Risques et sécurité des systèmes nomades

Serge Bordères
Centre d'Etudes Nucléaires de Bordeaux-Gradignan
Observatoire des TEchnologies Nomade et de l'Internet pour la Recherche

JDEV2013

Ecole Polytechnique

4 septembre 2013

Quelques mots sur OBTENIR

Observatoire des Technologies Nomades et de l'Internet

http://www.obtenir.cnrs.fr

- Favoriser l'émergence d'une expertise dans le domaine des technologies nomades et de l'Internet.

- Favoriser la diffusion des connaissances par des formations, conférences, articles...

- Prospecter les technologies.

- Connaître et faire connaître l'usage de ces technologies au service de la recherche et plus particulièrement au sein des expériences.

Quelques mots sur OBTENIR

Observatoire des Technologies Nomades et de l'Internet

Site web => http://www.obtenir.cnrs.fr

Liste de diffusion => nomadisme ///AT/// service.cnrs.fr

- Un groupe d'une dizaine de personnes
- Parrainé par RESINFO et DEVLOG
- S'adresse à TOUS les acteurs de la recherche, informaticiens et utilisateurs
- Concerne tous les aspects du nomadisme physique (les postes de travail) ou virtuels (les données les services).

Pour commencer...deux citations

1ère citation

Document « Recommandations de sécurité relatives aux ordiphones » de l'ANSSI

Il est illusoire d'espérer atteindre un haut niveau de sécurité avec un ordiphone ou une tablette ordinaire, quel que soit le soin consacré à son paramétrage.

2ème citation

Patrick Paillou, directeur de l'ANSSI

[...]Je vais vous dire ma vision des choses : il faut entrer en résistance contre la liberté totale dans l'usage des technologies de l'information. [...] La sécurité c'est aussi avoir le courage de dire non

Sommaire

- Historique du conflit entre sécurité et nouvelles technologies
- Types de menaces
- Enjeu de la sécurité
- Comment casser la sécurité ? Rooter ou Jailbreaker
- Modèle de base de la sécurité dans IOS ou Androïd
  - Bac à sable
  - Système de fichiers
  - Permissions
  - Protections des « credentials » : keychains
  - Installation d'applications
  - Malware/Virus
- Le mélange des mondes : BYOD
- Principales fonctions de sécurité
  - Verrouillage d'écran
  - Mutli-utilisateur
  - Chiffrement : des principes très différents
- Protection du système d'information et de la sphère professionnelle
  - Les mobiles vecteurs de compromission
  - Mode professionnel : principe du silo
- Un exemple

Historique du conflit entre sécurité et nouvelles technologies

Fin des années 80

- Apparition des premiers virus sur les micro-ordinateurs diffusés par l' échange de disquettes

Milieu des années 90 : Développement d'Internet

- Basé sur le protocole IP, pas sécurisé et permettant divers types d'attaques
- Déploiement de protocole de messagerie pas sécurisés
- Possibilité de porter des attaques distantes
- Propagation des virus grandement facilitée

Début 2000 : Boom des services en ligne

- Nouvelles méthodes d'attaques sur les serveurs
- Attaques par social-engineering sur les utilisateurs

Historique du conflit entre sécurité et nouvelles technologies

Malgré tout nous continuons à utiliser toutes ces technologies pour payer nos achats ou pour piloter des instruments à distance.

Pourtant ces technologies sont pétries de problèmes de sécurité, et ne pouvaient « espérer atteindre un haut niveau de sécurité »....

Historique du conflit entre sécurité et nouvelles technologies

« L'Histoire nous apprend que l'Histoire ne nous apprend rien »

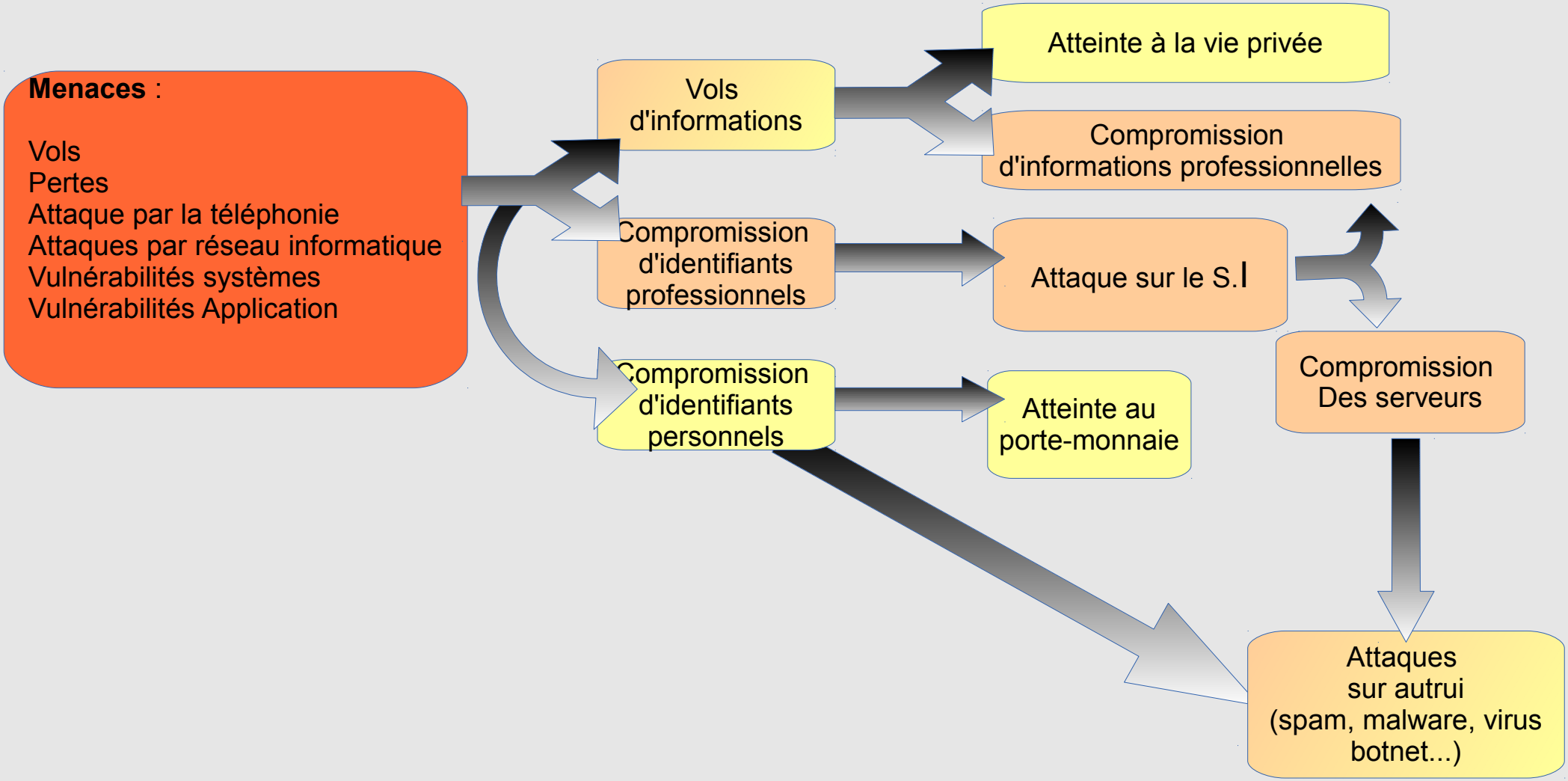
Comme d'habitude, la nouvelle vague technologique des mobiles n'a pas suffisamment intégré la sécurité dés le départ

Et pour compliquer les choses :

Pour la première fois de nouvelles technologies sont massivement introduites d'abord dans la sphère privée puis professionnelle

Types de menaces

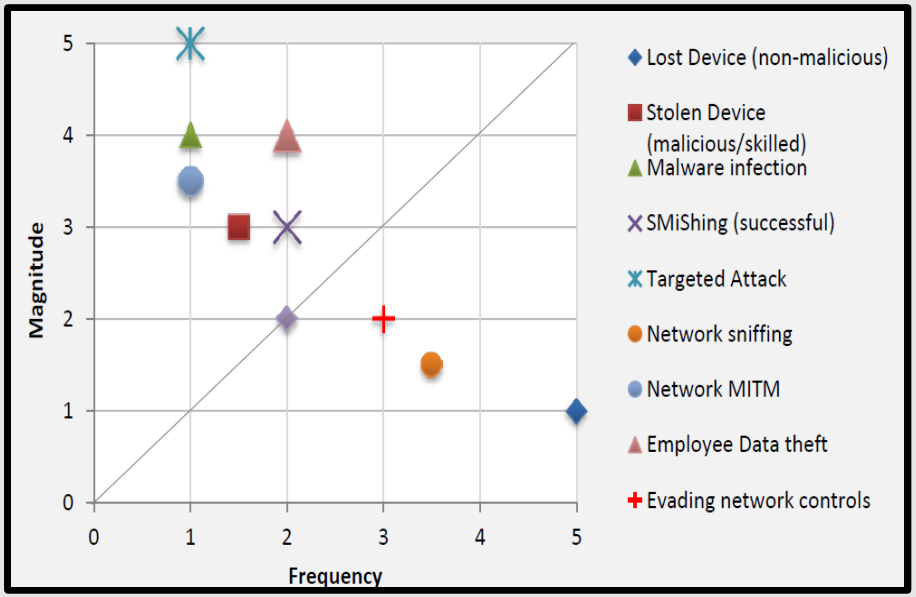
Des méthodes d'attaques classiques mais des risques exacerbés par le nombre de mobiles, leur diversité technique, les comportements, l'imbrication de tous les facteurs défavorables.



Types de menaces

Facteurs aggravants

- Forte volatilité des matériels
- L'effet statistique joue contre la sécurité
  (un mobile ça va...un milliard bonjour les dégâts)
- Outils très personnel, insouciance
- Matériels conçus avant tout pour une diffusion grand public.
- Manque de formation ou sur-estimation de connaissances
- Des applications regroupées en un seul lieu et très faciles à installer. Tentation de tout essayer (Google Play, Apple store)



Mobility Security risk report (viaForensics)
https://viaforensics.com/resources/reports/mobile-security-risk-report/

Enjeu de sécurité lié aux mobiles

Dans un établissement la probabilité qu'un mobile soit compromis est de plus en plus grande
Donc la probabilité que le S.I, lui-même, soit compromis augmente d'autant

*Risque = nbre de d'utilisateurs * nbre de matériels par utilisateur * comportements*

L'enjeu

Maîtriser ces aspects de sécurité pour définir les relations possibles avec le SI pour ne pas se faire ringardiser, déborder et trouver face à un SI underground encore plus risqué.

