SSTIC 2014

ANALYSE DE LA SÉCURITÉ DES MODEMS DES TERMINAUX MOBILES

Benoit MICHAU (ANSSI)

benoit.michau [à] ssi.gouv.fr

MISSION

Mise en place d'un banc de test radio
pour les terminaux mobiles récents.

- USRP et OpenBTS pour la 2G
- Equipement radio 3G commercial
- Station de base LTE logicielle Amarisoft
- Développement d'un coeur de réseau 3G / LTE minimal
- Intégration de scénarios de test

DANS LE RESPECT DE LA RÉGLEMENTATION

POURQUOI ?

Historique et évolutions des technologies mobiles, et de l'évaluation de leur sécurité.

Des centaines de millions de terminaux 2G + 3G + LTE pour les plus récents.

GSM, GPRS ET EDGE

- Technologies de la fin des années 80 et des années 90
- Cryptographie non publique (54 puis 64 bits)
- Niveau de sécurité théorique faible (en 2014)
- Nombreuses études et évaluations pratiques de sécurité, logiciels en source ouverte (OpenBTS, Osmocom, Kraken, ...)

Sécurité:

3G

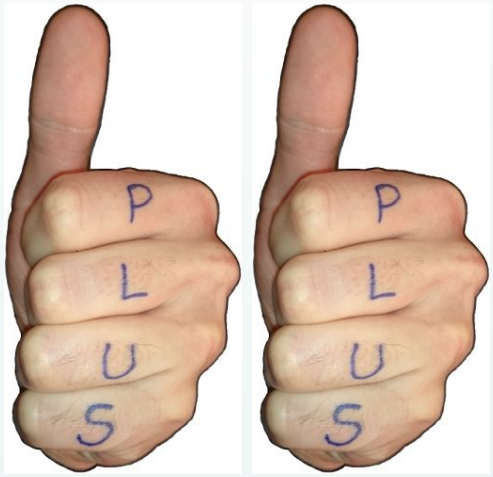
- Technologies de la fin des années 90
- Cryptographie publique (128 bits)
- Niveau de sécurité théorique bon
- Peu d'études de sécurité, aucun système pratique et peu coûteux disponible

Sécurité:

LTE

- Technologies de la fin des années 2000
- Cryptographie publique (128 / 256 bits)
- Niveau de sécurité théorique bon, améliorations par rapport à la 3G
- Peu d'études de sécurité, peu de systèmes pratiques et peu coûteux disponibles

Sécurité:



QUOI ?

Mécanismes de protection des communications radio-mobiles.

TESTER LES IMPLÉMENTATIONS

- **Procédures non sécurisées**
  - Décodage des canaux de diffusion des antennes (CSN.1, ASN.1)
  - Demande d'accès au réseau et établissement des canaux radio duplex
- **Gestionnaires protocolaires**
  - Plusieurs protocoles (RRC, MM, GMM, EMM)
  - Procédures d'authentification
  - Procédures de mise en oeuvre des algorithmes cryptographiques (chiffrement, contrôle d'intégrité)
- Mécanismes de **gestion / allocation mémoire** au sein du modem, et du terminal

TESTS SUR LES SYNTAXES

- Modifications simples sur le format des messages
- Exemple: encapsulation TLV d'un élément de longueur fixée
- Déclencher des corruptions mémoires

TESTS SUR LES PROTOCOLES

- Modifications plus avancées sur les machines à états
- Exemples: déséquencement du gestionnaire de mobilité, abaissement du niveau d'authentification ou de contrôle d'intégrité
- Contourner les procédures de sécurité

