www.cnrs.fr

Sécurité des mobiles et de leur environnement

SARI Grenoble 13/12/2013

François Morris

Livre blanc
Défense et sécurité nationale

- **Publié 29/04/2013, précédent 2008**
- ***Les cyberattaques, parce qu'elles n'ont pas, jusqu'à présent, causé la mort d'hommes, n'ont pas dans l'opinion l'impact d'actes terroristes. Cependant […] elles constituent une menace majeure, à forte probabilité et à fort impact potentiel.***
- ***La sécurité de l'ensemble de la société de l'information nécessite que chacun soit sensibilisé aux risques et aux menaces et adapte en conséquence ses comportements et ses pratiques. Il importe également d'accroître le volume d'experts formés en France.***

NSA, Prism, Edward Snowden

- **Feuilleton**
  - Chaque jour on découvre un nouveau programme
  - La NSA sait-elle ce qui a effectivement fuit ?
- **Portée des révélations**
  - Officialise ce qui était connu ou au moins suspecté par les spécialistes
  - L'étendue de l'espionnage dépasse tout ce que l'on imaginait
  - Amène a réévaluer des faits antérieurs
  - Biais dans la nature des documents révélés (formations, marketing interne)
- **Que peut-on faire ?**
  - Prudence vis-à-vis de l'externalisation, du cloud, etc.
  - Sécuriser, maintenir à jour, surveiller, chiffrer
    - Statistiques montrent qu'ils récupèrent moins lorsque c'est chiffré
    - Appréciation des risques pour cibler l'attaque

Plan

- ❑ Cryptographie
- ❑ Vie privée
- ❑ Menaces, vulnérabilités, exploits, risques
- ❑ Modèle de sécurité
- ❑ Ecosystème & sécurité
- ❑ Outils de sécurité
- ❑ Perspectives

Plan

- ❑ **Cryptographie**
- ❑ Vie privée
- ❑ Menaces, vulnérabilités, exploits, risques
- ❑ Modèle de sécurité
- ❑ Ecosystème & sécurité
- ❑ Outils de sécurité
- ❑ Perspectives

Cryptographie

- **Pourquoi s'attarder sur la cryptographie ?**
  - Base de nombreux mécanismes de sécurité
    - Disponibilité, **intégrité, confidentialité, traçabilité**
  - Mise en œuvre délicate sujette à des erreurs
    - Le diable est dans les détails
  - Fournir des conseils aux développeurs
- **Vocabulaire**
  - Chiffrer/déchiffrer
  - Décrypter
  - ~~Crypter~~

Chiffrement symétrique

- **C = f(k, M) où M message, k clé, C chiffré**
- **$M = f^{-1}(k, C)$**
- **Chiffre de Vernam (masque jetable)**
  - Longueur de la clé = celle du message
  - Clé **aléatoire** et ne devant **jamais être réutilisée**
  - Sécurité absolue (Shannon)
  - XOR
  - En pratique inutilisable

