Sécurité des plateformes mobiles

Entre mythes et réalités

Nicolas RUFF

EADS Innovation Works

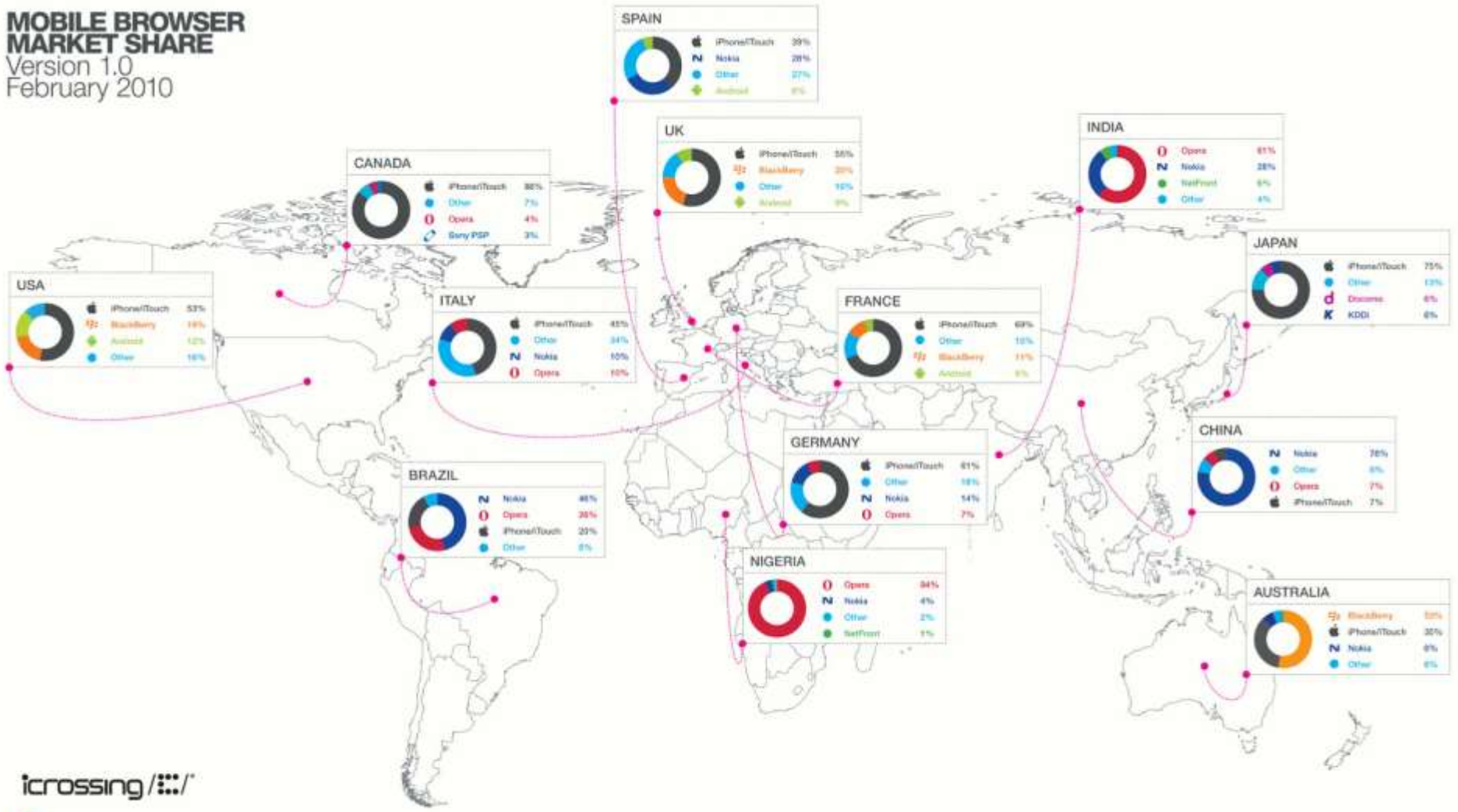
nicolas.ruff(à)eads.net

Quelques chiffres

- A l'heure où je vous parle (Q3 2012)
  - Parts de marché
  - Samsung: 31,3%
  - Apple: 15,0%
    - http://www.idc.com/getdoc.jsp?containerId=prUS23753512
  - 1/3 des français se connectent à Internet avec leur SmartPhone avant de sortir du lit
    - Source:
      - http://www.blog-ericssonfrance.com/2012/09/infographie-selon-le-consumerlab-d%E2%80%99ericsson-les-francais-sont-les-plus-connectes-a-leur-smartphone-dans-les-transports/infographie-ericsson-consumerlab-france-septembre-2012/