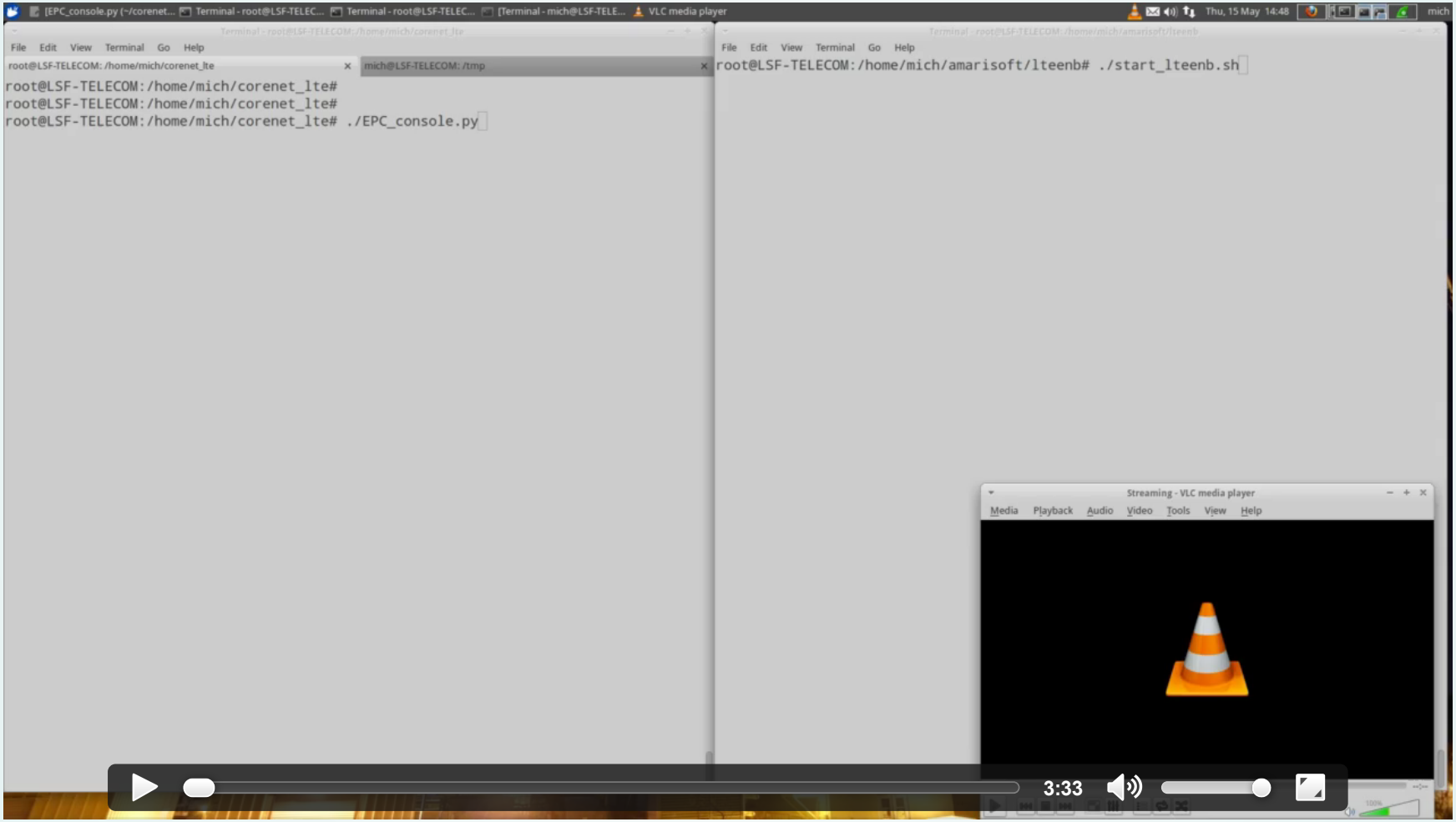
COMMENT ?

Mettre en place un banc de test.

