

SSTIC 2014

ANALYSE DE LA SÉCURITÉ DES MODEMS DES TERMINAUX MOBILES

Benoit MICHAU (ANSSI)

benoit.michau [à] ssi.gouv.fr



Agence nationale de la sécurité
des systèmes d'information

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

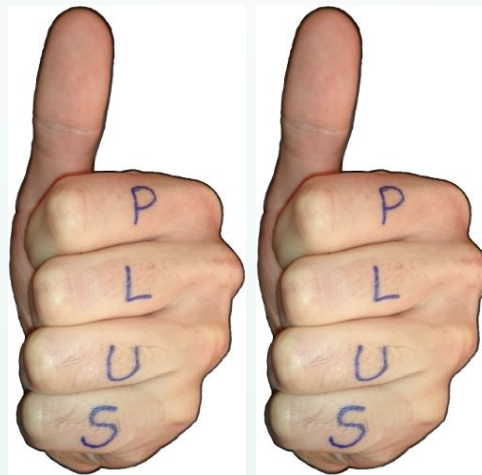
Sécurité:



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

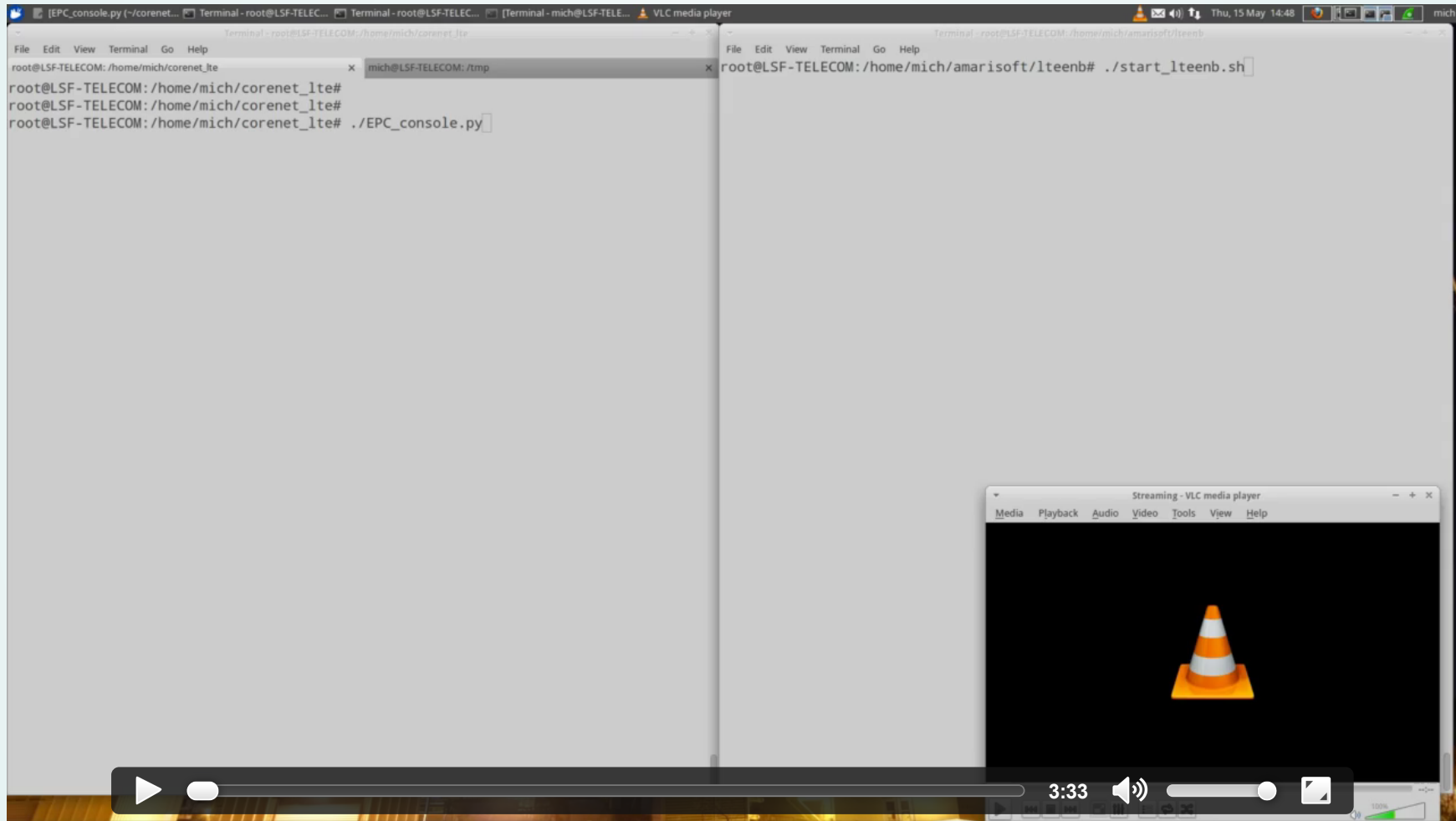
COMMENT ?

