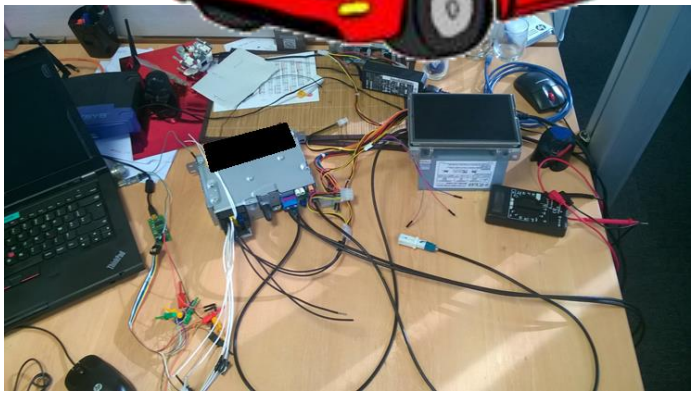
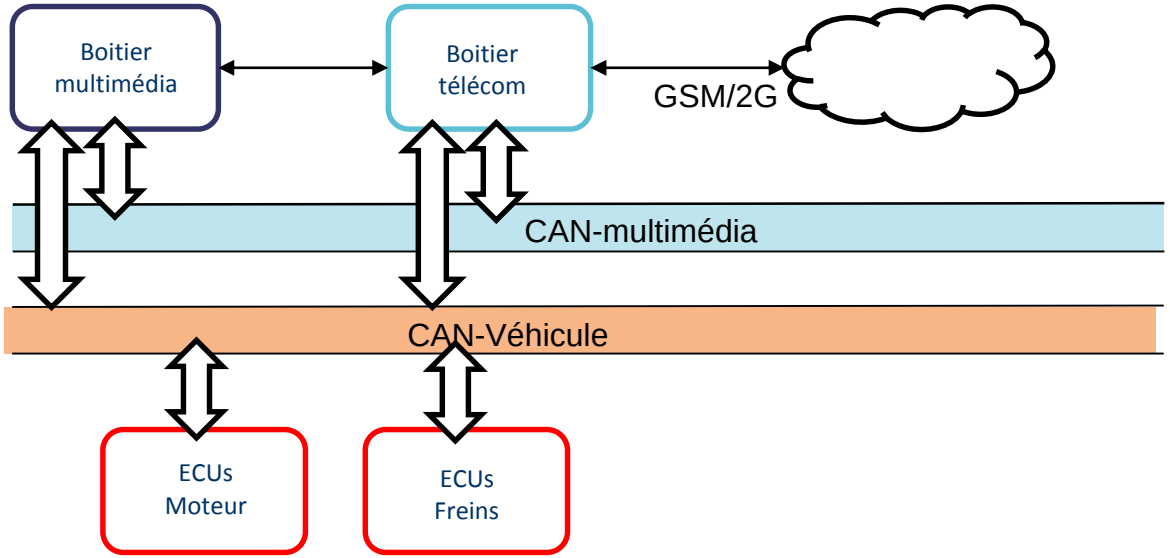
Évolutions et dé-évolutions de la sécurité des systèmes multimédia automobiles