Quelques chiffres

Quelques chiffres



Plan (horizontal)

- Principalement …
  - Android
  - iOS
- Et accessoirement …
  - Windows Phone 7.x
  - Windows Phone 8
  - BlackBerry
  - Autres / propriétaires

Plan (vertical)

- Points clés
- Modèles de sécurité
- Chiffrement et verrouillage
- Stockage des secrets
- *Markets / Stores*
- *Jailbreaking*
- Failles connues
- *Baseband*
- ROM alternatives
- Risques
- BYOD
- MDM
- Gestion en entreprise
- Antivirus
- Bonnes pratiques

Android vs. iOS
Points clés

Android

- Système ouvert et bien documenté
  - http://developer.android.com/index.html
- Noyau Linux
- Applications Java
- Matériel multiple
  - ARM, MIPS, x86 …
  - Téléphones, tablettes, TV, voitures …
- Surcouches "constructeurs"
  - Samsung Kies, HTC Sense, etc.

iOS

- Système complètement fermé
- Noyau OS X
  - MACH + FreeBSD
- Applications Objective-C
- Matériel unique
  - iPod, iPhone, iPad, …

Android vs. iOS
Modèle de sécurité

Android

- Permissions
  - Par catégories
  - Affichées à l'installation
  - Acceptées globalement
- Signature des applications
  - Destinée à l'identification / révocation
  - … mais pas au contrôle d'intégrité
- Chiffrement des applications par *device*
  - Depuis Android 4.1
- Séparation des applications par "uid" Unix
  - 1 application = 1 processus = 1 "uid"
- Emulateur disponible

iOS

- Permissions
  - Par catégories
  - Affichées à l'utilisation
  - Acceptées unitairement
- Signature des applications
  - … y compris en mémoire à l'exécution
- Chiffrement des applications par *device*
- Séparation des applications par "*sandboxing*"
  - TrustedBSD + scripts Scheme
- Pas d'émulateur disponible

Android vs. iOS
Chiffrement et verrouillage

Android

- Chiffrement
  - Disponible depuis Android 3.0
  - Uniquement les partitions utilisateur
  - Clé dérivée du code de verrouillage
- Verrouillage
  - Code de verrouillage stocké dans un fichier
  - Peut être attaqué "*offline*" en force brute

iOS

- Chiffrement
  - Disponible depuis iPhone 3GS
  - Chiffrement intégral de la mémoire Flash
  - Elément de sécurité matériel
- Verrouillage
  - Vérifié par un élément matériel
  - Difficile à attaquer
    - ~1h pour un code PIN à 4 chiffres

Android vs. iOS
Stockage des secrets

Android

- Pas de méthode standard
  - SQLite recommandé pour les applications
    - … mais on voit de tout
  - Pas de méthode standard pour le système
    - Ex. stockage des clés WiFi en clair dans un fichier à plat

iOS

- *Keychain* avec plusieurs niveaux de protection
  1. Démarrage du système
  2. Téléphone déverrouillé
  3. Aucun

Android vs. iOS
Markets / stores

Android

- Sources d'installation
  - Google Play
    - Outil "bouncer" – peu efficace
  - Fichiers APK
    - Provenance souvent illégale
  - Markets alternatifs
    - Ex. Amazon
    - Souvent aucune vérification
- Problème(s)
  - "*Repacking*"
    - Les applications gratuites sont la cause n°1 des problèmes de sécurité sur Android

iOS

- Sources d'installation
  - AppStore officiel
  - Cydia / fichiers IPA
    - Provenance souvent illégale
    - Appareils jailbreakés uniquement
- Problème(s)
  - Mises à jour lentes
  - Compatibilité avec les anciennes versions iOS pas toujours assurée

