Replicant, système d'exploitation libre pour smartphones

Paul Kocialkowski Benjamin Bayart

Samedi 17 octobre 2015

Appareils mobiles, logiciel libre et vie privée/sécurité

Anatomie d'un appareil mobile :

- Nombre croissant de composants programmés
- Traitements implémentés sur ces composants
- Rôle central du processeur principal ?
- Accès aux communications et aux données

Appareils mobiles, logiciel libre et vie privée/sécurité

Anatomie d'un appareil mobile :

- Nombre croissant de composants programmés
- Traitements implémentés sur ces composants
- Rôle central du processeur principal ?
- Accès aux communications et aux données

Logiciel libre :

- Contrôle (individuel et collectif), 4 libertés fondamentales
- Confiance en l'appareil
- Accès au savoir et sa préservation (biens communs)

Appareils mobiles, logiciel libre et vie privée/sécurité

Anatomie d'un appareil mobile :

- Nombre croissant de composants programmés
- Traitements implémentés sur ces composants
- Rôle central du processeur principal ?
- Accès aux communications et aux données

Logiciel libre :

- Contrôle (individuel et collectif), 4 libertés fondamentales
- Confiance en l'appareil
- Accès au savoir et sa préservation (biens communs)

Matériel libre ?

Composants, implémentations et liberté

Composants d'un appareil mobile :

- Processeurs
  - Processeur principal (CPU)
  - Processeurs auxiliaires de calcul (GPU, VPU, DSP, etc)
  - Processeur de communciation (modem/baseband/radio)
- Contrôleurs (E/S, protocoles, etc)
- Périphériques (stockage, communications, etc)

Composants, implémentations et liberté

Composants d'un appareil mobile :

- Processeurs
  - Processeur principal (CPU)
  - Processeurs auxiliaires de calcul (GPU, VPU, DSP, etc)
  - Processeur de communciation (modem/baseband/radio)
- Contrôleurs (E/S, protocoles, etc)
- Périphériques (stockage, communications, etc)

Situation actuelle :

- Implémentations matérielles (circuits intégrés : ASIC)
- Implémentations logicielles (microcodage des processeurs, microcontrôleurs)
- Matériel libre, logiciel libre ?

Matériel libre

Libérer le matériel ?

- 4 libertés fondamentales du logiciel libre
- Enjeux de vie privée et sécurité
- Modifier le matériel ?
- Notion de code source :
  - Circuits intégrés : langage de description matérielle (HDL)
  - Circuits imprimés : description CAO (schémas, couches, etc)
- Formats de description du matériel ? (Gerber, Eagle, etc)
- Coût pour un individu (circuits imprimés, circuits intégrés)
- 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"

Toujours loin d'être aussi simple que :

```
$ ./configure
$ make
# make install
```

Libérer le logiciel, à tous les niveaux

Composants programmés, logiciels de plus en plus répandus :

- Processeurs :
  - Microcodage des séquenceurs
  - Logiciels exécutés (micrologiciels aux systèmes d'exploitation)
- Microcontrôleurs : micrologiciels, tâches spécifiques
- État du logiciel libre variable

Libérer le logiciel, à tous les niveaux

Composants programmés, logiciels de plus en plus répandus :

- Processeurs :
  - Microcodage des séquenceurs
  - Logiciels exécutés (micrologiciels aux systèmes d'exploitation)
- Microcontrôleurs : micrologiciels, tâches spécifiques
- État du logiciel libre variable

Travail de libération du logiciel :

- 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 :

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

Logiciel libre et microcontrôleurs

Microcontrôleurs dans différents contrôleurs et périphériques :

- Wi-Fi, bluetooth
- GPS
- Contrôleurs USB 3
- Plus (dépend de la plateforme)

Logiciel libre et microcontrôleurs

Microcontrôleurs dans différents contrôleurs et périphériques :

- Wi-Fi, bluetooth
- GPS
- Contrôleurs USB 3
- Plus (dépend de la plateforme)

Prise en charge du logiciel libre :

- Matériel spécifique (Arduino, BusPirate, FX2LA)
- Périphériques Wi-Fi (ath9k_htc, AR9170, OpenFWWF)
- Micrologiciels privateurs en grande majorité,
  souvent chargés au démarrage et rarement signés

Pas de micrologiciels libres pour les appareils mobiles

Logiciel libre et processeurs auxiliaires de traitement

Processeurs auxiliaires de traitement :

- Tâches spécifiques : micrologiciels
- GPUs : programmés à la volée (shaders)
- Généralement pas de microcodes
- Micrologiciels chargés au démarrage, rarement signés