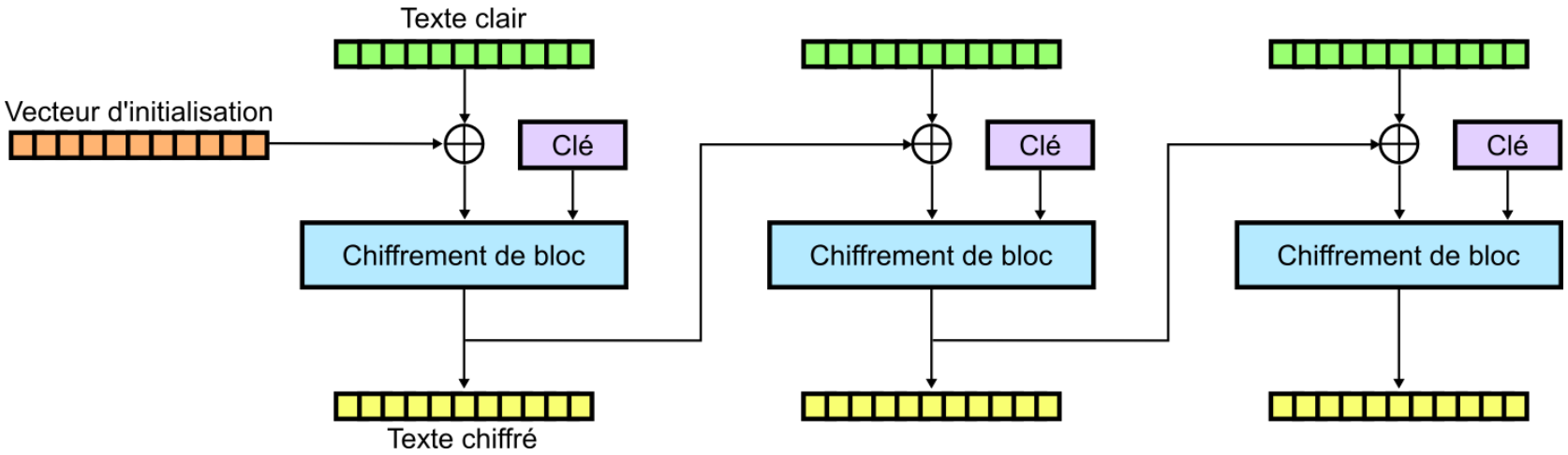
Chiffrement symétrique par flot

- Générateur pseudo-aléatoire public
- Clé k secrète partagée entre Alice et Bob
- Alice choisi un IV (*initialisation vector*) aléatoire
- Alice initialise le générateur pseudo-aléatoire avec une combinaison de IV et k
- Alice chiffre son message en utilisant la méthode de Vernam avec la suite produite par le générateur
- Alice envoie à Bob le chiffré et IV
- Bob déchiffre
- Exemple
  - RC4
    - Cassé en temps réel par la NSA ?

Chiffrement symétrique par bloc

- Blocs de taille fixe (128 bits pour AES)
- Mode de chiffrement (ECB, CBC, GCM, CTR, etc.)

CBC



Cryptographie asymétrique

- **Couple clé publique / clé privée**
  - Seule la clé privée est à protéger
  - Difficile de déduire la clé privée de la clé publique
- **Opérations mathématiques complexes et longues ➔ données de taille réduite**
  - Clé symétrique de chiffrement
  - Condensat (hachage) pour la signature notamment
- **Algorithmes**
  - DSA
  - RSA
  - Courbes elliptiques (fort intérêt, clés plus courtes)

Cryptographie asymétrique

❑ Chiffrement

- ➢ $C = f(k_{pub}, M)$ où M message, k_{pub} clé publique, C chiffré
- ➢ $M = f^{-1}(k_{priv}, C)$ où k_{priv} clé privée

❑ Signature

- ➢ $S = f(k_{priv}, M)$ où M message, k_{priv} clé privée
- ➢ $M = f^{-1}(k_{pub}, S)$ où k_{pub} clé publique

Fonctions de hachages

- **H = f(M)**
  - M message de taille arbitraire
  - H haché de taille fixe
- **Difficile de trouver**
  - 2 messages ayant même haché (collision)
  - 1 message ayant même haché qu'un message connu (seconde préimage)
  - 1 message ayant un haché donné (première préimage)
- **Fonctions**
  - ~~MD5~~ : cassé
  - SHA-1 : fragile, faute de mieux
  - **SHA-2** : OK (256, 384, 512)
  - SHA-3 (Keccak) : futur

Nombre aléatoires

- **Interviennent partout en cryptographie**
  - Clés de chiffrement
  - Vecteurs d'initialisation
  - Diversifiants (salt)
  - Nonces
- **Critiques**
  - Si prévisible réduit l'entropie et donc l'espace à explorer
  - Difficile à produire sur une machine déterministe
- **Faiblesses**
  - Debian
  - Courbes elliptiques et NSA
  - Matériel Intel ?

Certificats

- **IGC**
- **X509**
  - Clé publique
  - Nom du détenteur + diverses information
  - Nom de l'autorité de certification
  - Usage du certificat (authentification, chiffrement, signature)
  - Signature par l'autorité de certification
- **Chaîne de confiance remontant à la racine**

Cryptographie matérielle

- **Dispositifs**
  - Carte bancaire
  - SIM
  - HSM (*Hardware Security Module*)
  - TPM (Trusted Platform Module)
  - Processeur cryptographique Apple
- **Eléments intégrés**
  - Stockage sécurisé de clés (impossible de les extraire)
  - Chiffrement symétrique et/ou asymétrique
  - Générateur de nombres aléatoires
  - Hachage
  - Protection par un code PIN

