

# Libérer son mobile avec Replicant : politique, technique

Paul Kocialkowski   Benjamin Bayart

Samedi 21 novembre 2015

Bazar  Libre

Composants, problématiques et liberté

# Composants, implémentations

Composants (numériques) d'un appareil mobile :

- Processeurs
  - Processeur principal
  - Processeurs auxiliaires de calcul
  - Processeur de communication
- Contrôleurs
- Périphériques

# Composants, implémentations

Composants (numériques) d'un appareil mobile :

- Processeurs
  - Processeur principal
  - Processeurs auxiliaires de calcul
  - Processeur de communication
- Contrôleurs
- Périphériques

Implémentations :

- Matérielles
- Logicielles

# Constats, problématiques

Constats, évolutions :

- Nombre de composants **programmés**
- Délocalisation du traitement
- Accès aux **communications** et aux **données**

# Constats, problématiques

Constats, évolutions :

- Nombre de composants **programmés**
- Délocalisation du traitement
- Accès aux **communications** et aux **données**

Problématiques :

- **Confiance** en la technologie
- **Contrôle** des appareils
- **Connaissance** du fonctionnement, préservation

Pondérées par le degré de complexité (logiciel/matériel)

# Libertés fondamentales et implémentations

Garanties : libertés fondamentales

1. Utilisation pour tous les usages
2. Étude et modification
3. Redistribution
4. Redistribution des modifications

# Libertés fondamentales et implémentations

Garanties : libertés fondamentales

1. Utilisation pour tous les usages
2. Étude et modification
3. Redistribution
4. Redistribution des modifications

Pour les appareils mobiles :

- Matériel libre
- Logiciel libre



## Liberté et appareils mobiles

# Liberté et appareils mobiles

Matériel libre

# Matériel libre

Technologies :

- Circuits imprimés
- Circuits intégrés

Libérer le matériel :

- Modifications ?
- Notion de code source :
  - Circuits intégrés
  - Circuits imprimés
- Formats de description
- Coûts, dimensions
- Réalisation des circuits, confiance

# Matériel libre

Situation actuelle :

- Possible à certains niveaux
- Initiatives de circuits intégrés libres :  
OpenRISC, OpenSPARC, LEON, LM32, lowRISC, etc
- Initiatives de circuits imprimés libres :  
Arduino, Freeduino, USB armory, Novena, etc
- Documentation matérielle et "OpenHardware"
- Rapport aux appareils mobiles

# Matériel libre

Situation actuelle :

- Possible à certains niveaux
- Initiatives de circuits intégrés libres :  
OpenRISC, OpenSPARC, LEON, LM32, lowRISC, etc
- Initiatives de circuits imprimés libres :  
Arduino, Freeduino, USB armory, Novena, etc
- Documentation matérielle et "OpenHardware"
- Rapport aux appareils mobiles

Toujours loin d'être aussi simple que :

```
$ ./configure
```

```
$ make
```

```
# make install
```

# Liberté et appareils mobiles

Logiciel libre, contraintes et limitations

# Libération du logiciel

Libération du logiciel :

- Positions des fabricants
  - Intérêt économique
  - Droits d'auteur (blocs), brevets
  - Gauche d'auteur (*Copyleft*)
  - Qualité, maintenabilité (référence)
- Travail d'ingénierie inverse
- Temps et ressources nécessaires
- Intérêt à long terme et obsolescence
- Possibilité technique, limitations récurrentes

# Limitations techniques à la libération du logiciel

Limitations récurrentes :

- Connaissances techniques et outils adaptés
- Contraintes légales (ingénierie inverse)
- Documentation du matériel, schémas, etc
- Possibilité de remplacer le logiciel :  
Mémoires en lecture seule, interfaces secrètes, accès "externe"
- Possibilité d'exécuter son propre code : signatures
- Possibilité de déboguer le code



# Limitations techniques à la libération du logiciel

Limitations récurrentes :