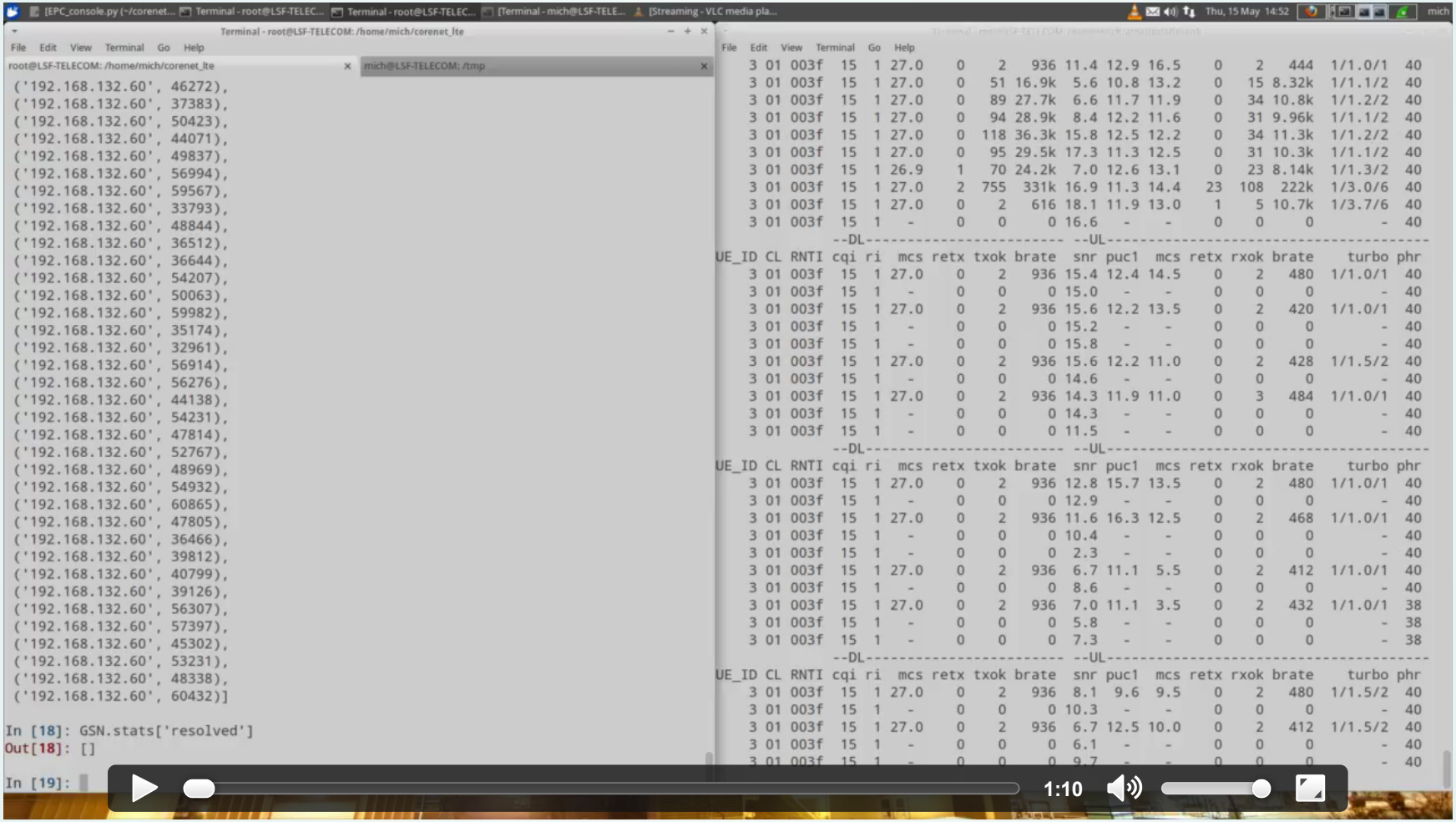
PRÉREQUIS

- Disposer d'un budget (matériel radio, cage de Faraday, licences logicielles)
- Etre persuasif (prêt de matériel, équipements radio, terminaux)
- Lire les normes 3GPP
- Développer, interfacer et configurer
- Tester...
- ... persévérer

VIDÉO 1 : CONNEXION AU BANC DE TEST LTE



VIDÉO 2 : SCAN DE MESSAGES LTE EMM



POUR QUELS RÉSULTATS ?

Les failles existent,
chez de nombreux fabricants et éditeurs ;

nombreux les corrigent ;

certains, non...