Les réponses ne peuvent pas être « j'interdis tout », ni « je laisse faire n'importe quoi »

Les réponses ne consisteront pas à simplement à sécuriser le mobile (si c'est possible) , mais aussi, et peut-être surtout, à se poser des questions sur le SI et, éventuellement, reconsidérer ses relations avec le monde extérieur.

Comment casser toute la sécurité ?

Comment casser toute la sécurité ? rooter ou jailbreaker !

Consiste à remplacer le système d'origine par un système modifié qui supprime la notion de privilèges. Toutes les applications tournent avec tous les privilèges.

Jailbreak : Principalement pour installer des applications depuis d'autres sources que Apple (notamment des applications payantes = piratage, violation du droit d'auteur....)
Fait perdre la garantie Apple

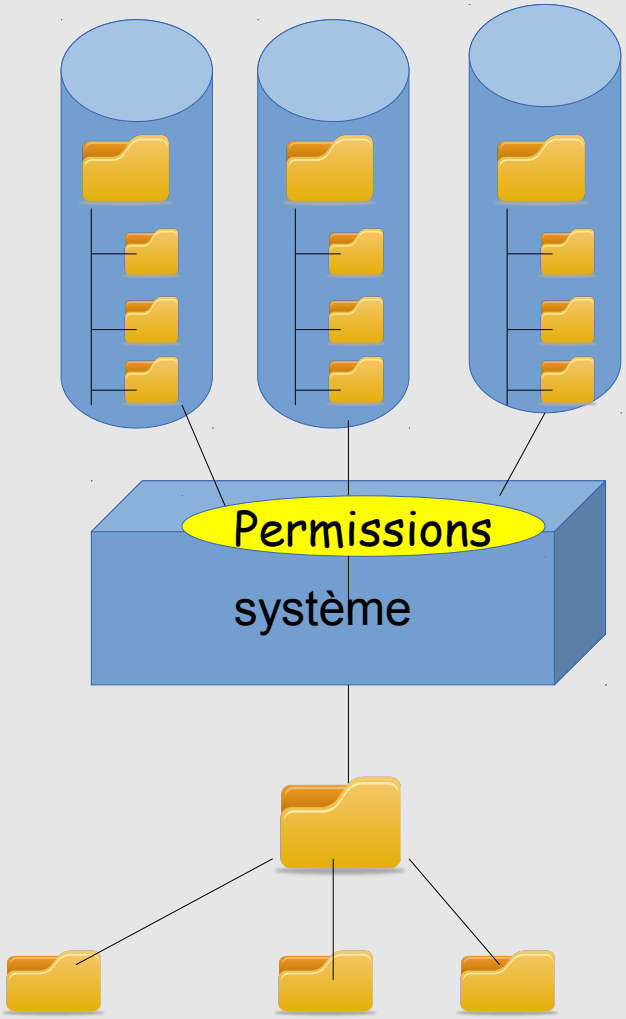
Rootage : n'est pas utile pour installer des applis de diverses sources, puisque c'est possible nativement.
Alors ?.... A quoi ça sert... ?

- La sécurité d'IOS ou Androïd est conçue pour des systèmes non rootés ou non jailbreakés
- Ce n'est pas la peine d'imaginer de sécuriser un mobile rooté/jailbreaké
- Il faut dissuader les utilisateurs de rooter/jailbreaker leur mobile
- Ne pas concevoir d'applications qui nécessiteraient de rooter/jailbreaker

Modèle de base de la sécurité dans IOS et Androïd

Le bac à sable

Le bac à sable est le principe général valable dans IOS et Androïd



- Chaque application tourne dans un conteneur (machine virtuelle/sandbox) qui l'isole des autres applications

- Dans Androïd une application ne peut interagir avec ce qui lui est extérieur qu'au travers des permissions qui lui sont accordées.

- Dans IOS pas de système de permission. Une application approuvée peut utiliser toutes les ressources du mobile.

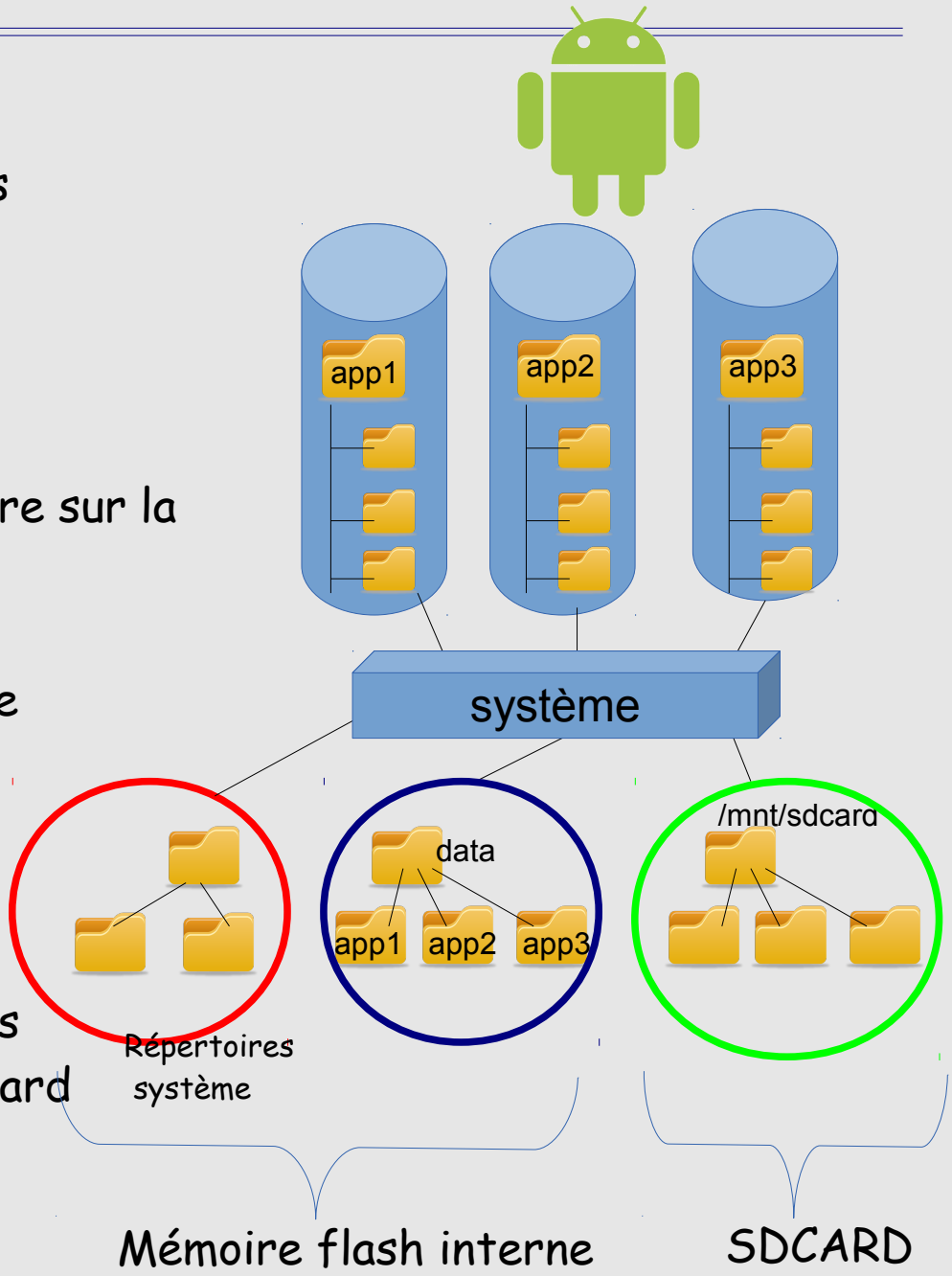
- Chaque application a sa propre arborescence

Système de fichiers

- Dans IOS il n'existe pas de système de fichiers partagés.
- Deux applications ne peuvent pas travailler sur le même document. (éventuellement il faut le dupliquer)
- La méthode de rangement est par application et non pas par projet.

Système de fichiers

- Androïd dispose de deux types d'emplacements mémoire :
  - La mémoire flash dite « interne »
  - La SDcard dite « externe »
- Lorsqu'une application est autorisée à lire/écrire sur la SDcard elle peut tout y lire/modifier
- L'utilisateur peut créer sa propre arborescence contenant toutes sortes de documents
- Structure en projet possible
- Il est possible de copier toute sorte de fichiers depuis un ordinateur ou une clé USB sur la SDcard



Système de fichiers

Dans la mémoire interne chaque application est propriétaire de son Home (chaque appli a un UID et un GID)

```
drwxr-x--x u0_a29   u0_a29   2013-04-18 09:09 com.android.wallpaper.livepicker
drwxr-x--x u0_a60   u0_a60   2013-04-18 09:09 com.example.android.apis
drwxr-x--x u0_a10   u0_a10   2013-04-18 09:09 com.example.android.livecubes
drwxr-x--x u0_a19   u0_a19   2013-04-18 09:09 com.google.android.apps.genie.geniewidget
drwxr-x--x u0_a31   u0_a31   2013-04-18 09:09 com.google.android.apps.uploader
drwxr-x--x system   system   2013-04-18 09:09 com.google.android.backup
drwxr-x--x u0_a21   u0_a21   2013-04-18 09:09 com.google.android.ears
drwxr-x--x u0_a22   u0_a22   2013-04-18 09:09 com.google.android.feedback
drwxr-x--x u0_a9    u0_a9    2013-07-02 15:48 com.google.android.gms
drwxr-x--x u0_a9    u0_a9    2013-04-18 09:09 com.google.android.gsf
drwxr-x--x u0_a9    u0_a9    2013-04-18 09:12 com.google.android.gsf.login
drwxr-x--x u0_a9    u0_a9    2013-04-18 09:09 com.google.android.location
drwxr-x--x u0_a52   u0_a52   2013-04-18 09:09 com.google.android.marvin.talkback
drwxr-x--x u0_a37   u0_a37   2013-04-18 09:09 com.google.android.onetimeinitializer
drwxr-x--x u0_a23   u0_a23   2013-04-18 09:09 com.google.android.partnersetup
drwxr-x--x u0_a46   u0_a46   2013-04-18 09:09 com.google.android.setupwizard
drwxr-x--x u0_a9    u0_a9    2013-04-18 09:12 com.google.android.syncadapters.bookmarks
drwxr-x--x u0_a20   u0_a20   2013-04-18 09:12 com.google.android.syncadapters.calendar
drwxr-x--x u0_a9    u0_a9    2013-04-19 09:59 com.google.android.syncadapters.contacts
drwxr-x--x u0_a51   u0_a51   2013-04-18 09:09 com.google.android.talk
drwxr-x--x u0_a57   u0_a57   2013-04-18 09:09 com.google.android.voicesearch
```

