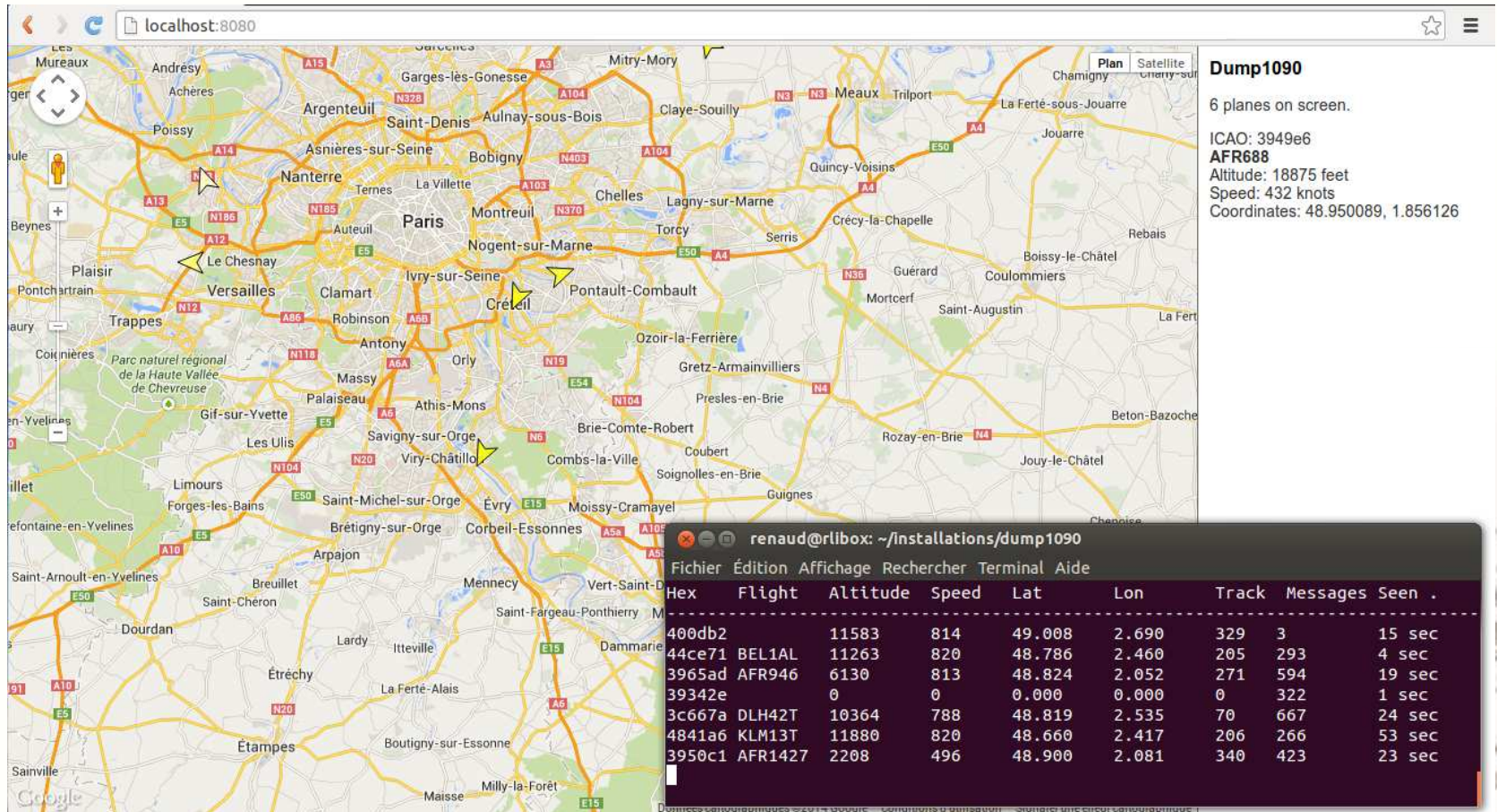


**Ecoute d'un casque sans fil avec...
un smartphone Android (SDR Touch)**

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

Géolocalisation et identification d'avions

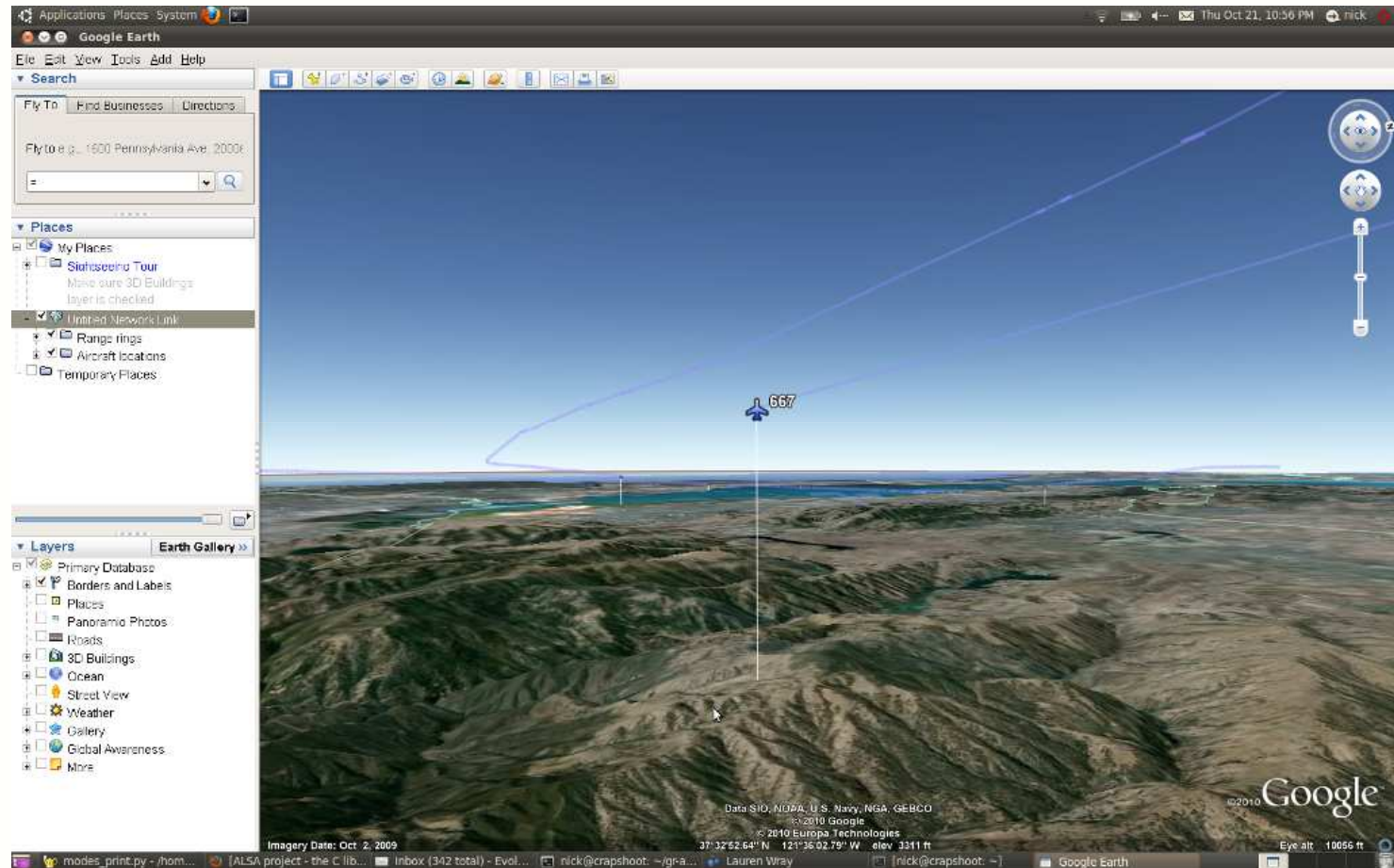


Dump1090
6 planes on screen.
ICAO: 3949e6
AFR688
Altitude: 18875 feet
Speed: 432 knots
Coordinates: 48.950089, 1.856126

Hex	Flight	Altitude	Speed	Lat	Lon	Track	Messages	Seen
400db2		11583	814	49.008	2.690	329	3	15 sec
44ce71	BEL1AL	11263	820	48.786	2.460	205	293	4 sec
3965ad	AFR946	6130	813	48.824	2.052	271	594	19 sec
39342e		0	0	0.000	0.000	0	322	1 sec
3c667a	DLH42T	10364	788	48.819	2.535	70	667	24 sec
4841a6	KLM13T	11880	820	48.660	2.417	206	266	53 sec
3950c1	AFR142T	2208	496	48.900	2.081	340	423	23 sec

Logiciel dump1090 (<https://github.com/antirez/dump1090>)

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>)

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)