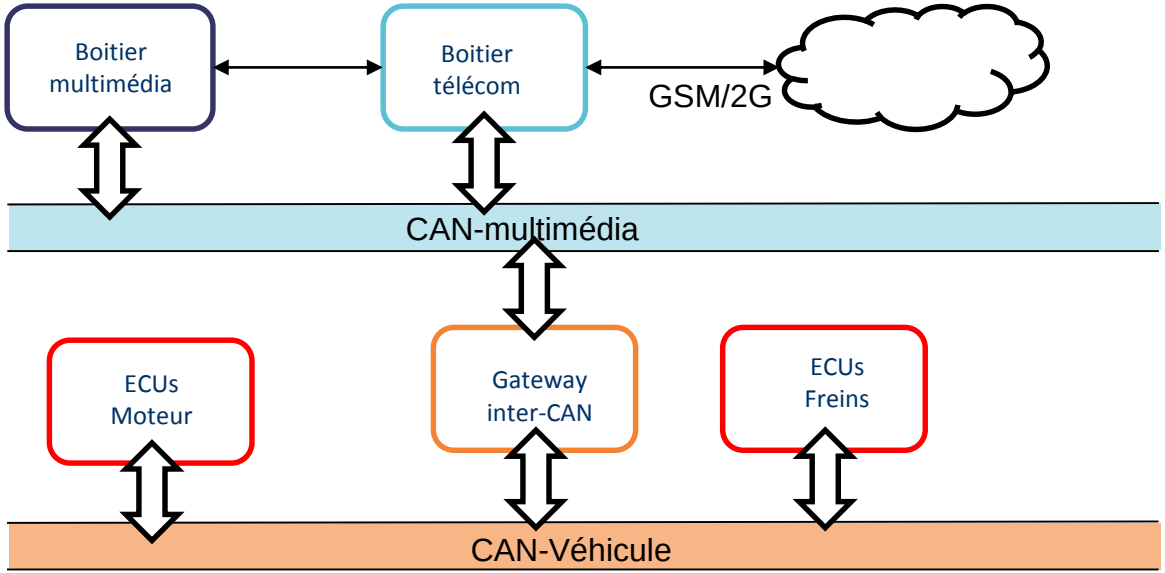
François POLLET, Nicolas MASSAVIOL

toucan system

THALES | FRP







Objectifs

- **Prise d'information**
  - Récupérer une image du système de fichiers
- **Code exec**
  - Interagir avec le système et ses périphériques
  - Détourner les fonctions légitimes
- **Emission sur le CAN**

Multimédia -Prise d’informations

Backdoors matérielles

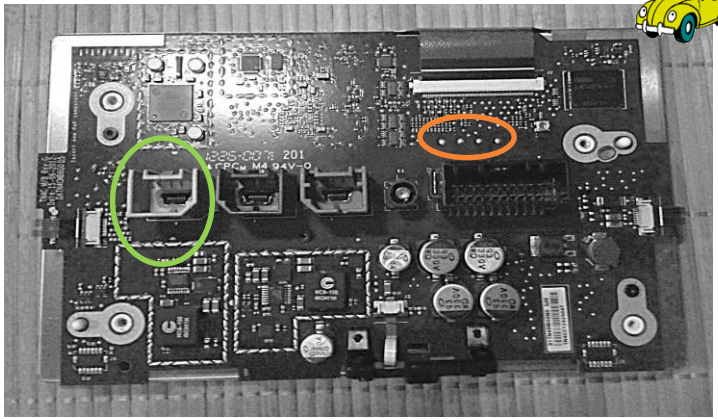
V1 :

- Port ADB, désactivé en prod
- Console non interactive

V2 :

- + JTAG désactivé en prod ou non

Console série + mire de login…



Fichier de mise à jour

V1 :

- Format propriétaire
- Fichier en clair

V2 :

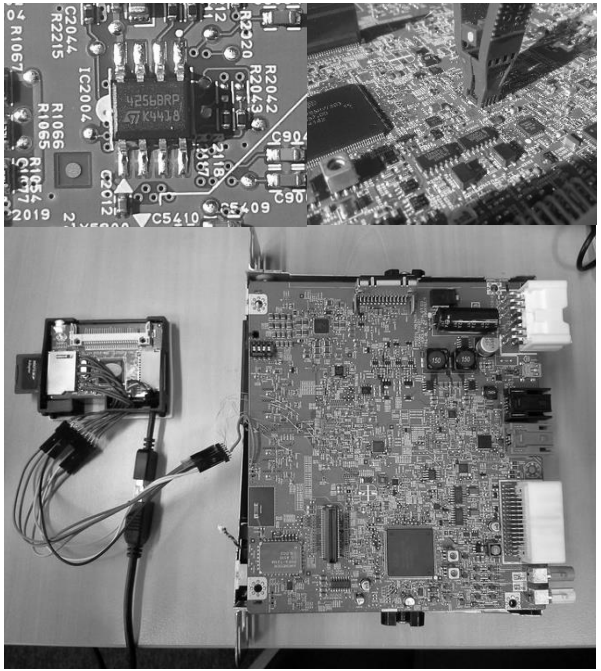
- Autre format propriétaire
- Toujours en clair

Fichiers chiffrés et signés

- En fait non…

Dump mémoire

- **EEPROM**
  - Plein d'info sympa
- **eMMC**
  - Lecteur de carte SD
  - Système de fichiers
- **NAND**
  - Corruptions
  - UBIFS…
  - /etc/passwd !



