# Les systèmes mobiles sont-ils plus sûrs ?

Nicolas RUFF
EADS Innovation Works
nicolas.ruff (à) eads.net

# Introduction

## Ex-leaders

- (Systèmes propriétaires)
- Symbian
- Windows Mobile

## Leaders

- Apple iOS
- Android
- BlackBerry

## Challengers

- Windows Phone 7
- WebOS (HP, ex-Palm)
- MeeGo (Nokia, Intel)
- BadaOS (Samsung)

# Introduction

## Ex-leaders

- (Systèmes propriétaires)
- Symbian
- Windows Mobile

## Leaders

- Apple iOS
- Android
- BlackBerry

## Challengers

- Windows Phone 7
- WebOS (HP, ex-Palm)
- MeeGo (Nokia, Intel)
- BadaOS (Samsung)

# L'histoire d'Android

- 2003
  - Création de la société Android, Inc.
  - Basée en Californie
  - Montée par des anciens du monde télécom
- 2005
  - Rachat par Google
- 2007
  - Sortie du "produit"
  - Annonce de l'Open Handset Alliance
- Les choix de conception n'ont pas été faits par Google

# Le système Android

- Matériel: *smartphones* & tablettes
  - Mais aussi TV, voitures, réfrigérateurs ... ?
- Processeur: ARM
  - X86, MIPS sont aussi supportés
- Noyau: GNU/Linux 2.6
- LibC: "Bionic" (basé sur *BSD)
- Runtime: "Dalvik"
  - Sorte de JVM
- La "plupart" du code est Open Source
  - Sauf les firmwares et les applications Google

# Remarques affectant la sécurité

- L'écriture de *shellcodes* Linux/ARM est un problème réglé
  - … en 2001
- La JVM n'est pas une frontière de sécurité
  - Code natif (NDK)
  - Les permissions Unix sont la véritable frontière
- Signature des applications
  - Utilisée uniquement à des fins de révocation
    - Certificats autosignés, expiration > 22 octobre 2033
  - Mécanisme de révocation connu et analysé
    - Processus GTalkService + SSL
- Y a-t-il un modèle de sécurité formel attaché aux permissions ?
  - adb shell pm list permissions

# Les risques

- Structure du marché de la téléphonie
  - Trop d'intervenants aux intérêts contradictoires
  - Diffusion des mises à jour longue et difficile

- Failles logicielles
  - Système
  - Navigateur
    - Flash Player
  - Failles logiques
    - Ex. mot de passe "null"

- Applications tierce partie
  - Le risque n°1 aujourd'hui
    - Les développeurs veulent gagner de l'argent …

# Risques - Failles système

- "Exploid"
  - CVE-2009-1185 (faille "udev")
    - No comment …
- "RageAgainstTheCage"
  - *adb* ne vérifie pas le code de retour de *setuid()*
  - Utilisation astucieuse de RLIMIT_NPROC
- "KillingInTheNameOf"
  - */dev/ashmem* permet d'accéder à la mémoire du noyau
  - *ro.secure* permet d'autoriser *adb* à tourner en *root*
- Des failles très concrètes
  - xSports, VISIONary+, DroidDream …

# Risques - Navigateur

- Le moteur WebKit …
  - Une passoire !
    - http://www.exploit-db.com/exploits/15423/
    - http://www.exploit-db.com/exploits/16974/
    - http://blog.metasploit.com/2011/01/mobile-device-security-and-android-file.html
    - Pwn2own
    - ( XSS sur la MarketPlace )
- Les spécificités Android …
  - Peu testées !
    - content://com.android.htmlfileprovider/<filename>
    - market://details?id=<package>

# Risques - Applications

- Failles accidentelles dans les applications
  - Failles conceptuelles
    - Ex. communications en clair
    - Ex. mots de passe en dur
      - http://jack-mannino.blogspot.com/2011/02/scary-scary-mobile-banking.html
  - Failles d'implémentation
    - Ex. il existe des injections SQLite !
    - Ex. *buffer overflow* dans du code natif (NDK)

- Failles intentionnelles dans les applications
    - Ex. Tank Hero
    - Ex. DroidDream

# Auditer les applications

- Aucune difficulté
  - Le *bytecode* se décompile
    - ProGuard introduit avec Android 2.2
  - Le code natif ne présente aucune spécificité délicate
  - L'environnement est très ouvert

- Outils
  - DEXDUMP
  - APKTOOLS (dont SMALI/BAKSMALI)
  - *Remote Debugging*
  - Instrumentation

# DEMO !

# Extrapolation

- Apple iOS
  - Basé sur du code "Open Source"
  - MarketPlace
    - Mais plus sévèrement contrôlée
- BlackBerry
  - Code propriétaire
    - Le navigateur est basé sur WebKit
    - "Des gens" savent faire
      - http://www.blackberry.com/btsc/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=KB26132&sliceId=1&docTypeID=DT_SECURITY_1_1
  - MarketPlace

# Conclusion

- Nous vivons l'an 1 de la sécurité mobile
  - Et l'an 0 de la sécurité logicielle sur mobile
    - C'est le bon moment pour s'y mettre ☺
- La différence avec un PC ?
  - L'utilisateur final est complètement démuni
  - L'avenir du monde libre repose entièrement sur Apple et Google
    - On peut dormir tranquille … ou pas