Signature du code

- **Fournisseur**
  - Calcule un haché du code
  - Le signe avec sa clé **privée**
- **Chargeur (BIOS, OS, JVM…)**
  - Vérifie qu'il a bien le certificat du fournisseur dans sa liste de confiance
  - Déchiffre le haché avec la clé publique
  - Calcule le haché du code
  - Compare les 2 hachés
  - Charge si accord

Echec : GSM A5/1 & A5/2

- **Algorithme non publié**
  - Non respect du principe de Kerkhoffs
    - Algorithme public, clé secrète
  - Publié en 1999 après rétroconception (*reverse engineering*)
- **Mauvais algorithme**
  - 10 bits de la clé mis à 0 ➔ 54 bits au lieu de 64
  - Résiste mal à la cryptanalyse
- **Développé par des gens du monde de la téléphonie sans consulter les spécialistes de la cryptographie**

Echec : WEP

- **Chiffrement par flot RC4, clé de 64 bits**
  - clé WEP : 40 bits
  - IV (initialisation vector) : 24 bits
- **Faiblesses**
  - Implémentation de RC4 et gestion des clés
  - IV
- **Se casse en quelques secondes**
- **WEP = Wired Equivalent Privacy**
  - Objectif non atteint et trop modeste
  - Mauvaise implémentation de la cryptographie

Echec : gestionnaire de mots de passe

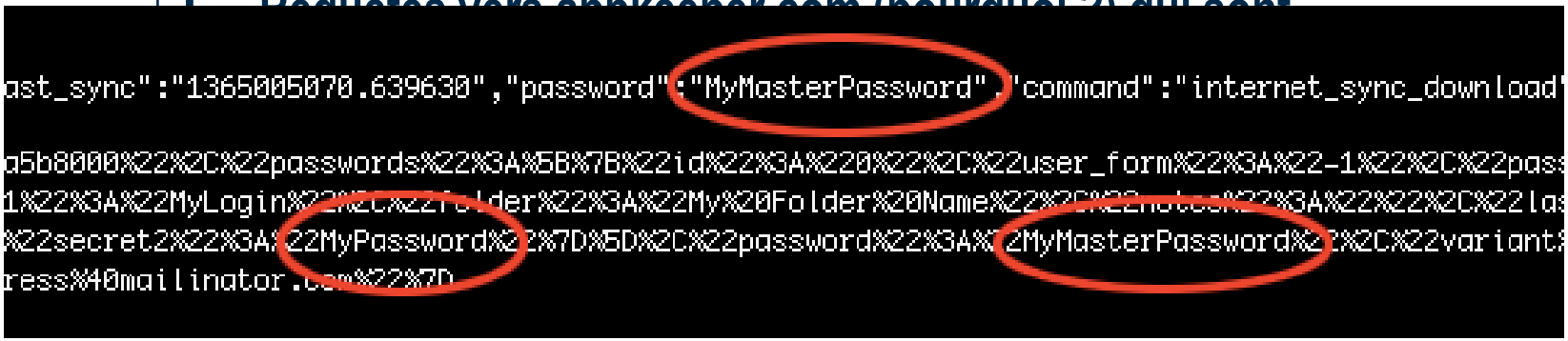
Table 1. Summary of our findings.

App name	Encrypts data?	Uses keychain?	Password verification complexity
Keeper® Password & Data Vault	Yes	No	1x MD5
	Remarks: Rainbow Tables and GPU crackers may be used		
Password Safe - iPassSafe free version	Yes	No	1x AES-256
My Eyes Only™ - Secure Password Manager	Yes	Yes	N/A (see Remarks)
	Remarks: Master password and user passwords can be decrypted due to misuse of public-key crypto		
Strip Lite - Password Manager	Yes	No	4000x PBKDF2-SHA1 + 1x AES-256
Safe - Password Awesome Password Lite Password Lock Lite	No	No	N/A (see Remarks)
	Remarks: Master password and user passwords are stored unencrypted		
iSecure Lite - Password Manager	No	No	N/A (see Remarks)
	Remarks: Master password and user passwords are stored unencrypted		
Ultimate Password Manager Free	No	No	N/A (see Remarks)
	Remarks: Master password and user passwords are stored unencrypted		
Secret Folder Lite	No	No	N/A (see Remarks)
	Remarks: Master password and user passwords are stored unencrypted		
SafeWallet - Password Manager	Yes	No	10x PBKDF2-SHA1 + 1x AES-256
SplashID Safe for iPhone	Yes	No	N/A (see Remarks)
	Remarks: Hard-coded key is used to encrypt master password		

