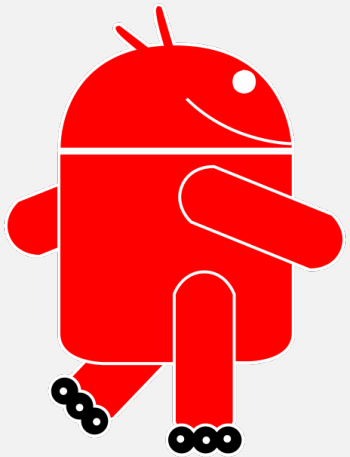
Replicant : appareils mobiles, logiciels libres et vie privée



Paul Kocialkowski
paulk@replicant.us

Samedi 2 Juin 2016

PAS SAGE EN SEINE

HACKER SPACE FESTIVAL

Composants, problématiques et libertés

Composants et implémentations

Composants (numériques) d'un appareil mobile :

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

Implémentations :

- Design matériel
- Logiciels

Situation actuelle, problématiques

Situation et 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

Degré de complexité

Libertés fondamentales et implémentations

Garanties : libertés fondamentales

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

Implémentations pour les appareils mobiles :

- Design matériel libre
- Logiciel libre

Appareils mobiles et liberté

Appareils mobiles et liberté

Design matériel libre

Design matériel libre

Technologies :

- Circuits imprimés
- Circuits intégrés

Libérer le matériel :

- Modifications, *code source* et design
- Formats et chaînes d'outils
- Coûts et dimensions
- Infrastructure et confiance

Design matériel libre

Situation actuelle:

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

Jamais aussi simple que:

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

Appareils mobiles et liberté

Libération du logiciel 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
- Possibilité technique, limitations récurrentes
- Intérêt à long terme et obsolescence

Limitations techniques à la libération du logiciel

Limitations récurrentes :

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

Une fois le logiciel libéré fonctionnel :

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

Logiciels sur différents composants

Différents composants exécutant des logiciels :

- Processeurs (principal, auxiliaires, communication)
- Contrôleurs
- Périphériques

Différents types de logiciels:

- Micrologiciels
- Logiciels de démarrage
- Environnements logiciels de confiance
- Systèmes d'exploitation

Appareils mobiles et liberté

Micrologiciels

Micrologiciels et liberté

Matériel associé :

- Processeurs auxiliaires
- Contrôleurs et périphériques

Prise en charge du logiciel libre :

- Matériel spécifique (Arduino, BusPirate, FX2LA)
- Périphériques Wi-Fi (ath9k_htc, AR9170, OpenFWWF)

Appareils mobiles :

- Micrologiciels **propriétaires**, rarement vérifiés
- Pre-installés ou chargés
- Wi-Fi, bluetooth, GPS, multimedia, caméras, ...

Pas de micrologiciels libres pour les appareils mobiles

Appareils mobiles et liberté

Processeur de communication (modem)

Processeur de communication (modem) et liberté

Processeur de communication (modem) :

- Processeur puissant
- Système d'exploitation complet
- Interfaces R/F

Logiciels pour le modem :

- Systèmes **propriétaires** (appareils modernes)
- Remplacer le système, vérifications

Prise en charge du logiciel libre :

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

Énorme problème pour la liberté et 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 modem :

- Contournement, autres moyens d'espionner
- Vérification pratique et confiance :
  preuve de mauvaise situation, modem intégré, schémas, matériel libre
- Problèmes de libertés ?

Solution pragmatique et jamais entièrement fiable

Appareils mobiles et liberté

Processeur principal

Logiciels sur le processeur principal

Différentes couches logicielles :

- Logiciels de démarrage
- Environnement logiciel de confiance
- Système d'exploitation :
  - Noyau (Linux)
  - Couches d'abstraction matérielle
  - *Frameworks*
  - Applications

Logiciels de démarrage et liberté

Logiciels de démarrage :

- Bootrom : **privateur**, mémoire non-réinscriptible (hardware)
- Vérifications de **signatures**, chargement en chaîne spécifique à la plateforme, variante
- Logiciels de démarrage libres : **U-Boot, Coreboot**
- Exemples de bonnes plateformes : i.MX, Allwinner, OMAP (GP), Tegra (non-ODM), Rockchip
- Quels appareils mobiles ?

Logiciels de démarrage libres pour quelques appareils mobiles

Environnement logiciel de confiance

Besoin de logiciels de confiance :

- Système d'exploitation imparfait
- Opérations privilégiées, accès matériel
- Opérations sensibles (vie privée/sécurité)

Implémentation d'un environnement logiciel de confiance:

- Coopération avec la puce (**TrustZone**)
- Mis en place rapidement (logiciel de démarrage)
- Mode privilégié, *Secure Monitor Call (SMC)*

Environnement logiciel de confiance et liberté

Conséquences pour la liberté :

- Pas bon ou mauvais *per-se*
- Privilèges
- Implications pour la **vie privée/sécurité**
- Implémentations libres
- Dépendance au logiciel de démarrage
- Implémentations **propriétaires** et **vérifiées** (appareils récents)
- Bons exemples connus : USB armory avec i.MX53, Rockchip

Souvent problématique pour les appareils récents
mais pourrait respecter la liberté

Système d'exploitation et liberté

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*

Au premier plan du logiciel libre :

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

Système d'exploitation et liberté

Couches des systèmes d'exploitation :

- Noyau : Linux, **libre**, versions modifiées, drivers 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 matérielle et liberté

Aspects généralement problématiques :

- Accélération graphique, GPU
- GPS

Selon les plateformes :

- Caméras (dépendance au GPU)
- Audio

Projets dédiés libération des aspects complexes (GPUs) :

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

Couches privatrices : 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

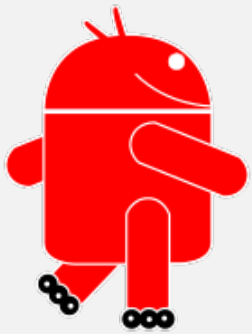
Approches à court et moyen terme :

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

Bilan et remédiations possibles

Système libre : Replicant

Replicant : système libre pour appareils mobiles



Replicant

Projet basé sur des idées et valeurs :

- Système mobile entièrement libre, basé sur Android
- Distribution et recommandation de logiciel libre exclusivement (GNU FSDG)
- Accent sur la vie privée/sécurité
- Fonctionnel et utilisable
- Information et documentation

État du projet Replicant

État actuel du projet :

- **Très peu** de développeurs, temps libre
- Peu (mais de plus en plus) 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

Maintenus

- 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

Objectifs futurs :

- Version plus récente (6.0)
- 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)

Améliorations vie privée/sécurité :

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

Bilan et remédiations possibles

Meilleurs appareils

Appareils pris en charge, liberté, vie privée/sécurité

Mauvaise isolation du modem
Chargeurs de démarrage
privateurs et signés

Choix d'appareils pour Replicant

Pris en charge de meilleurs appareils :

- Designs matériels libres, documentation du matériel
- Appareils sans modem, isolation du modem
- Logiciels de démarrage libres
- Protocoles connus et drivers libres

Communauté **OpenPhoenux** :

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

Appareils chinois peu coûteux :

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

Appareils produits en masse :

- **Optimus Black** (LG)
- **Kindle Fire** première génération (Amazon)

Autres **formats** d'appareils !

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)