Exécution de code

Protéger son intégrité

Deux approches :

- 
  - Secure boot (ou tentatives pour V2)
  - Système de fichiers signé

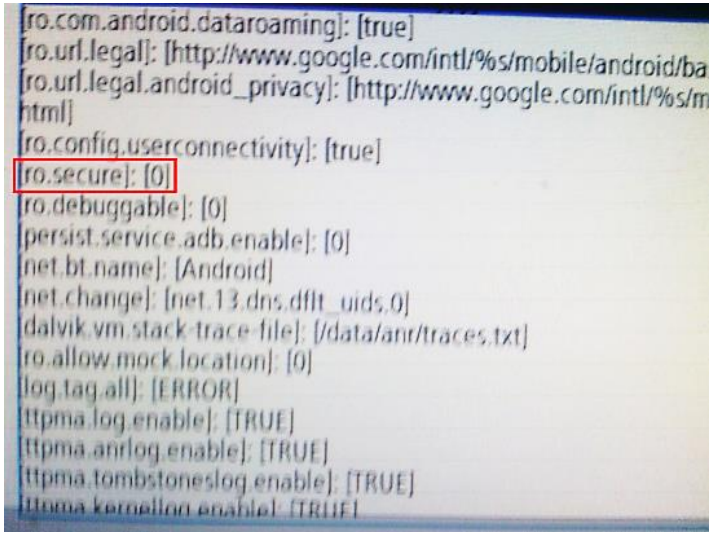
Blocs de données	Blocs de hash de niveau 0	Hashs de niveau 1	Signature

  - Mise à jour en clair, non signée
  - ➢ Une mise à jour corrompue brique la pièce
- 
  - Pas de secure boot
  - Mise à jour « chiffrée », « signée »
  - Pas de protection du système de fichiers
  - ➢ Personne n'irait modifier le contenu de la NAND …

Un système à jour et sécurisé

Systèmes Android:

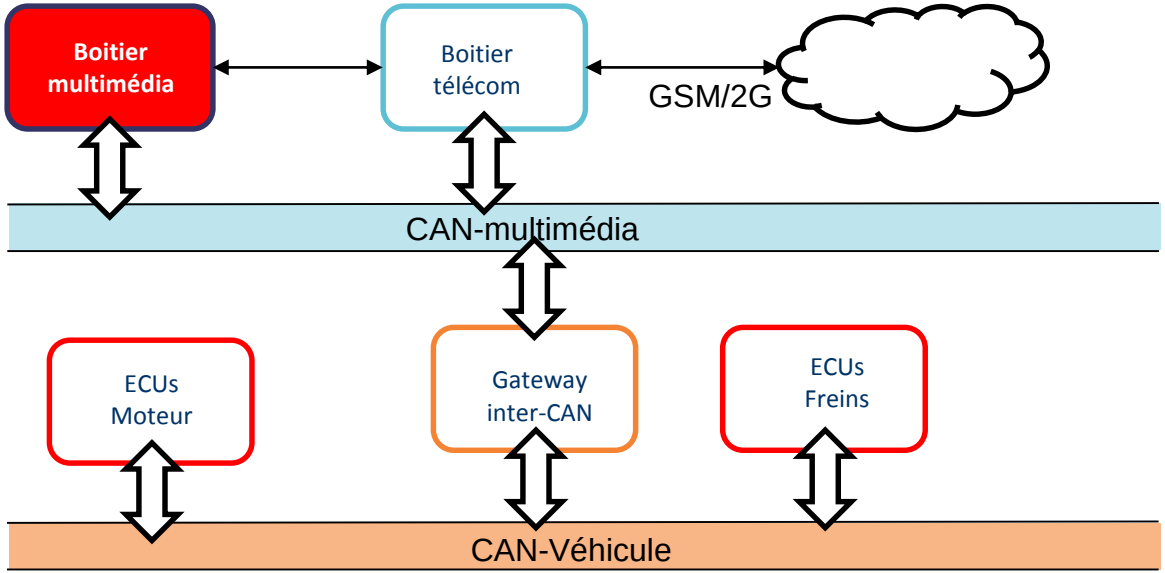
- V1 : Android 2.2
  - KillingInTheNameOf, GingerBreak, zergrush…
  - ADB tourne, de base, en root
- V2 : Android 4.0
  - Webview, MasterKeys, …
  - /data/local.prop



Linux

- Compte root sans mot de passe + console…
- Vulnérabilités du processus de mise à jour