/data

Sur la carte SD tous les répertoires sont accessibles en RWX

```
u0_a63@android:/mnt/sdcard #
u0_a63@android:/mnt/sdcard #
u0_a63@android:/mnt/sdcard #
u0_a63@android:/mnt/sdcard #
u0_a63@android:/mnt/sdcard #
u0_a63@android:/mnt/sdcard # ls -l
drwxrwxrwx root     root              2013-04-18 07:09 Alarms
drwxrwxrwx root     root              2013-04-18 09:12 Android
drwxrwxrwx root     root              2013-04-18 07:09 DCIM
drwxrwxrwx root     root              2013-04-18 07:09 Download
drwxrwxrwx root     root              2013-04-18 07:09 Movies
drwxrwxrwx root     root              2013-04-18 07:09 Music
drwxrwxrwx root     root              2013-04-18 07:09 Notifications
drwxrwxrwx root     root              2013-04-18 07:09 Pictures
drwxrwxrwx root     root              2013-04-18 07:09 Podcasts
drwxrwxrwx root     root              2013-04-18 07:09 Ringtones
drwxrwxrwx root     root              2013-05-07 08:57 tmp
u0_a63@android:/mnt/sdcard #
u0_a63@android:/mnt/sdcard #
u0_a63@android:/mnt/sdcard #
u0_a63@android:/mnt/sdcard #
```

SDCARD

Donc accessibles pour toutes les applications qui ont la permission de lire/écrire sur la SDCARD(Modifier/supprimer le contenu du stockage USB)

Permissions

Entre Androïd et IOS le principe des permissions est très différent

Androïd

- Chaque application doit déclarer les permissions dont elle a besoin (manifest)
- Lors de l'installation, l'utilisateur doit accepter, ou pas, de délivrer les permissions à l'application
- Obligation d'accepter tout ou rien

IOS

- Pas de système d'approbation de permissions, une fois installée une application peut utiliser toutes les ressources de l'appareil
- Il n'y a pas de moyen de savoir ce qu'elle utilise.
- Depuis IOS 6.0, lorsqu'une application fait appel à certaines ressources (contact, calendrier....) une autorisation est demandée à l'utilisateur.
- Apple s'appuie sur son système d'approbation d'applications

Protection des « credentials » : Keychains

- Dans une base SQlite protégée avec un système différent du Data Protection
- Chiffré avec le passcode et/ou la clé stockée dans le processeur cryptographique.
- Accessible uniquement au travers d'un daemon spécialisé (systemd)
- Permet de stocker des certificats ou des mots de passe

- Même principe, géré par le service keystore
- Aujourd'hui stocke uniquement des certificats.
- Chiffré par une clé dérivée du passcode.
- Le dépôt d'un certificat dans le Keychain, impose le positionnement d'un passcode
- Dans Androïd 4.3 : Possibilité de « hardware-backed » pour protéger les clés (Nexus 4)

Protection des « credentials » : Keychains

Lost iPhone? Lost Passwords!
Practical Consideration of iOS Device Encryption Security

Fraunhofer Institute for Secure Information Technology
http://sit.sit.fraunhofer.de/studies/en/sc-iphone-passwords.pdf
http://sit.sit.fraunhofer.de/studies/en/sc-iphone-passwords-faq.pdf

Ces chercheurs expliquent qu'il est possible d'atteindre une bonne partie des secrets du keychain (mots de passe, certificats), même si le mobile est verrouillé par un passcode.
Concerne toutes les versions IOS au moins jusqu'à 6.0.1, mais avec des améliorations.

After using a jailbreaking tool, to get access to a command shell, we run a small script to access and decrypt the passwords found in the keychain. The decryption is done with the help of functions provided by the operating system itself (…) overall approach takes six minutes.

Ceci montre qu'un processeur cryptographique
n'est pas forcément un gage de sécurité.

Protection des « credentials » dans les applications

- Les développeurs sont libres d'utiliser ou pas les API keychain
- On ne sait pas vraiment si une application utilise le keychain pour stocker les mots de passe
- La gestion des mots de passe n'est donc pas forcément correcte (mot de passe en clair)

Et dans Goggle Play ?

- Tout utilisateur d'un mobile Androïd doit disposer d'un compte Gmail (et donc d'un mot de passe) pour pouvoir accéder à Google Play.
- Ce mot de passe n'est pas stocké dans le mobile.
- Lors de la première authentification un token est téléchargé sur le mobile (en clair dans /data/system/users/0/accounts.db)
- Ce token ne peut servir qu'à partir du mobile pour Google play et pas pour se connecter sur le compte Google avec un navigateur.
- Le changement de mot de passe Gmail, invalide le Token.

Installation d'applications

IOS

- Les applications peuvent être installées uniquement depuis l'Apple store (sauf jailbreak)

Sur Androïd plusieurs sources d'installation sont possibles :

- Le market de Google : Google Play
- Des markets tiers : Amazon, samsung....
- Directement à partir des packages
- L'utilisateur doit explicitement donner son autorisation pour utiliser autre chose que Google Play.

Installation d'applications

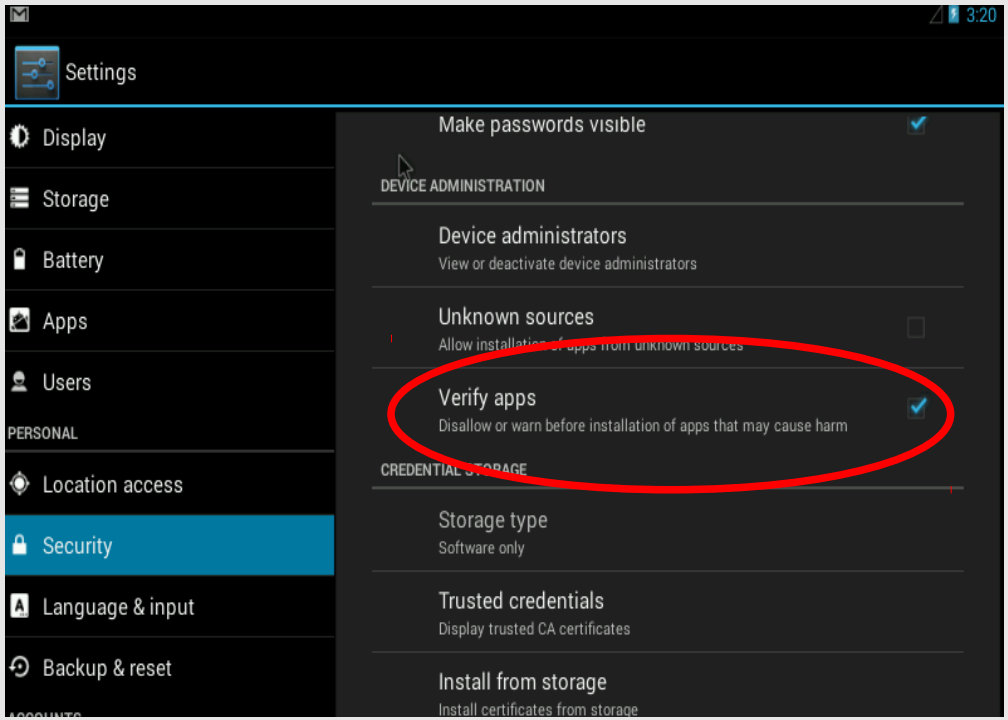
Apple met en avant son processus d'approbation d'application

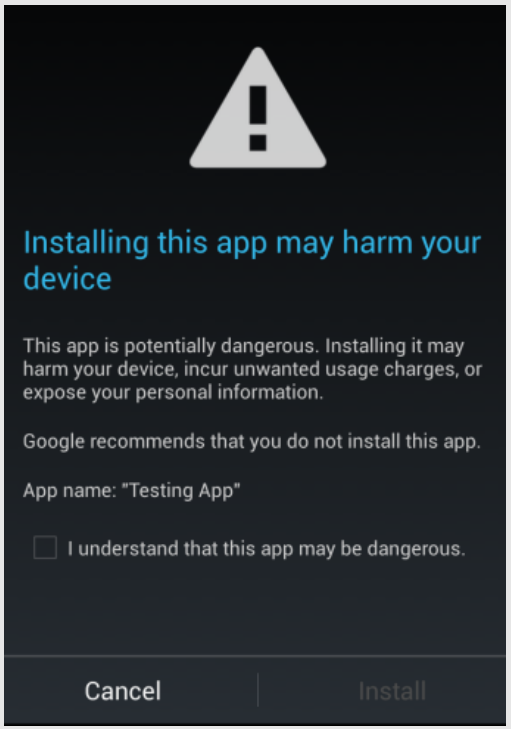
- Vérifie toutes les applications et leurs mises à jour
- Recherche de malware/dysfonctionnement
- Ne concerne pas seulement la sécurité
- Respect de règles d'éthiques (de qui?)
- Non concurrence avec les produits Apple.

Depuis 2012, Google a mis en place le service **Bouncer** qui scan toutes les applications soumises dans un environnement virtuel et simule leur comportement sur les serveurs de la firme.

Installation d'applications

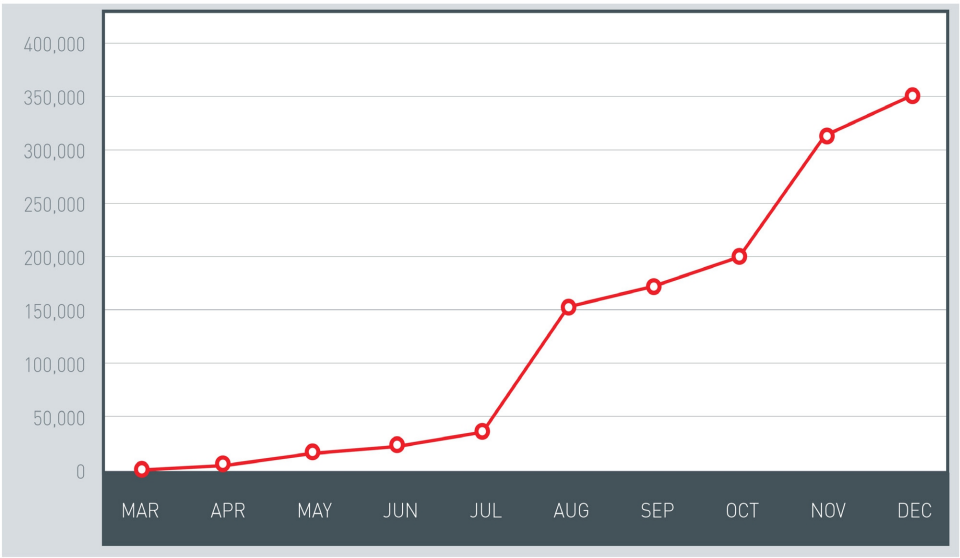
Avec Androïd 4.2 introduction de l'option « verify apps »
Qui permet d'analyser une application au moment de l'installation **quelle que soit** la source de l'installation.