Mettre en place un banc de test.

PRÉREQUIS

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

VIDÉO 1 : CONNEXION AU BANC DE TEST LTE



VIDÉO 2 : SCAN DE MESSAGES LTE EMM

The screenshot displays a video player interface with a terminal window showing the output of an LTE EMM scan. The terminal output is divided into two main sections: a list of IP addresses and a detailed performance table.

IP Address List:

```
( '192.168.132.60', 46272 ),  
( '192.168.132.60', 37383 ),  
( '192.168.132.60', 50423 ),  
( '192.168.132.60', 44071 ),  
( '192.168.132.60', 49837 ),  
( '192.168.132.60', 56994 ),  
( '192.168.132.60', 59567 ),  
( '192.168.132.60', 33793 ),  
( '192.168.132.60', 48844 ),  
( '192.168.132.60', 36512 ),  
( '192.168.132.60', 36644 ),  
( '192.168.132.60', 54207 ),  
( '192.168.132.60', 50063 ),  
( '192.168.132.60', 59982 ),  
( '192.168.132.60', 35174 ),  
( '192.168.132.60', 32961 ),  
( '192.168.132.60', 56914 ),  
( '192.168.132.60', 56276 ),  
( '192.168.132.60', 44138 ),  
( '192.168.132.60', 54231 ),  
( '192.168.132.60', 47814 ),  
( '192.168.132.60', 52767 ),  
( '192.168.132.60', 48969 ),  
( '192.168.132.60', 54932 ),  
( '192.168.132.60', 60865 ),  
( '192.168.132.60', 47805 ),  
( '192.168.132.60', 36466 ),  
( '192.168.132.60', 39812 ),  
( '192.168.132.60', 40799 ),  
( '192.168.132.60', 39126 ),  
( '192.168.132.60', 56307 ),  
( '192.168.132.60', 57397 ),  
( '192.168.132.60', 45302 ),  
( '192.168.132.60', 53231 ),  
( '192.168.132.60', 48338 ),  
( '192.168.132.60', 60432 )
```

Performance Table:

```
3 01 003f 15 1 27.0 0 2 936 11.4 12.9 16.5 0 2 444 1/1.0/1 40  
3 01 003f 15 1 27.0 0 51 16.9k 5.6 10.8 13.2 0 15 8.32k 1/1.1/2 40  
3 01 003f 15 1 27.0 0 89 27.7k 6.6 11.7 11.9 0 34 10.8k 1/1.2/2 40  
3 01 003f 15 1 27.0 0 94 28.9k 8.4 12.2 11.6 0 31 9.96k 1/1.1/2 40  
3 01 003f 15 1 27.0 0 118 36.3k 15.8 12.5 12.2 0 34 11.3k 1/1.2/2 40  
3 01 003f 15 1 27.0 0 95 29.5k 17.3 11.3 12.5 0 31 10.3k 1/1.1/2 40  
3 01 003f 15 1 26.9 1 70 24.2k 7.0 12.6 13.1 0 23 8.14k 1/1.3/2 40  
3 01 003f 15 1 27.0 2 755 331k 16.9 11.3 14.4 23 108 222k 1/3.0/6 40  
3 01 003f 15 1 27.0 0 2 616 18.1 11.9 13.0 1 5 10.7k 1/3.7/6 40  
3 01 003f 15 1 - 0 0 0 16.6 - - 0 0 0 - 40
```