QUELQUES EXEMPLES

INDICATION DE CHIFFREMENT DU CANAL RADIO INEXISTANTE

Quel que soit le terminal, fabricant, éditeur ou opérateur

CORRUPTION MÉMOIRE LORS DE L'AUTHENTIFICATION 3G

- Paramètre AUTN du message AUTHENTICATION CIPHERING REQUEST en mode PS
- Encapsulation TLV, mais longueur fixée à 16 octets : encodage d'un paramètre plus long
- Corruption d'une variable globale du RTOS et écrasement d'autres variables globales du système
- Exception levée par le RTOS et redémarrage du modem
- Bug similaire à celui découvert par Ralf-Philipp Weinmann en 2009
- Corrigé par l'éditeur

CONNEXION LTE SANS CONTRÔLE D'INTÉGRITÉ (MODE EIA0)

ATTACHEMENT D'UN MOBILE À UN FAUX RÉSEAU LTE

- Mobile précédemment connecté et authentifié à son réseau légitime
- Usurpation des codes réseaux légitimes (MCC, MNC) par le faux réseau
- Demande du faux réseau pour :
  - réutiliser le vecteur d'authentification précédent
  - utiliser les modes EEA0 (sans chiffrement) et EIA0 (sans contrôle d'intégrité)
- Acceptation du mobile...
- Vulnérabilité corrigée par l'éditeur