- Connaissances techniques et outils adaptés
- Contraintes légales (ingénierie inverse)
- Documentation du matériel, schémas, etc
- Possibilité de remplacer le logiciel :  
Mémoires en lecture seule, interfaces secrètes, accès "externe"
- Possibilité d'exécuter son propre code : signatures
- Possibilité de déboguer le code

Une fois le logiciel libéré fonctionnel :

- Facilité d'installation pour l'utilisateur
- Risque de rendre le tout inopérant

# Liberté et appareils mobiles

Micrologiciels

# Logiciel libre et micrologiciels

Micrologiciels :

- Indépendants, tâches spécifiques
- Contrôleurs, périphériques, processeurs auxiliaires

# Logiciel libre et micrologiciels

Micrologiciels :

- Indépendants, tâches spécifiques
- Contrôleurs, périphériques, processeurs auxiliaires

Appareils mobiles :

- Micrologiciels **privateurs**, rarement signés
- Souvent chargés au démarrage, distribués avec le système
- Wi-Fi, bluetooth, GPS, traitement multimédia, caméras, . . .

# Logiciel libre et micrologiciels

Micrologiciels :

- Indépendants, tâches spécifiques
- Contrôleurs, périphériques, processeurs auxiliaires

Appareils mobiles :

- Micrologiciels **privateurs**, rarement signés
- Souvent chargés au démarrage, distribués avec le système
- Wi-Fi, bluetooth, GPS, traitement multimédia, caméras, . . .

Prise en charge du logiciel libre :

- Matériel spécifique (Arduino, BusPirate, FX2LA)
- Périphériques Wi-Fi (ath9k\_htc, AR9170, OpenFWWF)

**Pas de micrologiciels libres pour les appareils mobiles**

## Liberté et appareils mobiles

Processeur de communication (modem)

# Logiciel libre et processeur de communication (modem)

Processeur de communication (modem) :

- Processeur puissant
- Système d'exploitation complet
- Parfois en charge du processeur principal

# Logiciel libre et processeur de communication (modem)

Processeur de communication (modem) :

- Processeur puissant
- Système d'exploitation complet
- Parfois en charge du processeur principal
- Systèmes **privateurs** (appareils mobiles récents)
- Remplacement du système, signatures



# Logiciel libre et processeur de communication (modem)

Processeur de communication (modem) :

- Processeur puissant
- Système d'exploitation complet
- Parfois en charge du processeur principal
- Systèmes **privateurs** (appareils mobiles récents)
- Remplacement du système, signatures

Prise en charge du logiciel libre :

- Pile GSM libre : **OsmocomBB**
- Limites : utilisation, prise en charge, certification

**Système privateur en pratique, gros problème pour la vie privée/sécurité**

# Isolation du processeur de communication (modem)

Enjeux de vie privée/sécurité :

- Accès au matériel
- Capacité d'espionner l'utilisateur
- Capacité de compromettre le processeur principal

# Isolation du processeur de communication (modem)

Enjeux de vie privée/sécurité :

- Accès au matériel
- Capacité d'espionner l'utilisateur
- Capacité de compromettre le processeur principal

Isolation du modem :

- Problèmes de liberté
- Autres moyens d'espionner (opérateurs de téléphone mobile)
- Vérification pratique et confiance :  
preuve de mauvaise situation, modem intégré, schémas,  
matériel libre

**Solution pragmatique et jamais entièrement fiable**

# Liberté et appareils mobiles

Processeur principal

# Logiciel libre et processeur principal

Logiciels sur le processeur principal:

- Microcodes
- Bootrom
- Chargeur de démarrage
- Système d'exploitation :
  - Noyau (Linux)
  - Couches d'abstraction matérielle
  - *Frameworks*
  - Applications

# Logiciel libre et microcodes

Microcodes :

- Traitement des instructions, techniques avancées
- Complexité, séquenceurs

# Logiciel libre et microcodes

Microcodes :