Echec : Keeper Password for iOS

- FoxIt : Unencrypted storage of confidential information in Keeper® Password & Data Vault v5.3 for iOS

- Requêtes vers appkeeper.com (pourquoi ?) qui sont



Echec : gestionnaires de mots de passe

- **Quel est le but des fournisseurs ?**
  - Faciliter l'usage d'Internet en évitant d'avoir à mémoriser et saisir des mots de passe
  - La sécurité n'est pas au cœur du produit, un vague discours commercial suffit
    - « Sécurité militaire »
  - Parfois carrément malveillant
- **Utiliser des solutions éprouvées**
  - Keychain

Echec : Samsung /dev/exynos-mem

- **/dev/exynos-mem**
  - *Device* permettant d'accéder à la mémoire
    - *Kernel direct-mapped RAM region. This maps the platforms RAM, and typically maps all platform RAM in a 1:1 relationship*.
  - Utilisé pour gérer une caméra
  - Lecture & écriture pour tous
- **Exploit**
  - Trivial
  - Permet de tout faire
- **Il faut tout réapprendre à chaque nouvelle technologie**
  - /dev/mem sous Linux

Echec : sécurisation des échanges

- **TLS, SSL, HTTPS**
  - Protocoles sûrs si bien utilisés
- **Failles dans les applications**
  - Non utilisation
  - Non vérification du certificat du serveur
    - Délivré par une AC reconnue
    - Date de validité
    - Liste de révocation
- **Les études ont montré une forte proportion d'applications qui n'implémentent pas ou mal TLS**
  - Vérifications supprimées pour le développement
  - API complexes d'où des erreurs

Conseils pour la cryptographie

- **Ne pas faire preuve d'imagination ou de créativité**
- **Utiliser des algorithmes connus et éprouvés**
- **Utiliser des implémentations (bibliothèques) connues et éprouvées**
  - Bien lire la documentation
  - Les appels sont souvent non triviaux et les erreurs faciles
  - Utiliser les outils du système : keychain

Conseils pour la cryptographie

- **Respecter les préconisation de l'ANSSI (RGS)**
  - Chiffrement symétrique
    - AES 128 bits (ou plus)
  - Chiffrement asymétrique
    - RSA 2048 (<2020), 4096 (>2020)
    - ECDSA (courbes elliptiques P-256, P-384, P-521, B-283, B-409 ou B-571)
      - NSA ?
  - Hachage
    - SHA-256

Plan

- ❑ Cryptographie
- ❑ **Vie privée**
- ❑ Menaces, vulnérabilités, exploits, risques
- ❑ Modèle de sécurité
- ❑ Ecosystème & sécurité
- ❑ Outils de sécurité
- ❑ Perspectives

Privacy by design

- **Ann Cavoukian au Canada (années 1990)**
  - prendre des mesures proactives et non réactives ; des mesures préventives et non correctives
  - assurer la protection implicite de la vie privée
  - intégrer la protection de la vie privée dans la conception des systèmes et des pratiques
  - assurer une fonctionnalité intégrale selon un paradigme à somme positive et non à somme nulle
  - assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements
  - assurer la visibilité et la transparence
  - respecter la vie privée des utilisateurs.
- **Repris dans le projet de règlement européen**
- **Privacy by default (Viviane Reding)**

Recommandations G29 pour les applications mobiles

- **G29 = CNIL européennes**
- **Limitation des données traitées**
  - *Privacy by design* ➔ seules les informations nécessaires doivent être recueillies
- **Transparence à l'égard des utilisateurs**
  - Informer sur les données traitées et les finalités
- **Maîtrise des informations par les utilisateurs**
  - Consentement exprès préalable
- **Attention particulière réservée à certaines informations**
  - Sensibles, permettant d'établir le profil social de la personne

Mobilitics

❑ Expérimentation *in vivo* CNIL + INRIA

Nombre d'applications utilisées durant l'expérimentation :	Total : 189	
•Qui accèdent au réseau	**176**	93%
•Qui accèdent à l'UDID (identifiant unique Apple)	**87**	46%
•Qui accèdent à la géolocalisation	**58**	31%
•Qui accèdent au nom de l'appareil	**30**	16%
•Qui accèdent à des comptes	19	10%
•Qui accèdent au carnet d'adresses	15	8%
•Qui accèdent au compte Apple	4	2%
•Qui accèdent au calendrier	3	2%

Autorisations indues

- **Services payants**
  - appeler directement des numéros de téléphone
- **Contrôles du matériel**
  - prendre des photos et filmer des vidéos
- **Votre position**
  - position approximative (réseau)
  - position précise (GPS et réseau)
- **Communications réseau**
  - bénéficier d'un accès complet au réseau
- **Appels téléphoniques**
  - voir l'état et l'identité du téléphone

Qui est-ce ?