Malware/ Virus

- Très forte hausse des détections de malwares sur Androïd
- La même histoire que sur les PC/Windows il y a quelques années
- La courbe de progression suit la courbe de déploiement d'Androïd (~80% du marché)
- Les éditeurs d'antivirus ne disent pas grand chose sur les malwares IOS (marché peu porteur?)
- Ne précisent pas la provenance des applications (markets officiels ou pas)
- Ne précisent pas si le code malveillant fonctionne sur du matériel non rooté et sur quel version d'Androïd



Progression de la détection de malware sous Androïd en 2012
(source trendmicro)

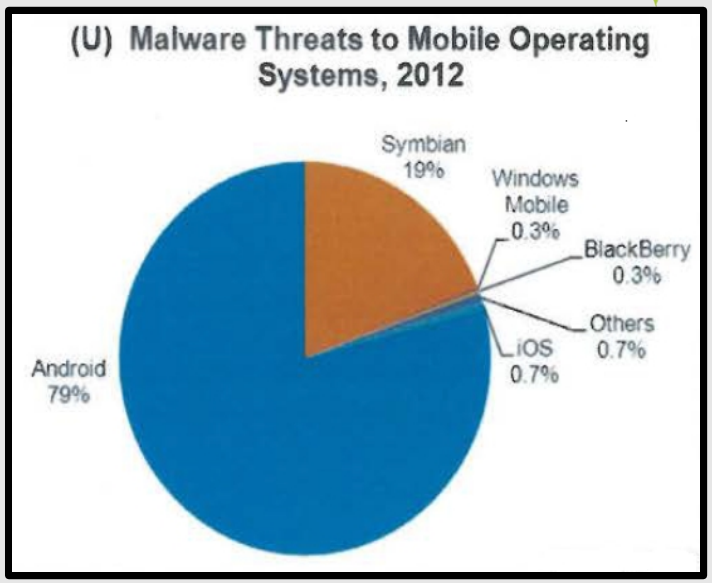
Malware/ Virus

Note de l'US Departement of Homeland Security du 23 juillet 2013

http://info.publicintelligence.net/DHS-FBI-AndroidThreats.pdf

- 79 % des malwares concernent Androïd
- 44 % des utilisateurs utilisent toujours une version Androïd < 2.3.7

- Préconise de mettre les systèmes à jour pour éliminer beaucoup de vulnérabilités connues



Androïd 4.3 demande une validation par l'utilisateur pour l'envoi d'une SMS

Security Threat	Description	Mitigation Strategy
SMS (Text Message) Trojans represent nearly half of the malicious applications circulating today on older Android OS.	Sends text messages to premium-rate numbers owned by criminal hackers without the user's knowledge, potentially resulting in exorbitant charges for the user.	Install an Android security suite designed to combat these threats. These security suites can be purchased or downloaded free from the Internet.
Rootkits are malware that hide their existence from normal forms of detection. In late 2011, a software developer's rootkit was discovered running on millions of mobile devices.	Logs the user's locations, keystrokes, and passwords without the user's knowledge.	Install the Carrier IQ Test—a free application that can detect and remove the malicious software.
Fake Google Play Domains are sites created by cybercriminals. Google Play enables users to browse and download music, books, magazines, movies, television programs, and other applications.	Tricks users into installing malicious applications that enable malicious actors to steal sensitive information, including financial data and log-in credentials.	Install only approved applications and follow IT department procedures to update devices' OS. Users should install and regularly update antivirus software for Android devices to detect and remove any malicious applications.

Malware/ Virus

Août 2013 - Jekyll on IOS : When Benign Apps become Evil

Des chercheurs de Geogia Institute of Technology ont montré qu'il était possible de contourner le processus d'approbation d'Apple pour injecter des malwares => Reconstruction du virus à l'exécution.

22th USENIX Security Symposiom 14-16 août 2013
https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_wang_2.pdf

Juillet 2013 - MACTANS: Injecting malware into IOS devices via malicious chargers

Une autre équipe de Georgia Institute of Technology a montré qu'il est possible d'injecter du code arbitraire dans IOS en utilisant un chargeur.

> Apple iOS devices are considered by many to be more secure than other mobile offerings. In evaluating this belief, we investigated the extent to which security threats were considered when performing everyday activities such as charging a device. The results were alarming: despite the plethora of defense mechanisms in iOS, we successfully injected arbitrary software into current generation Apple devices running the latest iOS software. All users are affected, as our approach requires neither a jailbroken device nor user interaction

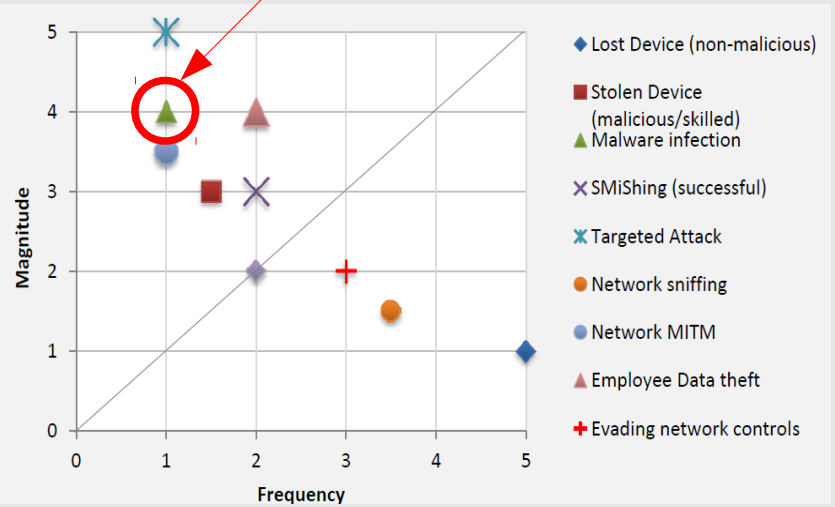
Conference BlackHat 27 juillet – 1 août 2013
https://media.blackhat.com/us-13/US-13-Lau-Mactans-Injecting-Malware-into-iOS-Devices-via-Malicious-Chargers-WP.pdf

Malware/ Virus

Quelle est la probabilité d'être victime d'un virus/malware ?

Faible à condition de respecter quelques règles :

- Ne pas rooter ou jailbreaker
- Installer les applications à partir de market reconnus
- S'interdire l'installation directe à partir de packages à l'origine douteuse
- Faire les mises à jour
- Vivre loin de ces pays



Top 10 des pays qui téléchargent le plus de malware (Trendmicro)

Malware/ Virus

Utilisation d'un scanner d'applications

Exemple avec VirusTotal (racheté par Google)

Consiste a scanner les packages des applications installées sur un mobile et à les confronter à une base d'antivirus située chez VirusTotal.

Méthode :

- Installer l'app VirusTotal sur le mobile depuis Google Play (ne demande aucun privilège à part l'accès réseau).
- Lancer l'application
- Le résultat est un listing qui donne l'état de chaque application (détection d'un malware ou pas)
- Il peut y avoir des faux positifs
- Peut-être difficile pour un utilisateur final
- Intéressant pour l'administrateur pour vérifier les applications qu'il conseille.
- Intéressant pour le développeur qui peut vérifier si son application ne déclenche pas de faux positifs.

Malware/ Virus

Utilisation d'un scanner d'applications
Exemple avec VirusTotal

Suppression à distance

Applications

Google et Apple ont la possibilité de supprimer à distance une application douteuse

Data

- IOS possède depuis longtemps une fonction de destruction à distance des données déclenchables par l'utilisateur
- Depuis Septembre 2013 (now!) Androïd (> 2.2) dispose également de cette fonction

Le mélange des mondes

B.Y.O.D

Bring Your Own Device

Pratique qui consiste à utiliser un matériel personnel dans l'activité professionnelle

Soit il s'agit d'une politique volontaire d'un établissement
Soit il s'agit d'un fait accompli

Pour la première fois les nouvelles technologies sont introduites d'abord dans la sphère privée puis professionnelle

Un mobile professionnel (acheté par l'employeur) devient très vite personnel

B.Y.O.D

- L'usage de matériel personnel n'est pas une nouveauté, cela concerne aussi les ordinateurs classiques.
- En réalité le BYOD ne doit pas être vu comme le simple usage d'appareil perso mais comme une **politique** qui intègre ce phénomène afin de conserver :

- Le contrôle sur le périmètre et les fonctions disponibles
  On ne fait pas n'importe quoi, on évolue
- La propriété des informations
  Le fait d'utiliser un matériel perso ne veut pas dire que les données vous appartiennent
- La localisation des données (Extension du cas précédent)
- La sécurité du système d'information

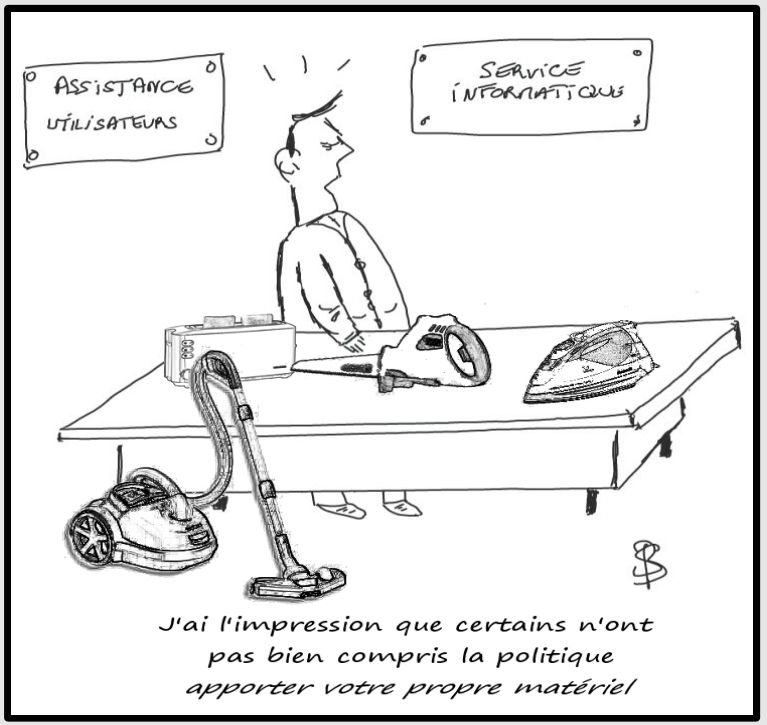
B.Y.O.D : Diversité accrue des OS

Le BYOD c'est comme la fin des uniformes dans les écoles

Citation magazine MISC N°66 mars/avril 2013

- La diversité des OS est **une contrainte** pour les informaticiens mais une tendance naturelle (bio-diversité plus riche qu'uniformité)

- IOS et Androïd sont des unix/linux donc il ne s'agit pas d'un changement fondamental de culture technique. C'est plus un problème de formation, de tests, d'intégration des procédures, de prise en main.