Android vs. iOS
Jailbreaking

Android

- Principes
  - "/system" remonté en écriture
  - Binaire "sudo"
- Parfois autorisé par le constructeur
  - Téléphone de développement Google
  - Outil "Odin" pour Samsung
  - Site officiel HTC
  - …

iOS

- Principes
  - "*Patch*" annulant toutes les sécurités logicielles
    - Signature de code
    - Sandboxing
    - W ^ X
    - …
- Totalement prohibé par Apple
  - … mais pas illégal
  - … et même indispensable aux auditeurs sécurité !

Jailbreaking

- Pourquoi *jailbreaker* ?
  - Fun / défi technique
  - Installer des ROM alternatives
  - Tricher dans les jeux
  - Auditer des applications tierces
  - Installer des applications piratées
  - …

- Ne pas confondre …
  - Faille "boot ROM" vs. "système"
    - Les failles "boot ROM" ne peuvent pas être corrigées par une mise à jour logicielle
  - *Jailbreak* "*tethered*" vs. "*untethered*"
    - "*tethered*" ne survit pas à un redémarrage
  - SIM *unlocking*
    - Attaque du *baseband* pour rendre le téléphone compatible tout opérateur

Android vs. iOS
Failles connues

Android

- Failles Linux
- Failles WebKit
  - Ex. Metasploit "android_htmlfileprovider"
- (Failles Flash)
- Failles spécifiques Android
  - Ex. "rage against the cage", "zerg rush", …
- Failles spécifiques à certains pilotes
  - Ex. PowerVR SGX ("levitator.c")

iOS

- Failles iOS
- Failles WebKit
- Failles logicielles diverses
  - Ex. vérification incorrecte des chaines de certificats avant iOS 4.3.5
  - Ex. jailbreakme.com
    - Faille dans le lecteur PDF
  - Ex. Contournement du W^X
    - Charlie Miller, 2011

Android vs. iOS
Failles connues

Android

- Utilisation des failles "dans la nature"
  - *Jailbreak*
  - *Forensics*
  - Applications malveillantes

iOS

- Utilisation des failles "dans la nature"
  - *Jailbreak*
  - *Forensics*

Failles connues

- Quelles failles ?
  - Rien de nouveau sous le soleil !
    - *Buffer / integer overflow*
    - Injections SQL
    - XSS
    - Permissions incorrectes
    - Implémentations cryptographiques défaillantes
    - Failles logiques
      - Cf. changelog iOS
    - …
  - … ainsi que quelques nouveautés
    - Ex. logique des "intents" (Android)
    - Ex. content://<…>
    - Ex. tel://<code magique>

Failles connues

- Y a-t-il moins de failles sous iOS ?
  - Non, mais elles coûtent plus cher !
    - Source: Forbes

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

Baseband

- *Baseband* = processeur de traitement téléphonique
  - Peu de fabricants
    - Qualcomm, Infineon …
  - Attaques connues
    - Ex. "*The Baseband Apocalypse*"
    - Implémentation facile (USRP / radio logicielle / OpenBTS / …)
  - Défense impossible
    - Echappe à tout contrôle par l'*Application Processor*

- WiFi
  - Ex. activation du mode "moniteur" dans le firmware Broadcom
    - Présenté par Core Security
- NFC
  - Ex. challenge PWN2OWN @ EuSecWest 2012

Android
ROMs alternatives

- Communautaires
  - Ex. CyanogenMod
- Professionnelles
  - Ex. Ercom, WhisperSys, SecDroid …
- Parfois plus sûres que les ROM constructeurs (!)
  - Moins de *bloatware*
  - Plus à jour
  - Nouvelles fonctionnalités
    - Ex. pare-feu applicatif

Android vs. iOS
Synthèse des risques

Android

- Obsolescence du matériel / fragmentation
- Rythme des mises à jour système
- Applications "constructeurs" (*bloatware*)
- Applications légitimes
  - Ex. pas de SSL
- Applications malveillantes

iOS

- Obsolescence du matériel
- Rythme des mises à jour système
- Applications légitimes
  - Ex. pas de SSL
- Aucun contrôle sur le *device* (sauf par Apple)