SNCF Transilien
SNCF
SNCF
TRANSILIEN
★★★★★(1 438)
INSTALLER
Autres articles du même développeur
SNCF DIRECT
PRÉSENTATION
AVIS DES UTILISATEURS
NOUVEAUTÉS
AUTORISATIONS
Description
Téléchargez gratuitement l'application officielle de SNCF Transilien pour tous vos déplacements en
Ile-de-France et restez informés en temps réel des horaires et des conditions de trafic sur votre
ligne Transilien !
* Nouveautés de la v2 : nouveau design et nouvelles fonctionnalités de la rubrique « Itinérair
» !

Autorisations indues (2)

- **Communications réseau**
  - bénéficier d'un accès complet au réseau
- **Appels téléphoniques**
  - voir l'état et l'identité du téléphone
- **Stockage**
  - **modifier ou supprimer le contenu de la mémoire de stockage USB, modifier ou supprimer le contenu de la carte SD**
- **Outils système**
  - empêcher la tablette de passer en mode veille, empêcher le téléphone de passer en mode veille
  - **modifier les paramètres du système**
- **Contrôles du matériel**
  - contrôler le vibreur
- **Communications réseau**
  - recevoir des données depuis Internet
- **Par défaut**
  - tester l'accès au stockage protégé

Qui est-ce ?

Wikiradio CNRS

Saooti

★★★★★(1)

INSTALLER

Autres articles du même développeur

Radio Médecine Douce

SAOOTI

★★★½☆ (10)

Gratuit

PRÉSENTATION | AVIS DES UTILISATEURS | NOUVEAUTÉS | AUTORISATIONS

Description

Le Centre National de la Recherche Scientifique (CNRS) regroupe près de 34 000 personnes, chercheurs, ingénieurs et techniciens. Ses laboratoires, implantés dans les universités, travaillent dans tous les domaines scientifiques et produisent des résultats qui font reculer chaque jour un peu plus les frontières de la connaissance. Avec la wikiradio CNRS, vivez la recherche en direct et au contact des chercheurs !

Accéder au site Web du développeur › Envoyer un e-mail au développeur ›

Captures d'écran de l'application

Dom's laptop is in Iran

- **Dom se fait voler son iPad**
- **App Hidden**
  - Activation cloud
  - Localise le matériel
  - Prends des photos
- **Dom est informé que son iPad est en Iran**
  - Il publie sur son blog des informations sur la vie privée du nouveau possesseur (photos)
  - Acheté en tout bonne foi
  - S'excuse et demande de garder
- **Limites morales et légales à ne pas franchir**

Téléphone outil d'espionnage

- **Depuis le début du GSM un téléphone peut être utilisé pour espionner**
  - Activation à distance du micro pour écouter une réunion
- **Smartphone multiplie les possibilités**
  - Caméra
  - Plus d'informations à espionner : voix + données
  - Point d'accès au SI de l'organisation
  - Installation d'application furtives
    - Disponibles largement sur Internet
- **Article 226-3 du code pénal**
  - 5 ans d'emprisonnement et 300 0000€ d'amende pour la détention, vente, fabrication de certains dispositifs de captation de données à l'insu des personnes concernées
- **Outils disponibles facilement**
  - Internet
  - Prétexte un usage « légitime »

Traçage par le Wi-FI (1/2)

- **Trames 802.11**
  - Radio, tout le monde peut écouter
  - En-têtes non chiffrées
  - MAC émetteur → identifiant unique
- **Economie d'énergie**
  - Bascules fréquente de l'interface actif/inactif ➔ réassociations fréquentes
  - Mode passif
    - Beacon émis par le point d'accès
    - Coûteux pour le terminal
  - Mode actif
    - Terminal envoie liste des SSID auquel il s'est déjà connecté
      - Evolution, liste vide, n'est pas encore implémenté par tous les terminaux
    - Réponse immédiate du point d'accès → moindre consommation pour le terminal

Traçage par le Wi-FI (2/2)