Une politique BYOD doit définir les OS supportés et donner aux informaticiens les moyens de se former.

B.Y.O.D : Volatilité des mobiles

L'ensemble des terminaux qui accèdent au S.I n'est plus complètement géré ni même connu.

- **Un utilisateur peut posséder plusieurs mobiles**
- **Que devient un mobile en fin de vie ?**
  - cédé à un membre de la famille ?
  - Vendu ?
  - Dans tous les cas a-t-il été remis en configuration d'usine et toutes les informations qu'il contient effacées (notamment les mots de passe) ?
- **En cas de panne, l'opérateur le remplace. Les informations sont-elles effacées ?**

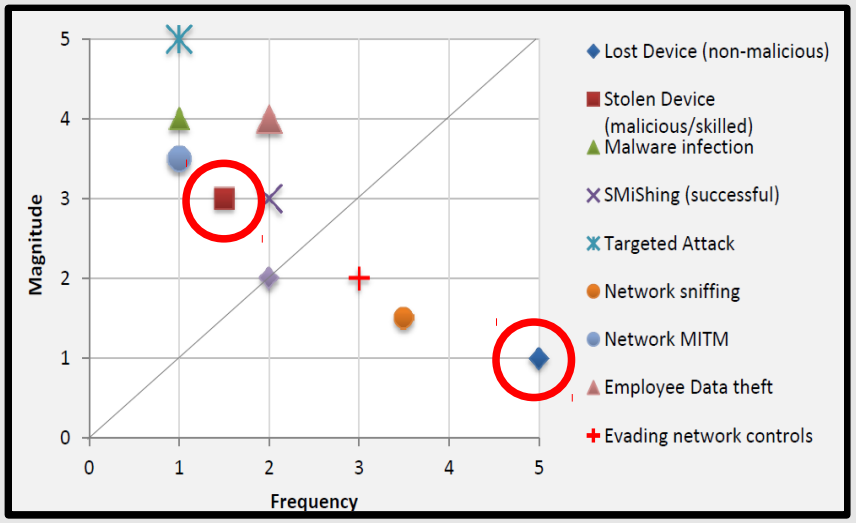
De gros risques de fuites d'informations et d'éléments d'authentification sans que cela soit perçu comme un incident de sécurité par l'usager...et donc signalés.

Une politique BYOD doit permettre d'identifier tous les mobiles (qui se connecte et avec quoi ?) et gérer des autorisations renouvelables pour éliminer les mobiles qui ne sont dans le circuit.

B.Y.O.D : Volatilité des mobiles

Pertes / Vols

- Les mobiles sont **plus exposés** aux pertes ou vols
  - On les amène partout
  - Produits technologiques très recherchés
  - Peu de sécurité et potentiellement beaucoup d'informations (y compris mots de passe...) qui peuvent alimenter un marché de revente.



- Des matériels personnels perdus/volés **sont-ils déclarés ?**
  - Risques de fuites d'informations non répertoriées
  - Pas de blocage des autorisations d'accès.

Une politique BYOD doit mettre en place une procédure d'alerte et de blocage des autorisations

B.Y.O.D : Quelques aspects juridiques

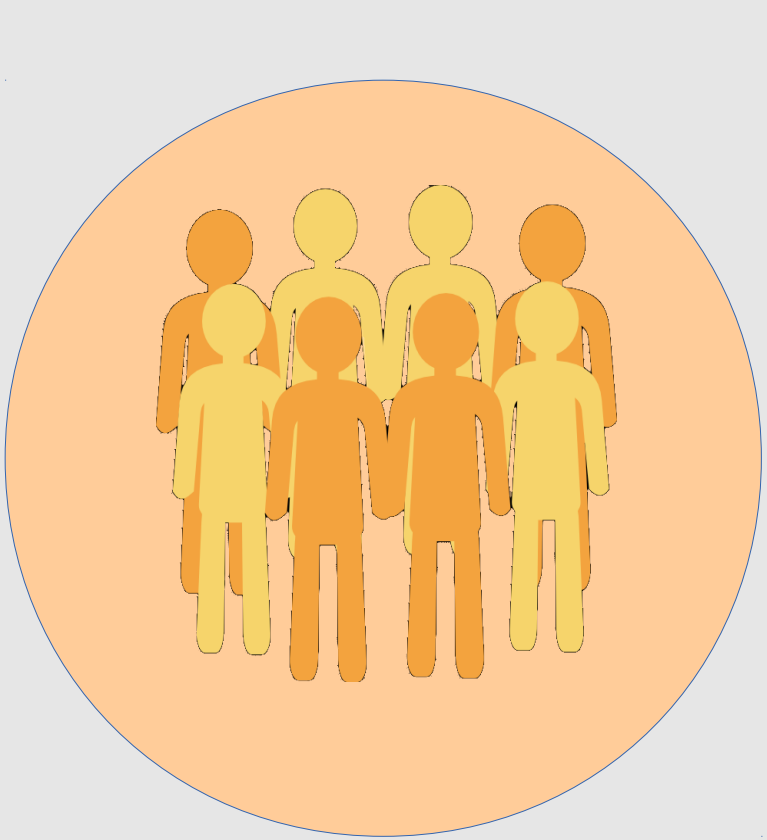
- Que se passe-t-il en cas de « détérioration » du matériel par le personnel de support (casse, dysfonctionnement, suppression accidentelle de données personnelles....) ?

- Comment l'employeur peut récupérer les informations stockées sur une machine portable et personnelle (ou ailleurs dans le cloud) ?

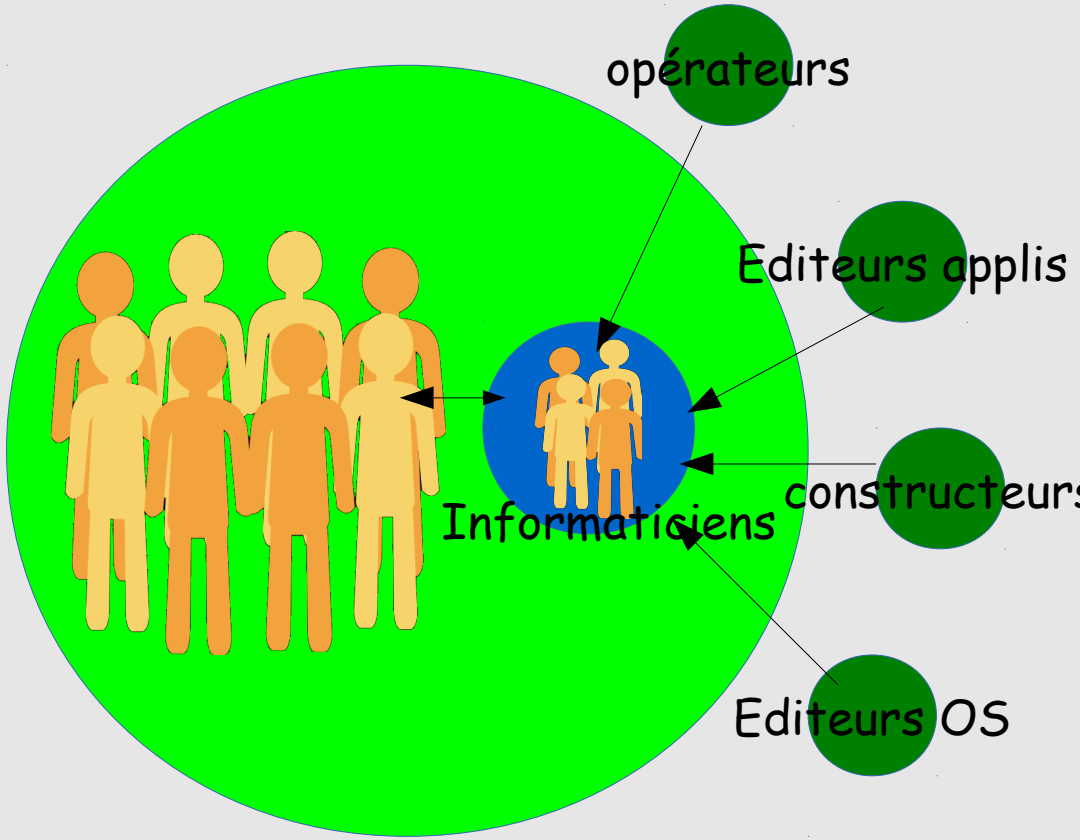
Une politique BYOD doit s'intégrer dans un PSSI qui spécifie les responsabilités

Votre mobile nous intéresse !