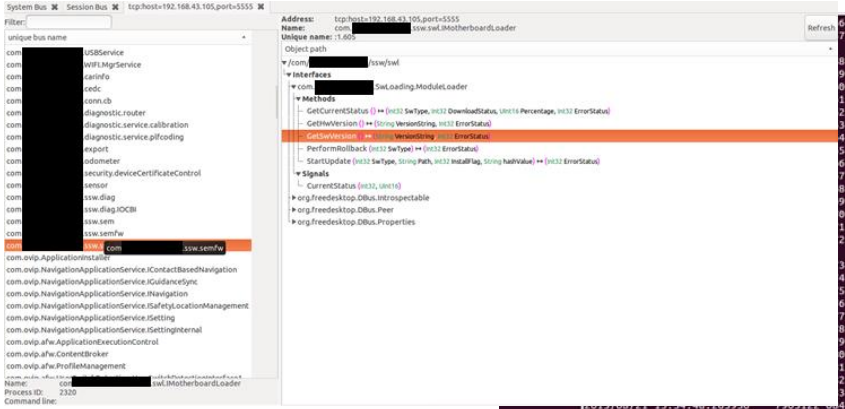
Et après ?

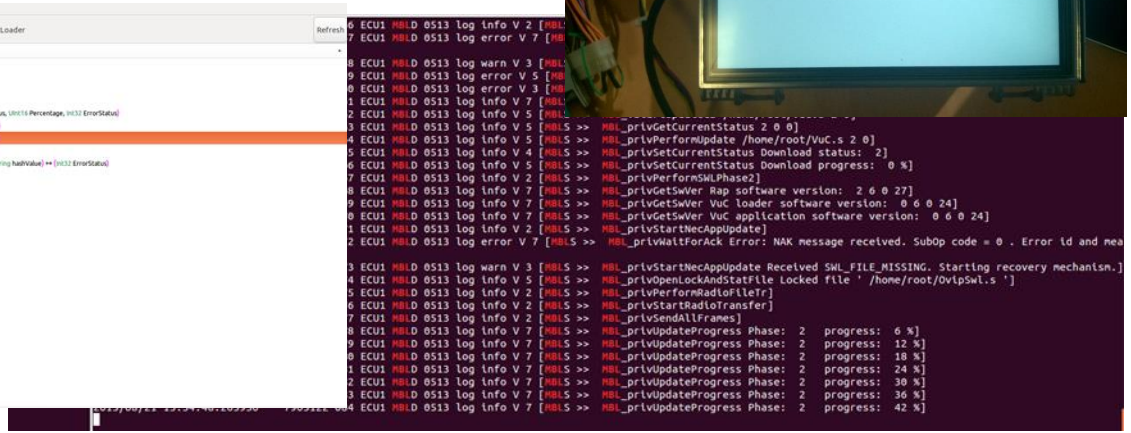


- Détourner les fonctionnalités légitimes

- Accès à internet

D-BUS est ton ami

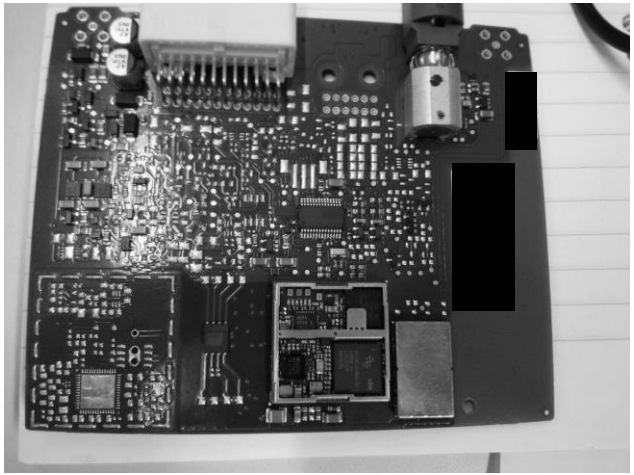




Boitier télécom

Surface d’exposition

- Couche matérielle (JTAG)
- Couche 2G/3G (data) + GSM
- Couche applicative (SSL)



OpenAT

```
Command WMP received: at+twmp=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa����
+CREG: 0

+CGREG: 0
����
OK

+CREG: 0

+CGREG: 0
[23:28:39][32]JAMMING DETECTION: FINAL STATUS
[23:28:39][32] UNKOWN
[23:28:39][32]JAMMING started
[23:28:39][32]SIM present

ERROR

+CREG: 2
[23:28:39][32]Registration status: Registered, home network
```

Gateway CAN

désolé

Bientôt dans vos voitures

toucan system

THALES | FRP

- Auto-partage dans le nuage
- Démarrage à distance
- Délégation de conduite en convois
- Véhicule autonome
- PYOD
- …

PYOD

- Intégration ordiphone <-> véhicule
- Tableaux de bord et de commandes déportés
- Dé-périmétrisation à travers le nuage