- Traitement des instructions, techniques avancées
- Complexité, séquenceurs

Appareils mobiles (ARMv7, MIPS) :

- Implémentations **matérielles**, pas de microcodes

# Logiciel libre et microcodes

Microcodes :

- Traitement des instructions, techniques avancées
- Complexité, séquenceurs

Appareils mobiles (ARMv7, MIPS) :

- Implémentations **matérielles**, pas de microcodes

Appareils mobiles (ARMv8, x86) :

- Microcodes **privateurs**
- Pré-installés, mises à jour chargées au démarrage
- Vérification de **signatures** (x86, ARMv8 ?)

**Microcodes pas utilisés ou privateurs sur les appareils mobiles**



# Logiciel libre et bootrom/chargeur de démarrage

Logiciels de démarrage :

- Bootrom : propriétaire, mémoire non-réinscriptible
- Vérifications de **signatures**, chargement en chaîne spécifique à la plateforme, variante
- Chargeurs de démarrage libres : **U-Boot, Coreboot**
- Bonnes plateformes :  
i.MX, Allwinner, OMAP (GP), Tegra (non-ODM), Rockchip
- Quelques appareils avec ces plateformes

**Logiciels de démarrage libres pour quelques appareils mobiles**

# Logiciel libre et système d'exploitation

Crucial pour la vie privée/sécurité :

- Accès aux contrôleurs et périphériques
- Accès aux données de l'utilisateur
- Accès aux communications de l'utilisateur
- *Samsung Galaxy Back-door*

# Logiciel libre et système d'exploitation

Crucial pour la vie privée/sécurité :

- Accès aux contrôleurs et périphériques
- Accès aux données de l'utilisateur
- Accès aux communications de l'utilisation
- *Samsung Galaxy Back-door*

Au premier plan du logiciel libre :

- Interaction directe
- Compréhension, modifications
- Nouvelles versions, mises à jour

# Logiciel libre et système d'exploitation

Couches des systèmes d'exploitation :

- Noyau : Linux, **libre**, versions modifiées, passoires
- Couches d'abstraction matérielle : **privateur** en majorité
- *Frameworks* : systèmes plutôt **libres**  
Android, FirefoxOS, Ubuntu Touch, OpenWebOS, etc
- Applications : diverses **libres**  
Dépôts d'applications (F-Droid)

# Couches d'abstraction matérielles

Aspects généralement problématiques :

- Accélération graphique, GPU
- GPS

Selon les plateformes :

- Caméras (dépendance au GPU)
- Audio

# Couches d'abstraction matérielles

Aspects généralement problématiques :

- Accélération graphique, GPU
- GPS

Selon les plateformes :

- Caméras (dépendance au GPU)
- Audio

Projets dédiés libération de certains aspects :

- Freedreno (GPUs Adreno)
- Lima (GPUs Mali)
- Nouveau (GPUs nVidia)

**Couches privatives : nécessité, privilèges, accès, savoir**

Bilan et remédiations possibles

# Bilan, approches pragmatiques

Après une vue d'ensemble des appareils mobiles :

- Situation imparfaite
- Appareils peuvent être compromis (données, communications)
- Évaluation des enjeux, niveaux de confiance
- Limites du possible à court terme
- Besoin fort de développeurs



# Bilan, approches pragmatiques

Après une vue d'ensemble des appareils mobiles :

- Situation imparfaite
- Appareils peuvent être compromis (données, communications)
- Évaluation des enjeux, niveaux de confiance
- Limites du possible à court terme
- Besoin fort de développeurs

Approches à court et moyen terme :

- Libérer le système du processeur principal
- Préférer de bonnes plateformes
- Intérêt pour l'isolation du modem
- Production d'appareils mobiles

## Bilan et remédiations possibles

Systeme libre : Replicant



# Replicant

Projet basé sur des idées et valeurs :