Avant le monde était simple....tout passait par les informaticiens



Sphère privée

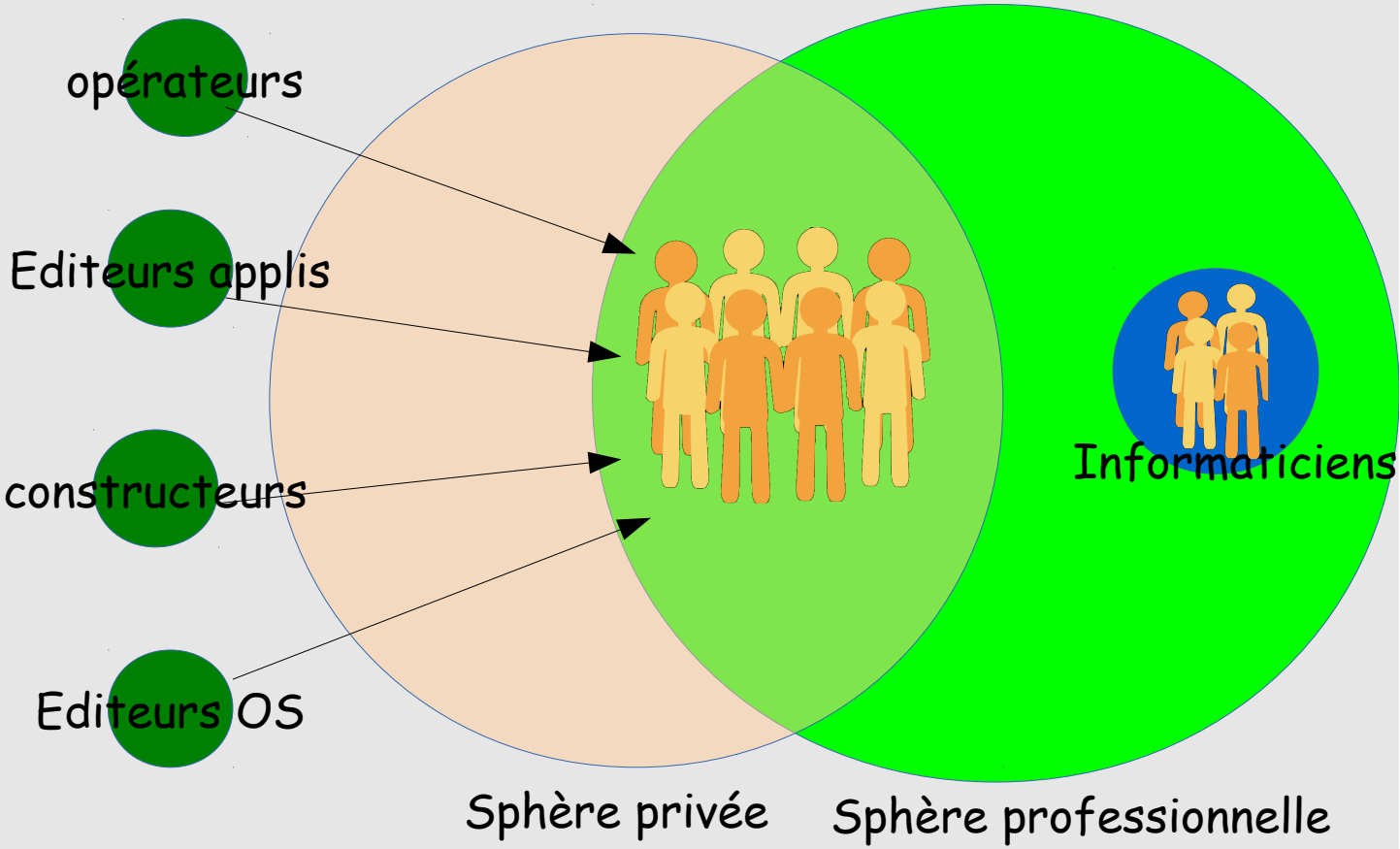


Sphère professionnelle

Votre mobile nous intéresse !

Aujourd'hui,
tous les acteurs s'adressent directement aux utilisateurs

- **Discours**
  - Marketing
  - Économique
  - Technologique
  - Pas du tout sécuritaire !
  - Nous avons des solutions pour votre entreprise
  - Venez, venez dans notre cloud



Principaux dispositifs de sécurité configurable

Verrouillage d'écran

- Le verrouillage d'écran est la protection minimale

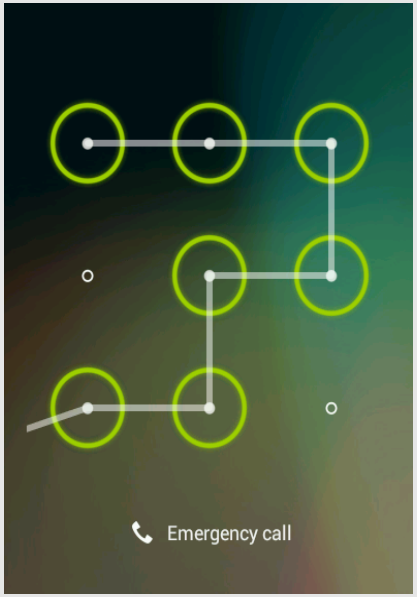
Tout mobile en relation avec le S.I doit verrouiller son écran

- Même si cette protection est considérée comme peu robuste

- Rien à voir avec le pincode de la carte SIM qui protège uniquement l'utilisation de cette carte

Verrouillage d'écran : Par modèle

Consiste à dessiner un motif entre les points contigüs



- La robustesse est proportionnelle à la complexité du motif

- Réputé peu robuste car le nombre de combinaisons est faible :
  - 4 points => 1624 solutions
  - 5 points => 7152 combinaisons
  - 6 points => 26016 combinaisons ==> plus de combinaisons qu'un pincode à 4 chiffres
  - 9 points => 140704 combinaisons
- Attention aux traces de doigts
- Une attaque force brute sur des combinaisons à 9 points révèle aussi les combinaisons de 4 à 8 points.
- Cela nécessite root du mobile, ou mauvais paramétrage (USB debbugging)

0	1	2
3	4	5
6	7	8

En 2012 le FBI n'a pas pu déverrouiller un smartphone verrouillé par un modèle et dû demandé l'aide de Google

Verrouillage d'écran : Par pincode

Verrouillage par une suite de 4 à 16 chiffres

- Robustesse proportionnelle au nombre de chiffres.
- En général 4 chiffres utilisés => 10000 combinaisons seulement
- Attaque force brute par root ou jailbreak, pas directement sur l'écran
- Plusieurs vulnérabilité publiées sous IOS
  (combinaison de touches permettant de contourner simplement le pincode
  http://www.zdnet.com/blog/security/iphone-passcode-lock-bypass-vulnerability-again/7544)

- La méthode pour casser le pin code sous IOS a été publiée
(consiste à booter sur un ramdisk ou jailbreaker)

Affaire Pistorus :
La police Sud-africain n'a pas pu déverrouiller l'iphone 5 d'Oscar Pistorius et a demandé l'aide d'Apple

Verrouillage d'écran : par mot de passe alpha-numérique

Utilisation d'un « vrai » mot de passe alpha-numérique

- Méthode la plus robuste
- Mais la moins pratique
- Difficile de tapez un mot de passe contenant chiffres, lettres, caractères spéciaux sur un smartphone :
  - basculement entre les claviers virtuels (numérique, alpha)
  - gros doigts – petites touches
  - Soleil…

Un intérêt important d'un smartphone est sa capacité multifonction qui nécessite de pouvoir le « dégainer » rapidement (téléphone, photo, gps, accès Internet, ou autre application).
Un mot de passe alpha-numérique est un gros frein qui fait perdre de l'intérêt au smartphone qui découragera les utilisateurs.

Gestion multi-utilisateurs

- Androïd 4.2 introduction de la possibilité de créer plusieurs comptes utilisateurs sur un mobile
- Androïd 4.3 introduction des profiles restreints

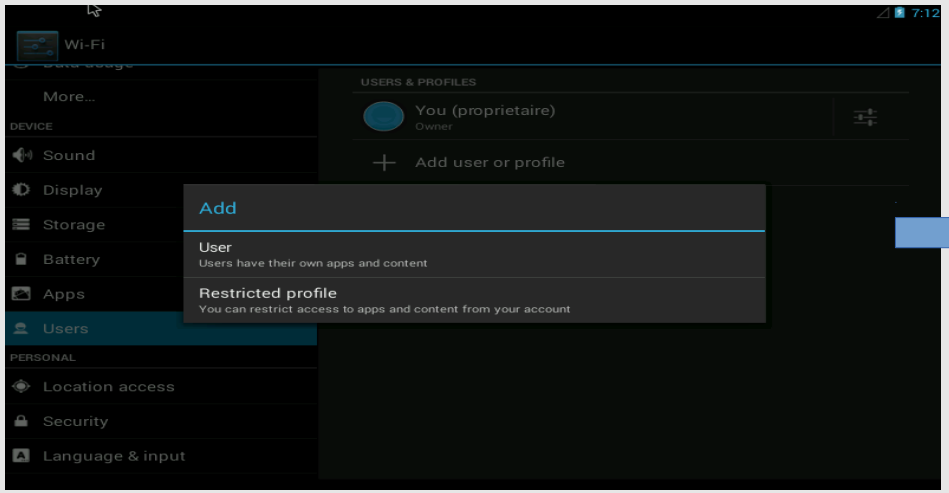
Intérêts

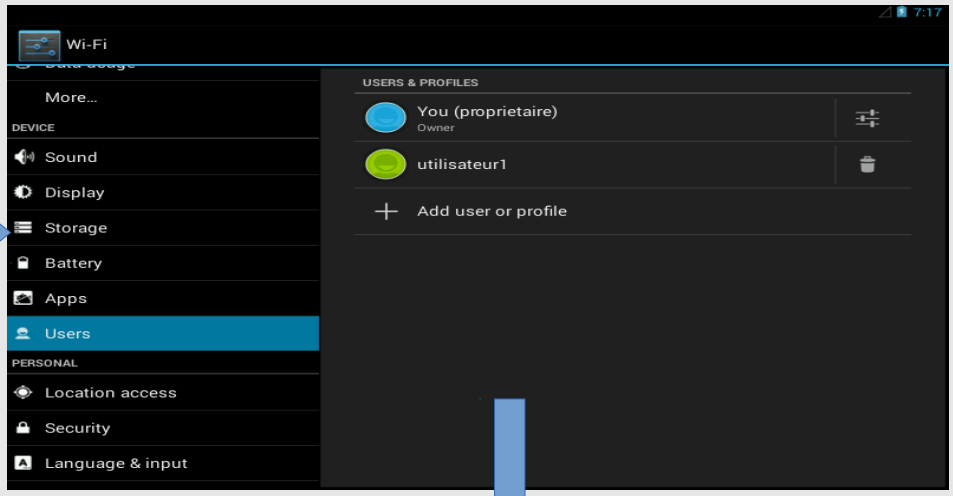
- Au départ : pouvoir partager un mobile (tablette) entre plusieurs personnes en préservant l'environnement de chacun ou pour restreindre les applications.

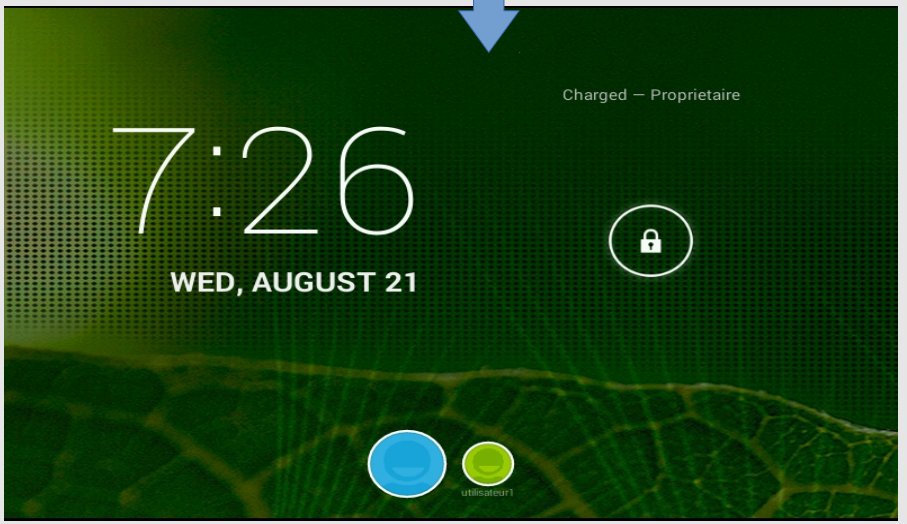
- Intéressant aussi pour séparer l'environnement professionnel du reste.