Autres systèmes

- Musée
  - Symbian
  - Windows CE (6.x) et Windows Phone 7.x

- Concurrents
  - Windows Phone 8
    - Pas de retour d'expérience pour le moment
  - BlackBerry 10
    - Noyau QNX
  - Autres / propriétaires
    - badaOS (Samsung)
    - webOS
    - meeGo (ou assimilé)
    - Facebook OS
    - Firefox OS
    - Ubuntu for Mobiles
    - …

BYO(N)D is FUD

1. Ne pas confondre "BYOD" et "*consumerization*"
   - Ne pas confondre "BYOD" et "ATAWADAC" ☺

2. Le "vrai" BYOD (à l'anglo-saxonne) n'existe(ra) pas en France
   - Cadre légal, respect des règlements, mentalités …
   - BYOD = "je veux lire mon mail sur iPad sans aucun contrôle de l'IT"

3. Toute résistance est inutile - préparez vous à l'assimilation
   - Dropbox, Gmail, SlideShare, réseaux 3G …
   - Le BYOD permet d'échapper à l'IT
   - Le BYOD est l'anti-BlackBerry

MDM (*Mobile Device Management*)

- Deux approches
  - "*Policy Enforcement*"
  - "*Containerization*"

- Pas de solution magique
  - Les produits ont l'obligation technique de passer par les API du système
  - Les produits sont des applications comme les autres
  - Les produits sont immatures
    - *Horror Stories*

Gestion en entreprise

- Tous les systèmes "modernes" supportent …
  - Synchronisation Exchange / ActiveSync
  - Définition de politiques de sécurité
    - GPO = MCX chez Apple

- Apple iOS
  - Certificat de signature "*enterprise developer*"
  - AppStore d'entreprise
  - Achat d'applications en volume (VPP)

Antivirus

- L'antivirus est une application comme les autres
  - … facile à désactiver / désinstaller
- L'antivirus demande les permissions maximales
  - … et il n'est pas toujours bien programmé
- … mais il peut quand même détecter les applications malveillantes les plus courantes !
  - Android uniquement

Quelques audits applicatifs …

- Les coffres-forts de mot de passe sur smartphone
  - Le meilleur est le code PIN proposé nativement par iOS

Name	Complexity	CPU p/s	GPU p/s	Len/24h
Keeper® Password & Data Vault	1x MD5	60 M	6000 M	14.7
Password Safe - iPassSafe Free	1x AES-256	20 M	N/A	12.2
Strip Lite - Password Manager	4000x PBKDF2-SHA1 + 1x AES-256	5000	160 K	10.1
SafeWallet - Password Manager	10x PBKDF2-SHA1 + 1x AES-256	1500 K	20 M	12.2
DataVault Password Manager	1x SHA-256 + 1x SHA-1	7 M	500 M	13.6
mSecure - Password Manager	1x SHA-256 + 1x Blowfish	300 K	N/A	10.4
~~LastPass for Premium Customers~~	~~2x SHA-256 + 1x AES-256~~	~~5 M~~	~~20 M~~	~~12.2~~
LastPass for Premium Customers	500*x PBKDF2-SHA256 + 1x AES-256	12K	600K	10.7
~~1Password Pro~~	~~1x MD5 + 1x AES-128~~	~~15 M~~	~~20 M~~	~~12.2~~
1Password Pro	10'000x PBKDF2-SHA1 + 1x AES-256	2000	65K	9.7
BlackBerry Password Keeper	3x PBKDF2-SHA1 + 1x AES-256	5 M	20 M	12.2
BlackBerry Wallet 1.0	2x SHA-256	6 M	300 M	13.4
BlackBerry Wallet 1.2	1x SHA-512 + 100x PBKDF2-SHA1 + 1x AES-256	200K	3200 K	11.4
iOS passcode	50000 iterations with HW AES	6	0	5.7

- Source
  - http://2012.hackitoergosum.org/blog/wp-content/uploads/2012/04/HES-2012-belenko_sklyarov-Secure-Password-Managers.pdf