DL/UL Headers:

```
--DL-----  
UE_ID CL RNTI cqi ri mcs retx txok brate snr puc1 mcs retx rxok brate turbo phr  
3 01 003f 15 1 27.0 0 2 936 15.4 12.4 14.5 0 2 480 1/1.0/1 40  
3 01 003f 15 1 - 0 0 0 15.0 - - 0 0 0 - 40  
3 01 003f 15 1 27.0 0 2 936 15.6 12.2 13.5 0 2 420 1/1.0/1 40  
3 01 003f 15 1 - 0 0 0 15.2 - - 0 0 0 - 40  
3 01 003f 15 1 - 0 0 0 15.8 - - 0 0 0 - 40  
3 01 003f 15 1 27.0 0 2 936 15.6 12.2 11.0 0 2 428 1/1.5/2 40  
3 01 003f 15 1 - 0 0 0 14.6 - - 0 0 0 - 40  
3 01 003f 15 1 27.0 0 2 936 14.3 11.9 11.0 0 3 484 1/1.0/1 40  
3 01 003f 15 1 - 0 0 0 14.3 - - 0 0 0 - 40  
3 01 003f 15 1 - 0 0 0 11.5 - - 0 0 0 - 40
```

DL/UL Headers (repeated):

```
--DL-----  
UE_ID CL RNTI cqi ri mcs retx txok brate snr puc1 mcs retx rxok brate turbo phr  
3 01 003f 15 1 27.0 0 2 936 12.8 15.7 13.5 0 2 480 1/1.0/1 40  
3 01 003f 15 1 - 0 0 0 12.9 - - 0 0 0 - 40  
3 01 003f 15 1 27.0 0 2 936 11.6 16.3 12.5 0 2 468 1/1.0/1 40  
3 01 003f 15 1 - 0 0 0 10.4 - - 0 0 0 - 40  
3 01 003f 15 1 - 0 0 0 2.3 - - 0 0 0 - 40  
3 01 003f 15 1 27.0 0 2 936 6.7 11.1 5.5 0 2 412 1/1.0/1 40  
3 01 003f 15 1 - 0 0 0 8.6 - - 0 0 0 - 40  
3 01 003f 15 1 27.0 0 2 936 7.0 11.1 3.5 0 2 432 1/1.0/1 38  
3 01 003f 15 1 - 0 0 0 5.8 - - 0 0 0 - 38  
3 01 003f 15 1 - 0 0 0 7.3 - - 0 0 0 - 38
```

DL/UL Headers (repeated):

```
--DL-----  
UE_ID CL RNTI cqi ri mcs retx txok brate snr puc1 mcs retx rxok brate turbo phr  
3 01 003f 15 1 27.0 0 2 936 8.1 9.6 9.5 0 2 480 1/1.5/2 40  
3 01 003f 15 1 - 0 0 0 10.3 - - 0 0 0 - 40  
3 01 003f 15 1 27.0 0 2 936 6.7 12.5 10.0 0 2 412 1/1.5/2 40  
3 01 003f 15 1 - 0 0 0 6.1 - - 0 0 0 - 40  
3 01 003f 15 1 - 0 0 0 9.7 - - 0 0 0 - 40
```

Terminal Interaction:

```
In [18]: GSN.stats['resolved']  
Out[18]: []  
In [19]:
```

The video player interface includes a play button, a progress bar at 1:10, and a volume icon.