Gestion multi-utilisateurs

- **Comptes utilisateurs**







- Le compte *utilisateur1* a la possibilité de définir son propre compte Google
- Il voit les applications de base
- Il ne voit pas les applications installées par les autres utilisateurs.
- Il peut installer ses propres applications
- Il peut définir son propre code de verrouillage.
- Etc…

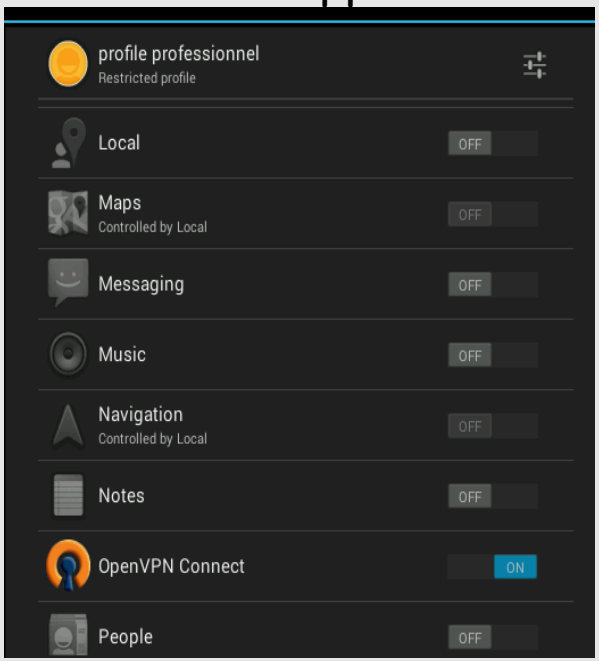
Gestion multi-utilisateurs

- **Profiles restreints**

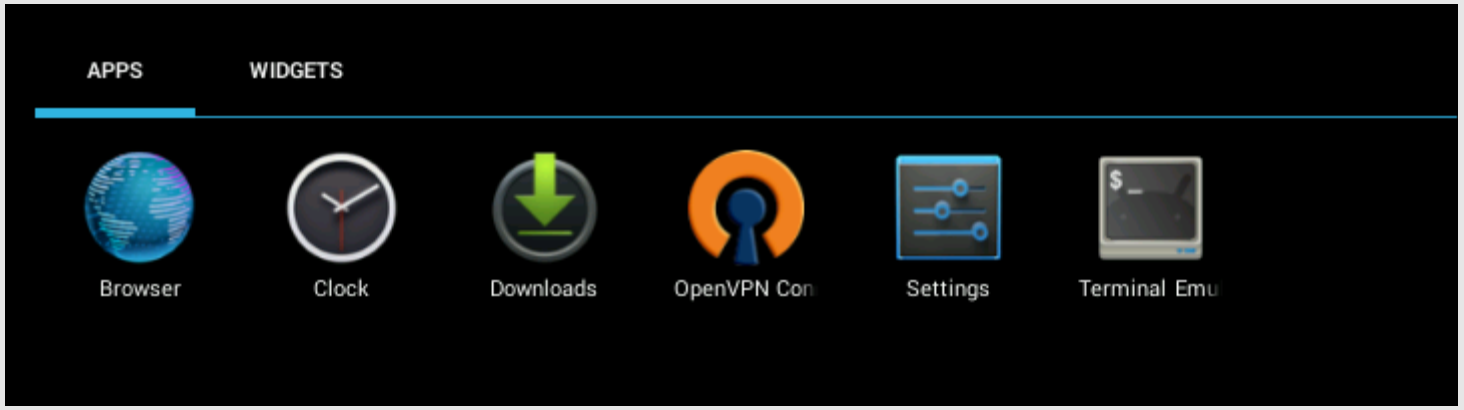
Mêmes caractéristiques que les comptes utilisateurs, avec en plus :

- Le compte du propriétaire doit obligatoirement avoir un code de verrouillage
- Seules les applications sélectionnées sont utilisables par le profile.

Sélection des applications



Applications utilisables depuis le profile



Chiffrement : des principes très différents

- Tous les smartphones et tablettes Apple intègrent un processeur cryptographique AES 256.
- Deux clés de chiffrement : UID spécifique au terminal et GID spécifique à un groupe de processeur.
- Les clés sont gravées dans le processeur et ne peuvent pas en être extraite.

- Depuis IOS 4.0 introduction de l'API Data Protection pour le chiffrement des fichiers.
  - Chaque fichier possède une clé de chiffrement qui lui est propre
  - Le déchiffrement est individuel
  - Chaque fichier peut être placé dans une classe qui détermine quand et comment le fichier est accessible.
  - Chaque application a la responsabilité de la gestion des classes pour ses propres fichiers

Chiffrement : des principes très différents

NSFileProtectionComplete

- Un fichier dans cette classe ne peut être accédé que lorsque le terminal est déverrouillé

NSFileProtectionCompleteUnlessOpen

•Un fichier dans cette classe peut être accédé même quand le terminal est verrouillé

NSFileProtectionCompleteUntilFirstUserAuthentication

•Un fichier dans cette classe est inaccessible pendant le boot et jusqu'au premier déverrouillage par passcode

NSFileProtectionNone

•Le fichier peut être accédé à tout moment.

Chiffrement : des principes très différents

- Le système de chiffrement d'IOS est très évolué et tient compte du fait que les mobiles sont des machines allumées et connectées en permanence

- Le niveau de protection dépend fortement de chaque application

- Dans les faits, peu d'applications utilisent les API Data Protection (le mail d'Apple).

- Le principe est assez déroutant pour l'utilisateur qui ne sait plus comment ses fichiers sont protégés.

- Dépend fortement de la présence d'un passcode et de sa robustesse

- Le processeur cryptographique rend impossible une attaque « offline »

Chiffrement : des principes très différents

- Le chiffrement est déclenché à la demande du propriétaire
- Tout l'espace de données (Répertoire /data et/ou Sdcard) est chiffré (dmcrypt)
- Complètement transparent pour toutes les applications. Tous les fichiers créés par les applications sont donc chiffrés
- Au boot l'utilisateur doit rentrer son passcode (alphanumérique) pour déverrouiller les partitions chiffrées
- Tant que le terminal est allumé, les fichiers sont déchiffrés

Chiffrement : des principes très différents

- Possibilité d'attaque hors du mobile.
- Utilisation de ressources processeur (pas vraiment sensible sur dual, voire quadri, core)
- L'obligation d'un passcode alphanumérique sur un smartphone est plutôt rédhibitoire

Chiffrement : des principes très différents

Avant chiffrement

```
root@android:/ # mount
rootfs / rootfs ro,relatime 0 0
tmpfs /dev tmpfs rw,nosuid,relatime,mode=755 0 0
devpts /dev/pts devpts rw,relatime,mode=600 0 0
proc /proc proc rw,relatime 0 0
sysfs /sys sysfs rw,relatime 0 0
tmpfs /mnt/asec tmpfs rw,relatime,mode=755,gid=1000 0 0
tmpfs /mnt/obb tmpfs rw,relatime,mode=755,gid=1000 0 0
/dev/block/sda6 /system ext4 ro,relatime,data=ordered 0 0
/dev/block/sdb1 /cache ext4 rw,nosuid,nodev,relatime,data=ordered 0 0
/dev/block/sdb3 /data ext4 rw,nosuid,nodev,relatime,data=ordered 0 0
/dev/block/sdc /mnt/sdcard vfat rw,relatime,fmask=0000,dmask=0000,allow_utime=0022,coc
root@android:/ #
```

Après chiffrement

```
rootfs / rootfs ro,relatime 0 0
tmpfs /dev tmpfs rw,nosuid,relatime,mode=755 0 0
devpts /dev/pts devpts rw,relatime,mode=600 0 0
proc /proc proc rw,relatime 0 0
sysfs /sys sysfs rw,relatime 0 0
tmpfs /mnt/asec tmpfs rw,relatime,mode=755,gid=1000 0 0
tmpfs /mnt/obb tmpfs rw,relatime,mode=755,gid=1000 0 0
/dev/block/sda6 /system ext4 ro,relatime,data=ordered 0 0
/dev/block/sdb1 /cache ext4 rw,nosuid,nodev,relatime,data=ordered 0 0
none /mnt/shared/android-extension vboxsf rw,nodev,relatime 0 0
/dev/block/sdc /mnt/sdcard vfat rw,relatime,fmask=0000,dmask=0000,allow_utime=0022,coc
/dev/block/dm-0 /data ext4 rw,nosuid,nodev,relatime,data=ordered 0 0
root@android:/ #
```

Chiffrement : des principes très différents

Plutôt que de mettre des fichiers « sensibles » directement sur un mobile, il est aussi possible de faire ça :

Chiffrement : des principes très différents

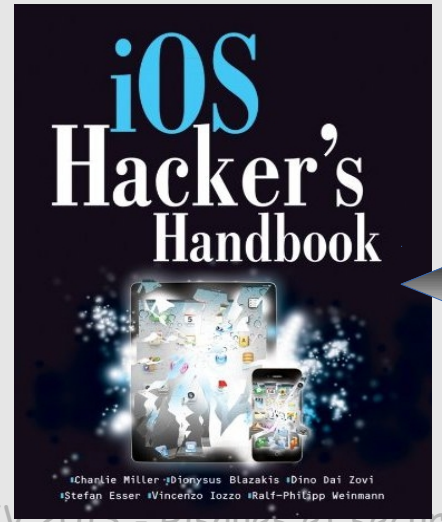
- Diverses Publications font état de faiblesses importantes

Platform	Circumvent Simple Passcode	Circumvent Complex Passcode
Android	Sometimes, device dependent	Sometimes, device dependent
Blackberry	Rarely	Rarely
iOS	Always	Always, however complex passcodes with at least 6 alphanumeric characters can provide protection to some encrypted files

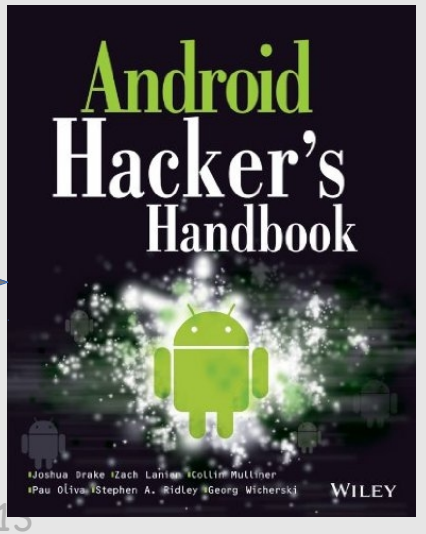
Contournement du passcode

Mobility risk report :Understanding the security impact of IOS and Androïd in the enterprise
https://viaforensics.com/resources/reports/mobile-security-risk-report/