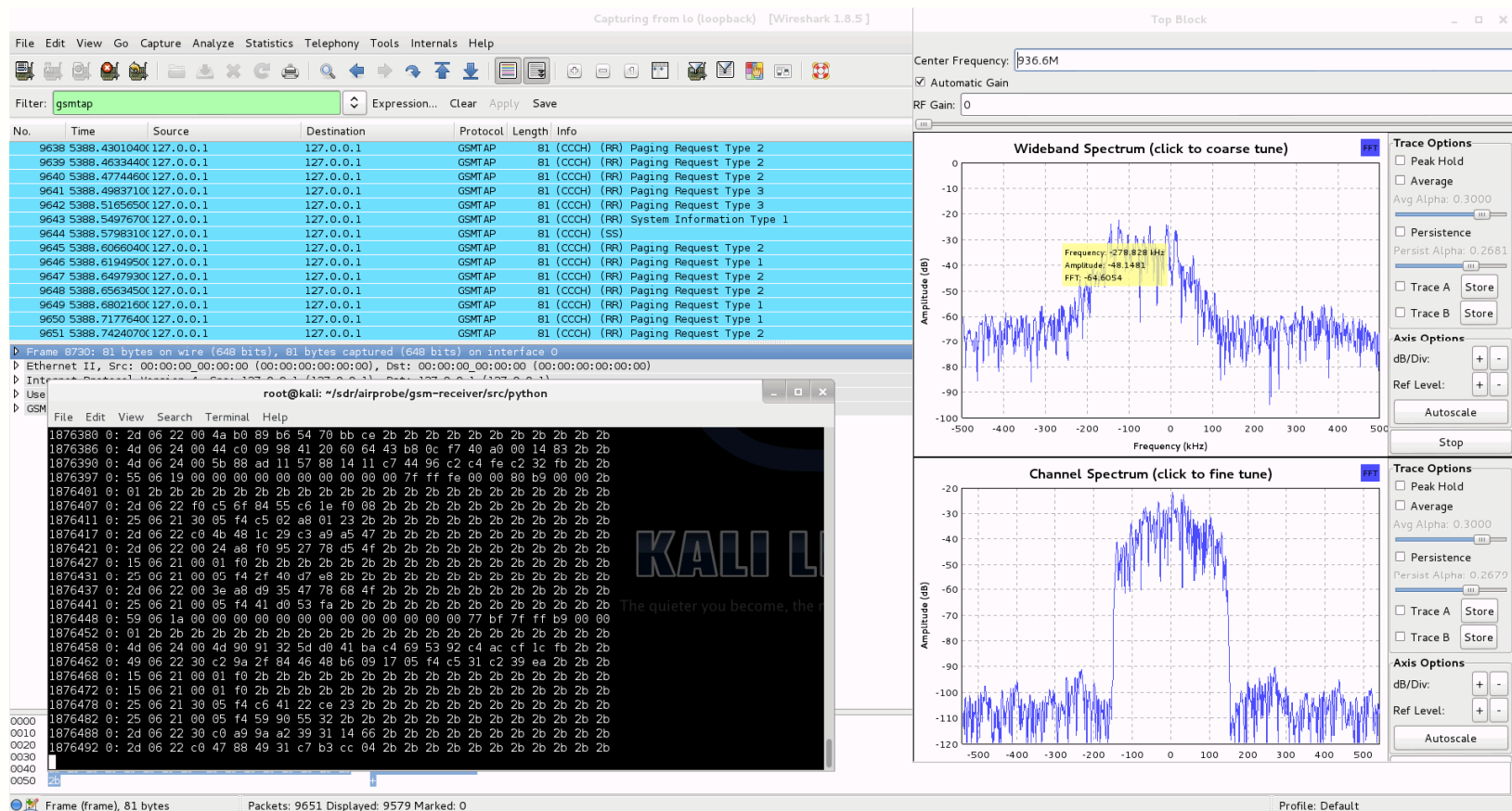
Géolocalisation d'antennes GSM et d'utilisateurs

- 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#)

Géolocalisation d'antennes GSM et d'utilisateurs

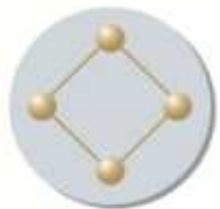
- Normalement, les IMSI utilisateurs ne doivent peu ou pas transiter en clair sur le réseau : utilisation d'identifiants temporaires (TMSI)
- En pratique, les IMSI en clair sont fréquents et nombreux (implémentation du protocole GSM imparfaite, charge importante des équipements, reconnections fréquentes 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, ...)

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/osmogeol/>

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/>

Perspectives



Perspectives

- La plupart des protocoles 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...

Merci !

Des questions ?