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

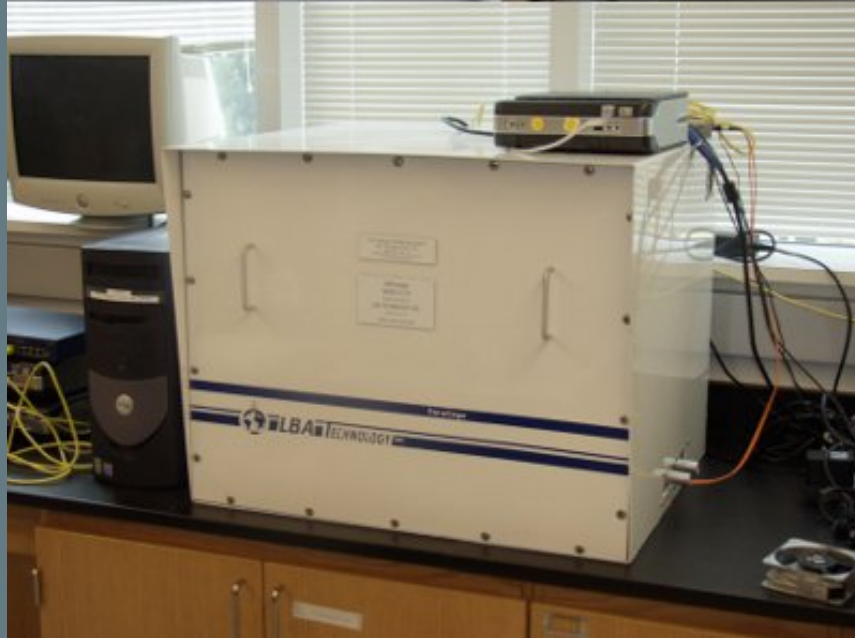
CHANGER LES COMPORTEMENTS

- 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

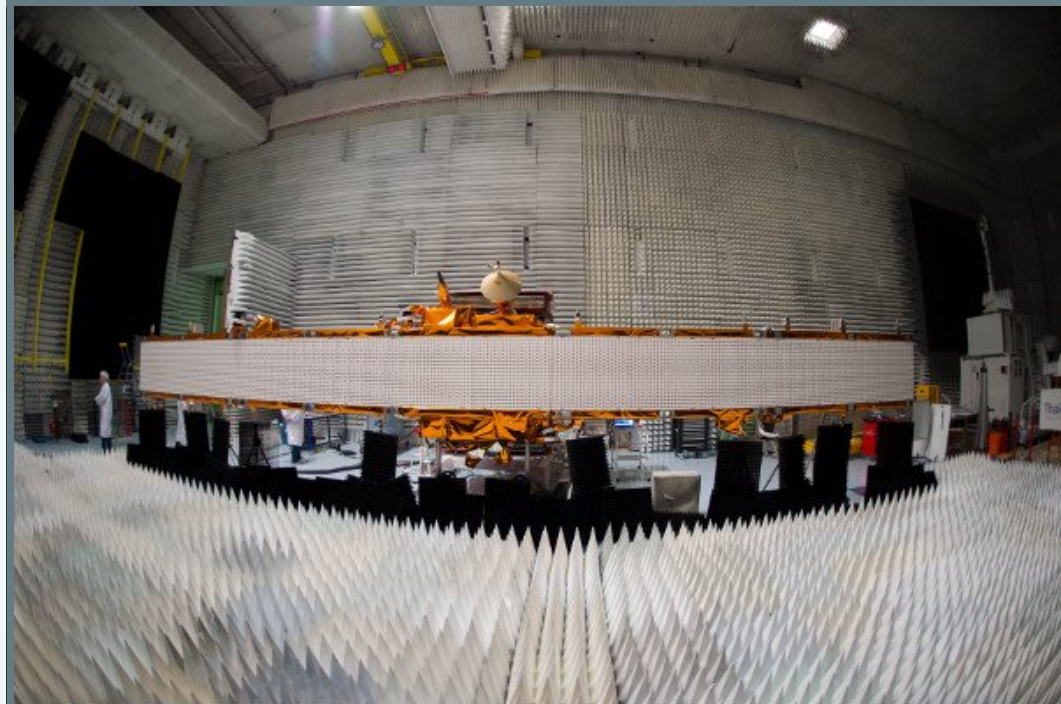
MERCI POUR VOTRE ATTENTION

Et à mes collègues (cde, en particulier)

ANNEXE 1 : EXPÉRIMENTATION RADIO 'DE BUREAU'



ANNEXE 2 : EXPÉRIMENTATION RADIO PROFESSIONNELLE



ANNEXE 3 : BIBLIOTHÈQUES LOGICIELLES OPEN-SOURCE

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