A paraître



Voir aussi



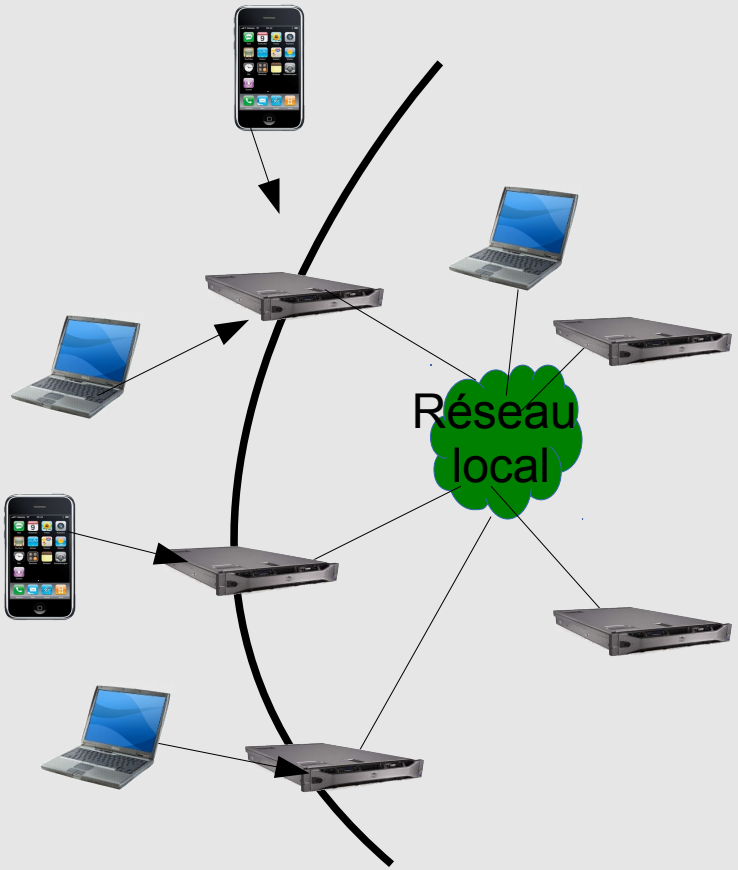
Protection du Système d'Information et de la sphère professionnelle

Traiter la sécurité SUR les mobiles n'est pas suffisant

Les mobiles vecteurs de compromission

- Nous évoluons rapidement d'une situation de rares matériels nomades, **gérés**, vers une situation d'une **multitude** de mobiles, **non gérés**, qui contiendront, **TOUS**, toutes les clés nécessaires pour attaquer le Système d'Information !! (les « credentials »).

- Les réseaux des établissements ont (ou auront) une vitrine de services accessibles depuis Internet … en général avec de simples mot de passe (messagerie, agenda, fichiers...)
  - Parce que le mot de passe ne coûte pas cher
  - Finalement plus pratique/facile pour l'utilisateur

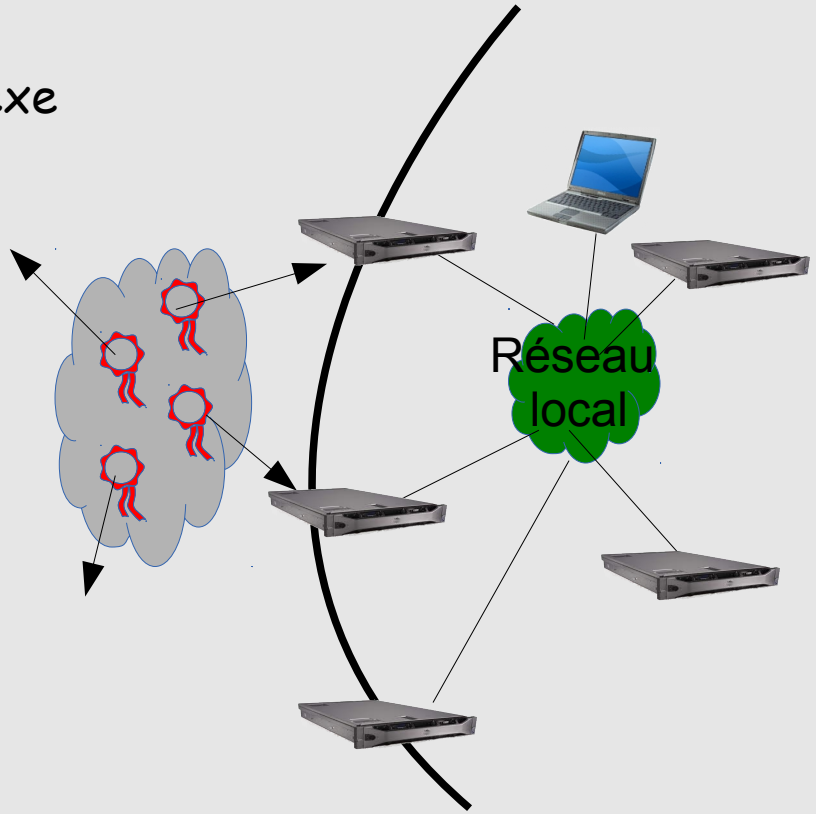


Les mobiles vecteurs de compromission

- L'enregistrement des mots de passe est déjà courant dans les ordinateurs classiques (Navigateur, client de messagerie....)

- L'ergonomie des mobiles impose pratiquement toujours l'enregistrement des mots de passe
  - Trop compliqué de taper un mot de passe complexe
  - Processus qui tournent en arrière-plan.

Les mobiles sont de vraies tirelires à mot de passe et créent un nuage de mots de passe incontrôlable.



Les mobiles vecteurs de compromission

Peut-on interdire toute relation des mobiles avec le système d'information ?

- A partir du moment où il suffit de configurer un login/mot de passe, rien ne peut interdire à un matériel de se connecter (et de stocker le mot de passe)

Exemple: service de messagerie IMAP

- La sécurité liés aux mobiles nécessite aussi de se poser des questions sur les accès au système d'information (reconsidérer la vitrine).
- La relation mobile – S.I doit être encapsulée dans une mode professionnel

Le mode professionnel

C'est quoi ?

- Sur le mobile séparer, et protéger, ce qui est professionnel du reste
- Les services du S.I ne sont accessibles qu'après établissement d'une liaison avec authentification sécurisée

Mode professionnel : Principe du Silo

Consiste à créer sur le mobile un conteneur sécurisé qui protège tous les éléments professionnels, données et credentials.

Divers solutions apparaissent :

- Samsung Knox
- Citrix
- Blackberry balance

- Il s'agit de solutions propriétaires
- Plus adaptées à une gestion de parc mobile d'entreprise
- Doivent fonctionner au moins sur les environnements IOS et Androïd
- Quid du coût ?
- Quid de l'infrastructure côté SI ?

- Manque de maturité et d'expérience des offres
- Pérennité pas évidente

Mode professionnel : Principe du Silo

Le silo est-il efficace ?

- Oui, si les services ne sont accessibles qu'à travers le silo
- Non, s'il reste des services accessibles avec un simple login/mot de passe parce dans ce cas les mobiles n'ont pas besoin du silo pour se connecter aux services (et donc stocke les mots de passe de façon non-sécurisée)

Un exemple de mise en place d'une méthode pour permettre l'accès sécurisé au mail depuis Internet. (ou d'autres applications)

- **Contexte préexistant**

Le service de messagerie (IMAP) n'est accessible qu'au travers d'une connexion VPN (IMAP pas ouvert directement sur l'extérieur)

- **Problème à résoudre**

  - Fournir le même accès à la messagerie aux mobiles sans affaiblir la sécurité déjà existante
  - Quel que soit le client de messagerie
  - Androïd ou IOS
  - 0 €

1) Configuration du mobile

- Un certificat est enregistré dans le mobile. Ce certificat est unique (même si le propriétaire a plusieurs mobiles) installé par le service informatique (même BYOD)
- Le mobile est enregistré dans les tables d'administration avec un pin code fourni par l'utilisateur.
- L'application Androïd ou IOS Openvpn Connect est installée et configurée par le service informatique

2) Connexion VPN

- L'utilisateur se connecte avec Openvpn.
  Il y a une authentification à deux facteurs sur le serveur Openvpn
  - Avec le certificat enregistré précédemment
  - Avec un mot de passe tapé par l'utilisateur (validé par le serveur, et pas sur le mobile)

  Ce mot de passe est constitué d'une partie variable et du pin code de l'utilisateur. Pour la partie variable il tape n'importe quoi, qui doit être différent de la fois précédente. Le serveur vérifie que la partie variable a bien variée. Cela empêche l'utilisateur d'enregistrer le mot de passe.

3) Configuration du client de messagerie

- Ouverture de la connexion VPN.
- Passage dans les paramétrages du client mail
- Dans le champ mot de passe l'utilisateur tape n'importe quoi au hasard sur son clavier
  Ce qu'il a tapé devient son mot de passe (**token**) pour ce mobile et cette application.
- Il n'a pas besoin de le connaître (puisque enregistré)
- Le mot de passe n'est utilisable que lorsque la connexion VPN est ouverte.
- Si l'utilisateur a un autre mobile, il reçoit sur ce mobile un autre certificat. Il utilise le même pincode.
- Il configure le client mail de la même manière et il a donc un autre token

- S'il veut réinstaller son client messagerie :
  - Il se connecte sur le VPN
  - Re-configure son client de messagerie en indiquant une chaîne convenue pour reseter le token (par exemple $$)
  - Une fois resetté il recommence la configuration en tapant un nouveau token

Moyens utilisés

- Ré-utilisation du dispositif déjà existant
  - un serveur VPN
  - un serveur Radius
  - Une IGC local
- Modification d'une ligne dans la configuration PAM du serveur de mail
- Une quinzaine de ligne en BASH dans le serveur Openvpn (vérification de la partie variable)
- Une trentaine de ligne de BASH dans le serveur Radius (enregistrement des tokens)

Avantages

- Ne dépend pas de l'application cliente
- Applicable pour d'autres applications

- Connaissance du parc de mobiles
  - Expiration de l'autorisation annuelle (l'utilisateur doit reconfirmer)
  - Expiration des certificats : un mobile qui n'est plus utilisé perd la validité de son certificat.
- On sait qui se connecte, mais aussi avec quoi.

Conclusion

Dans le passé on n'a pas toujours bien imaginé quels usages on ferait des nouvelles technologies

Exemple : le chiffrement
D'abord utilisé à des fins militaire, aujourd'hui utilisé pour télécharger illégalement ou par les terroristes.

Alors....

Que ferons-nous avec nos smartphones et nos tablettes demain ? Dans quoi iront se nicher Androïd ou IOS ? (montres, lunettes, fer à repasser... ?)

Nous verrons probablement apparaître des mobiles partout dans l'environnement scientifique, pour des usages que nous n'imaginons même pas encore .