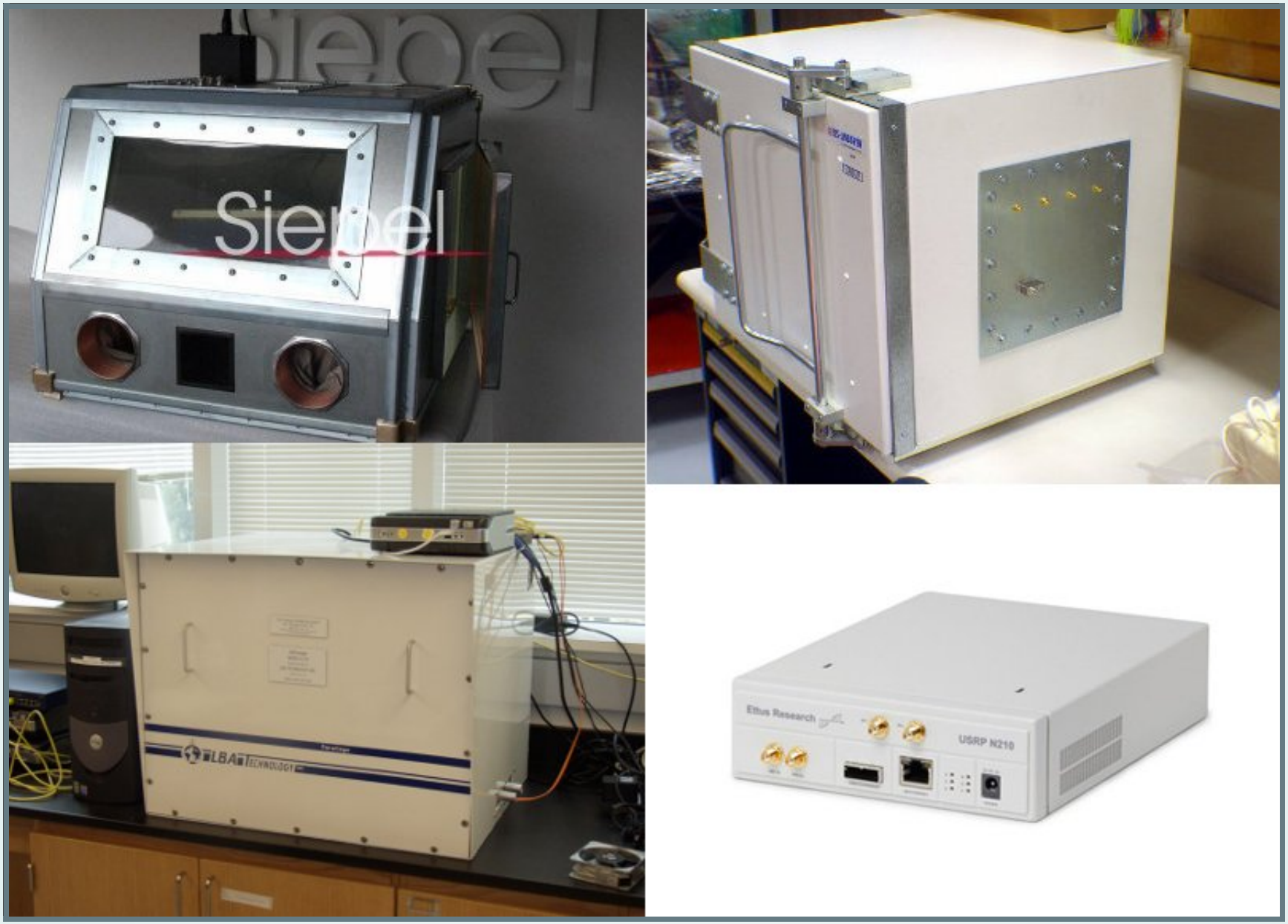
CHANGER LES COMPORTEMENTS

- Fabricants, éditeurs : analyser leurs systèmes, les corriger, pousser les mises à jour
- Opérateurs, distributeurs : analyser les terminaux, faciliter les mises à jour
- Utilisateurs : guetter les mises à jour, les installer

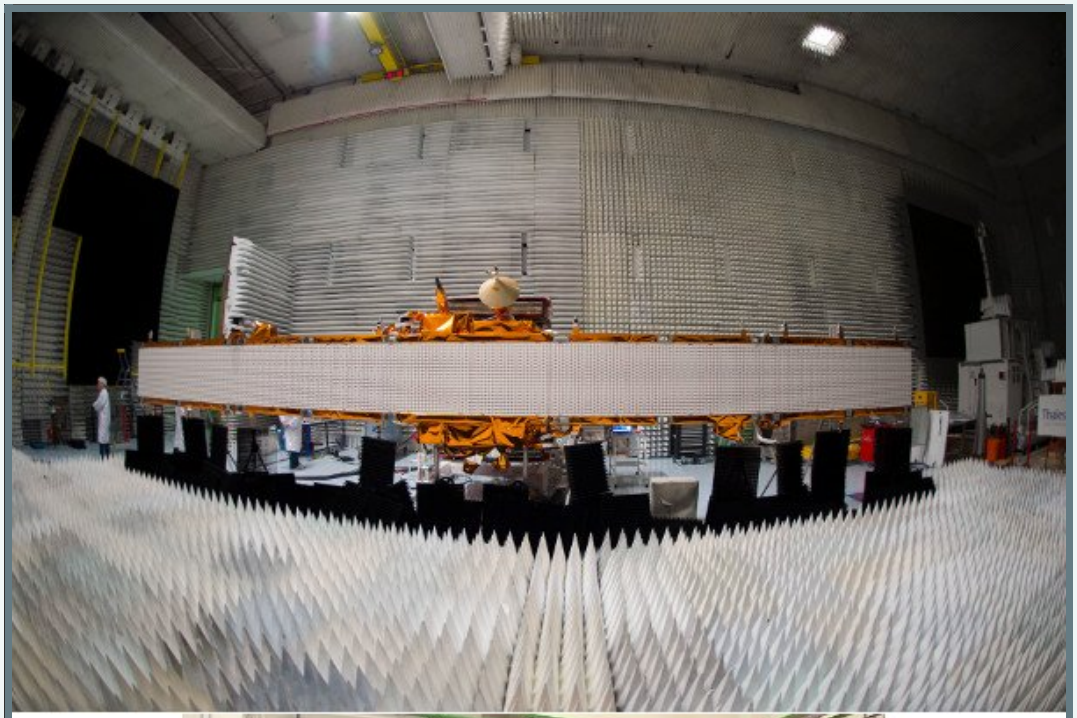
MERCI POUR VOTRE ATTENTION

Et à mes collègues (cde, en particulier)

ANNEXE 1 : EXPÉRIMENTATION RADIO 'DE BUREAU'



ANNEXE 2 : EXPÉRIMENTATION RADIO PROFESSIONELLE



ANNEXE 3 : BIBLIOTHÈQUES LOGICIELLES OPEN-SOURCE

- CryptoMobile : algorithmes cryptographiques 3G et LTE
- libmich : encodage / décodage des messages de signalisation 2G, 3G et LTE