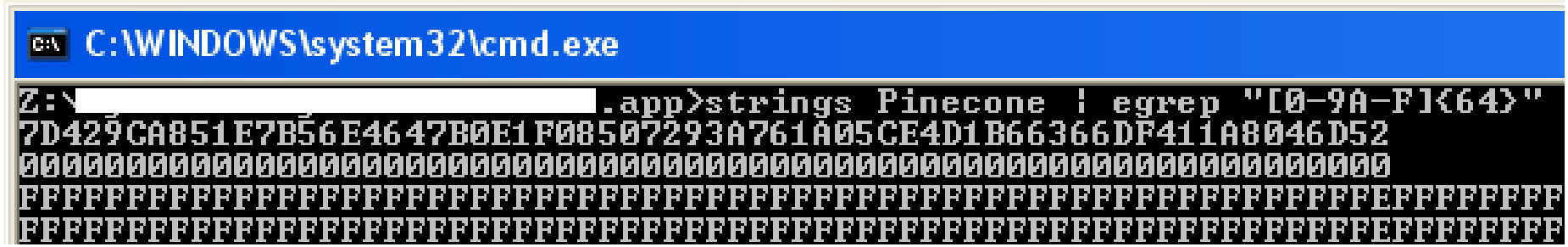
Quelques audits applicatifs …

```
Description
-----------
GMA is known as "Good™ Mobile Access" and part of "Good for Enteprise"
"The secure browser is integrated into the Good for Enterprise application, delivering a safe,
intelligent user experience. Employees can launch Good's browser directly from the Good launcher bar,
as well as through links included in emails. Links to public websites will automatically launch
the native browser."

Title : GOOD for Enterprise GMA below 2.0.2 vulnerable to MITM
URL : http://www-staging.good.com/products/good-mobile-access.php
Root Cause: GMA failed to validate server authenticity when connecting through HTTPS

I spotted what appears to be an undisclosed vulnerability in an
enterprise mobile device management system.

https://itunes.apple.com/us/app/good-for-enterprise/id333202351?mt=8

Excerpt from above :

What's New in Version 2.0.2
This release addresses the following
[..]- GMA now validates server authenticity when connecting through HTTPS.
[..]

This would imply GMA to have been vulnerable to MITM prior to version 2.0.2

Disclosure Timeline :
=====================
- GOOD disclosed over iTunes on the 02.08.2012
```

- Source
  - http://seclists.org/fulldisclosure/2012/Nov/72

Quelques audits applicatifs …

- *Containerization*
  - Quizz: où est la clé du chiffrement du conteneur ?



Quelques audits applicatifs …

- Côté serveur ?
  - Ca reste des applications Web …

25913 https://10.99.71.2 GET /mics/mics.html?action=getLocalUserList&limit=20&_dc=1352804861078&action=getLocalUserList 200

Request | Response

Raw | Headers | Hex

```
HTTP/1.1 200 OK
Date: Tue, 13 Nov 2012 11:07:41 GMT
Server: Apache-Coyote/1.1
Content-Type: application/json;charset=ISO-8859-1
Content-Language: en-US
Vary: Accept-Encoding
X-Frame-Options: SameOrigin
Content-Length: 508
Connection: close

{"total":2,"generationTime":1352804861265,"results":[{"deviceId":"","email":"","firstName":"","group":"","groupId":"","hashcode":"","id":0,"lastName":"","o
ldPassword":"","password":"[redacted]","principal":"admin","protocol":"","userActionId":0,"uuid":""},{"deviceId":"","email":"[redacted]","firstN
ame":"Fatima","group":"DEFAULT","groupId":"","hashcode":"","id":0,"lastName":"Ramos","oldPassword":"","password":"[redacted]","principal":"fatima","protocol"
:"","userActionId":0,"uuid":""}],"rc":true}
```

- Source
  - https://hackinparis.com/talk-sebastien-andrivet

Quelques audits applicatifs …

- Prix du meilleur "hack"
  - Désinstaller l'application de MDM sur iOS …
  - Note: il n'existe aucune parade à cette attaque