Logiciel libre et processeurs auxiliaires de traitement

Processeurs auxiliaires de traitement :

- Tâches spécifiques : micrologiciels
- GPUs : programmés à la volée (shaders)
- Généralement pas de microcodes
- Micrologiciels chargés au démarrage, rarement signés

Prise en charge du logiciel libre :

- GPUs : Freedreno, Lima, Nouveau, Radeon
  parfois des micrologiciels (privateurs)
- VPUs/DPSs : Compilateurs, micrologiciels privateurs
  généralement

Émergence de logiciels libres pour quelques modèles

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

Prise en charge du logiciel libre :

- Systèmes privateurs (appareils mobiles récents)
- Replacement du système, signatures
- 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

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

Situation spécifique pour chaque appareil et plateforme

Logiciel libre et bootrom/chargeur de démarrage

Logiciels de démarrage :

- Bootrom : privateur, 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

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'utilisation
- *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, versions modifiées, passoires
- Couches d'abstraction matérielle : privateur en majorité
- *Frameworks* : systèmes plutôt libres
  Android, FirefoxOS, Ubuntu Touch, OpenWebOS, etc
- Applications : diverses libres

Reste des composants privateurs : privilèges, accès, savoir

Bilan et remédiations possibles

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

Bilan et remédiations possibles

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

Approches pragmatiques :

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

Système d'exploitation libre

Vers un système d'exploitation mobile libre :

- Situation en 2008 : GNU/Linux et Android
  Openmoko Neo FreeRunner et HTC Dream
- Libération (partielle) d'Android par Google : AOSP
- Courant 2010 : Initiatives de libération d'Android
  LibrePlanet Italia, SFLC
- Version entièrement libre d'Android : Replicant

Différentes versions d'Android

Android comme famille de systèmes d'exploitation :

- Version interne de Google
- Versions des fabricants (OEMs)
- Android Open Source Project (AOSP)
- Versions communautaires

Différentes versions d'Android

Android comme famille de systèmes d'exploitation :

- Version interne de Google
- Versions des fabricants (OEMs)
- Android Open Source Project (AOSP)
- Versions communautaires

Versions communautaires :

- Rapport au logiciel libre
- Composants privateurs
- Fonctionnalités malveillantes
- Recommandation, installation de logiciels privateurs

Idées et valeurs fondatrices de Replicant

Projet basé sur des idées et valeurs :

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

Système mobile **éthique**, qui **respecte** ses utilisateurs

- Projet soutenu par RMS et la FSF
- Système approuvé par la FSF

Bases techniques de Replicant

- Version dérivée de CyanogenMod
- Composants privateurs replacés ou supprimés
- Suppression des fonctionnalités malveillantes
- Dépôt d'applications libres : **F-Droid**
- Adaptation du système
- Aspect, identité
- Maintenance, mises à jour de sécurité

Travail technique, libération du système

Remplacer les composants privateurs :

- Ingénierie inverse :
  - Compréhension du fonctionnement
  - Remplacements libres
- Conditions en partie favorables
- Absence de documentation
- Différents aspects liés au matériel : audio, caméra, modem, capteurs
- Coopération inter-projets

Travail technique, libération du système

Remplacer les composants privateurs :

- Ingénierie inverse :
  - Compréhension du fonctionnement
  - Remplacements libres
- Conditions en partie favorables
- Absence de documentation
- Différents aspects liés au matériel :
  audio, caméra, modem, capteurs
- Coopération inter-projets

Aspects non pris en charge:

- Au-delà du processeur principal :
  micrologiciels, systèmes des processeurs auxiliaires et modem
- Accélération graphique (GPU)

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 dans la prise en charge des appareils

Appareils Samsung :

- RIL : Samsung-RIL, libsamsung-ipc, transport spécifique
  Réécriture à l'été 2014

Nexus S (I902x) , Galaxy S (I9000) :

- Caméra : aperçu, EGL
- Capteurs : accéléromètres, champ magnétique

Galaxy S 2 (I9100), Galaxy Note (N7000) :

- Audio : Yamahell, Yamaha-MC1N2-Audio, TinyALSA-Audio
- Caméra : Exynos Camera

Galaxy S 3 (I9300), Galaxy Note 2 (N7100):

- Camera : Exynos Camera (réécriture), format S5C73M3
- Capteurs

Limitations récurrentes

Fonctionnalités généralement manquantes :

- Accélération graphique, 3D
- Micrologiciels Wi-Fi et bluetooth
- Encodage et décodage accéléré des vidéos
- Caméra

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**

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 d'autres appareils sans modem :
  tablettes Wi-Fi

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 **OpenPhoenux** :

- **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!