- Système mobile entièrement libre, basé sur Android
- Distribution et recommandation de logiciel libre exclusivement
- Accent sur la vie privée/sécurité
- Fonctionnel et utilisable

# État du projet Replicant

État actuel du projet :

- **Un seul** développeur, temps libre
- Peu de contributions externes (sécurité)
- 12 appareils pris en charge :  
Samsung Galaxy, Nexus
- Fonctionnalités manquantes
- Base CyanogenMod 10.1, Android 4.2
- Soutien financier : **dons**

Dernières images : **Replicant 4.2 0004**

# Appareils pris en charge par Replicant



## Pris en charge

- Nexus S (I902x) : 2011
- Galaxy S (I9000) : 2012
- Galaxy S 2 (I9100) : 2012
- Galaxy Note (N7000) : 2013
- Galaxy Nexus (I9250) : 2012
- Galaxy Tab 2 7.0 (P31xx) : 2013
- Galaxy Tab 2 10.1 (P51xx) : 2013
- Galaxy S 3 (I9300) : 2013
- Galaxy Note 2 (N7100) : 2014

## Pas complété

- GTA04 : 2012

## Plus maintenus

- HTC Dream/Magic : 2010
- Nexus One : 2011

# Challenges et objectifs futurs

Challenges futurs :

- Confiance en CyanogenMod, OmniROM
- Nouvelles versions, prise en charge des appareils
- Applications Google et AOSP

# Challenges et objectifs futurs

## Challenges futurs :

- Confiance en CyanogenMod, OmniROM
- Nouvelles versions, prise en charge des appareils
- Applications Google et AOSP

## Objectifs futurs :

- Hébergement du code source
- Nouvelle version
- Meilleure documentation
- Améliorations pour la vie privée et la sécurité
- Meilleurs appareils pris en charge

# Meilleure documentation, vie privée/sécurité

Mise à jour du wiki :

- Évaluation des appareils et informations : chargeurs de démarrage, vie privée/sécurité, isolation du modem
- Recherche à propos d'autres appareils
- Documentation des projets inachevés (GPS, etc)

Vie privée/sécurité :

- Version de Replicant orientée sécurité ?  
au détriment de certaines fonctionnalités
- Prise en charge de meilleurs appareils



# Bilan et remédiation possibles

Meilleurs appareils

# Appareils pris en charge, liberté, vie privée/sécurité



Mauvaise isolation du modem

# Appareils pris en charge, liberté, vie privée/sécurité



Chargeurs de démarrage  
privateurs et signés



# Choix des appareils pour Replicant

Pris en charge de meilleurs appareils :

- Designs matériels libres
- Documentation du matériel
- Appareils sans modem
- Isolation du modem
- Chargeurs de démarrage libres
- Puces, protocoles et pilotes

# Choix des appareils pour Replicant

Pris en charge de meilleurs appareils :

- Designs matériels libres
- Documentation du matériel
- Appareils sans modem
- Isolation du modem
- Chargeurs de démarrage libres
- Puces, protocoles et pilotes

Communauté **OpenPhoenix** :

- **GTA04**, appareils **Letux**
- **Neo900**

Appareils chinois peu coûteux :

- Tablettes **Allwinner**
- Tablettes **Rockchip**

Appareils produits en masse :

- **Optimus Black (P970)**
- **Kindle Fire**  
première génération

Autres **formats** d'appareils !

# Replicant

En apprendre plus à propos de Replicant :

- Site web : <http://www.replicant.us/>
- Blog : <http://blog.replicant.us/>
- Wiki/tracker : <http://redmine.replicant.us/>

Rejoignez la communauté :

- Forums
- Liste de diffusion
- Canal IRC : **#replicant** chez **freenode**

Le projet a besoin de vous !

- Replicant mérite **plus qu'un seul développeur**
- Les **dons** sont bienvenus (les appareils coûtent cher)



*That's all Folks!*