Quelques audits applicatifs …

- Prix de la meilleure réponse
  - "*La version 1.0 de notre produit n'est plus supportée. Nous avons racheté une société, et leur produit est devenu la version 2.0 du nôtre*"

Quelques audits applicatifs …

- Les produits de sécurité mobile …
  - … sont tous les mêmes
    - Ils sont limités par les API système
  - … ne sont pas mûrs
    - Pas d'audit indépendant
    - Pas de cycle de vie des vulnérabilités et des mises à jour
    - Evolution très rapide des plateformes
    - Plus de 40 vendeurs
- Note:
  - La détection à 100% de jailbreak sur iOS est théoriquement impossible

Démonstrations

Conclusion : bonnes pratiques

- Que faire ?
  - "*Lors ces choses nous dépassent, feignons d'en être les organisateurs*"
  - Détecter / surveiller les usages
  - Proposer des services alternatifs
  - Sensibiliser les utilisateurs
    - Rappeler les règles de base …
  - Anticiper les problèmes
  - (*Red Team*)

Conclusion : bonnes pratiques

- Quelques données brutes …
  - Barack Obama lit son *morning briefing* sur iPad
    - http://www.washingtonpost.com/blogs/checkpoint-washington/post/oval-office-ipad-presidents-daily-intelligence-brief-goes-high-tech/2012/04/12/gIQAVaLEDT_blog.html
  - La NSA autorise le BYOD
    - http://www.schneier.com/blog/archives/2012/09/the_nsa_and_the.html
  - L'application officielle des pilotes Airbus est disponible sur l'AppStore
    - https://itunes.apple.com/fr/app/flysmart-with-airbus-perfo/id535289299?mt=8
  - Le revenu Q3 2012 d'Apple est supérieur à celui de Microsoft, Google et Facebook cumulé
    - http://www.nytimes.com/2012/10/26/technology/apple-profits-rise-24-on-iphone-5-sales.html?_r=0
  - IBM fait machine arrière sur l'utilisation débridée des iDevices
    - http://www.journaldunet.com/solutions/mobilite/ibm-et-le-bring-your-own-device-0512.shtml

Conclusion : bonnes pratiques

- Les problèmes ouverts (en France)
  - Cadre légal
  - Propriété des données
  - Compte iTunes / Google associé au terminal
  - Carte bleue associée au terminal
  - Administrateurs malveillants
  - Contrôle par Apple / Google
    - Ex. révocation
  - Demain ?
    - Brevets, procès, évolution des CLUF, …

Questions

Références

- Android
  - Collectif
    - http://www.android.com/
  - Individus
    - http://jon.oberheide.org/
    - …
- iPhone
  - Collectif
    - http://theiphonewiki.com/wiki/
    - http://jailbrea.kr/
  - Individus
    - http://fr.wikipedia.org/wiki/George_Hotz
    - https://github.com/comex
    - https://github.com/planetbeing
    - …

Références

- Sogeti/ESEC
  - iPhone Data Protection Toolkit
    - http://code.google.com/p/iphone-dataprotection/
  - Analyse du *baseband*
    - http://esec-lab.sogeti.com/pages/Publications
- XDA Developers (forum)
    - http://www.xda-developers.com/
- Mobile PWN2OWN (challenge)
    - http://www.zdnet.com/mobile-pwn2own-iphone-4s-hacked-by-dutch-team-7000004498/

Références

- iOS ChangeLog
  - iOS 6.0.1
    - http://support.apple.com/kb/HT5567
  - iOS 6
    - http://support.apple.com/kb/HT5503
  - iOS 5.1.1
    - http://support.apple.com/kb/HT5278
  - iOS 5.1
    - http://support.apple.com/kb/HT5192
  - iOS 5.0.1
    - http://support.apple.com/kb/HT5052
  - iOS 5
    - http://support.apple.com/kb/HT4999
  - iOS 4.3.5
    - http://support.apple.com/kb/HT4824
  - …

  - Avis de sécurité Apple
    - http://support.apple.com/kb/HT1222

Références

- iOS Hacker Handbook
  - http://www.amazon.fr/iOS-Hackers-Handbook-Charlie-Miller/dp/1118204123