- **Localisation d'un terminal**
  - Mesure du signal reçu → distance
  - 3 récepteurs pour déterminer la position
  - Précision de l'ordre du mètre
- **Comment implémenter**
  - Bornes spécifiques
    - Bornes Wi-FI adaptées
    - Raspberry PI ou analogues
  - Firmware adapté sur les points d'accès
- **Utilisations**
  - Suivi des clients dans les rayons d'un magasin
- **Adresse MAC = donnée à caractère personnel**
  - MAC → smartphone → individu
  - Applications qui récupère et envoie l'adresse MAC
  - Corrélations permettent de remonter à l'individu
    - Paiement
    - Et au sexe (toilettes)
    - Domicile + travail + … → lève l'ambigüité

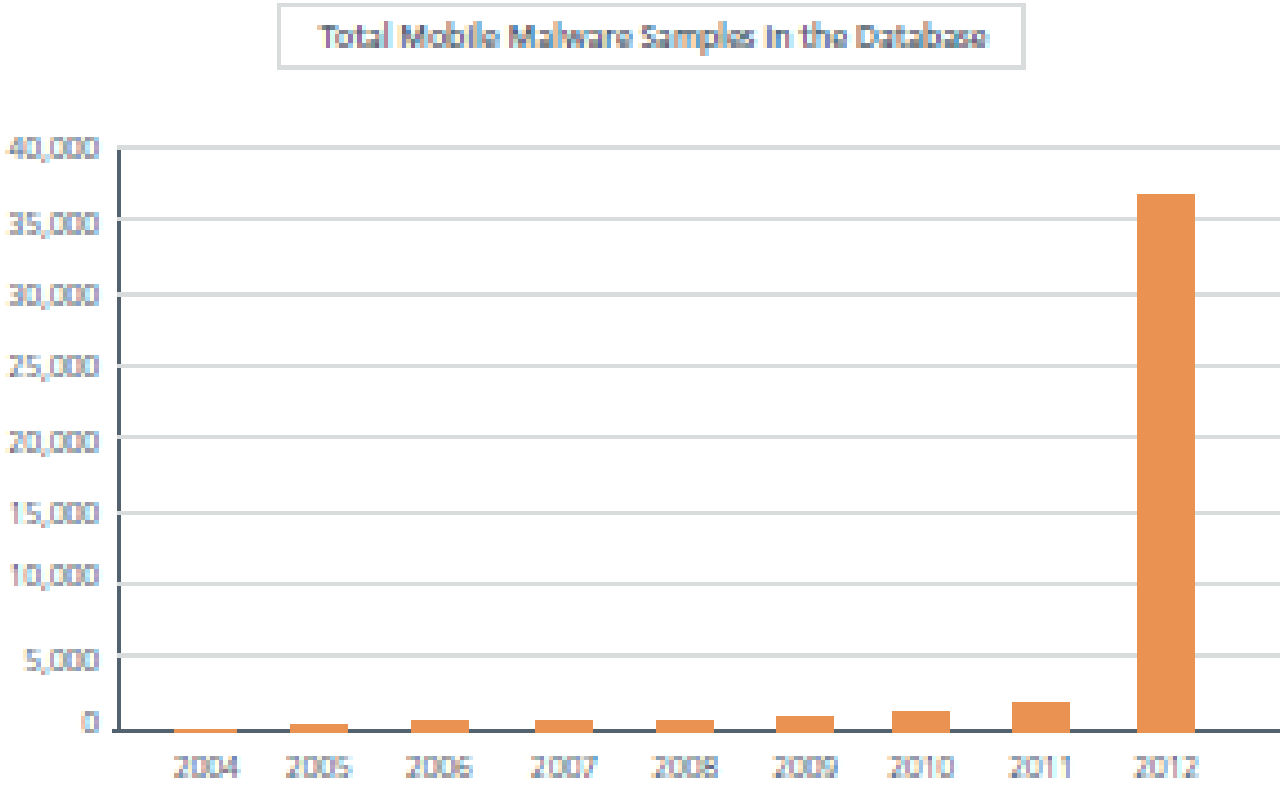
Respect de la vie privée

- **Le vrai enjeu**
- **Comprendre l'économie**
  - Si c'est gratuit ou très peu cher c'est que les acteurs se rémunère par les informations qu'ils recueillent
- **Faisons en sorte de la respecter dans les développements**
- **Réglementation**
  - Informations à caractère personnel
  - Données de santé
- **Sciences humaines et sociales**

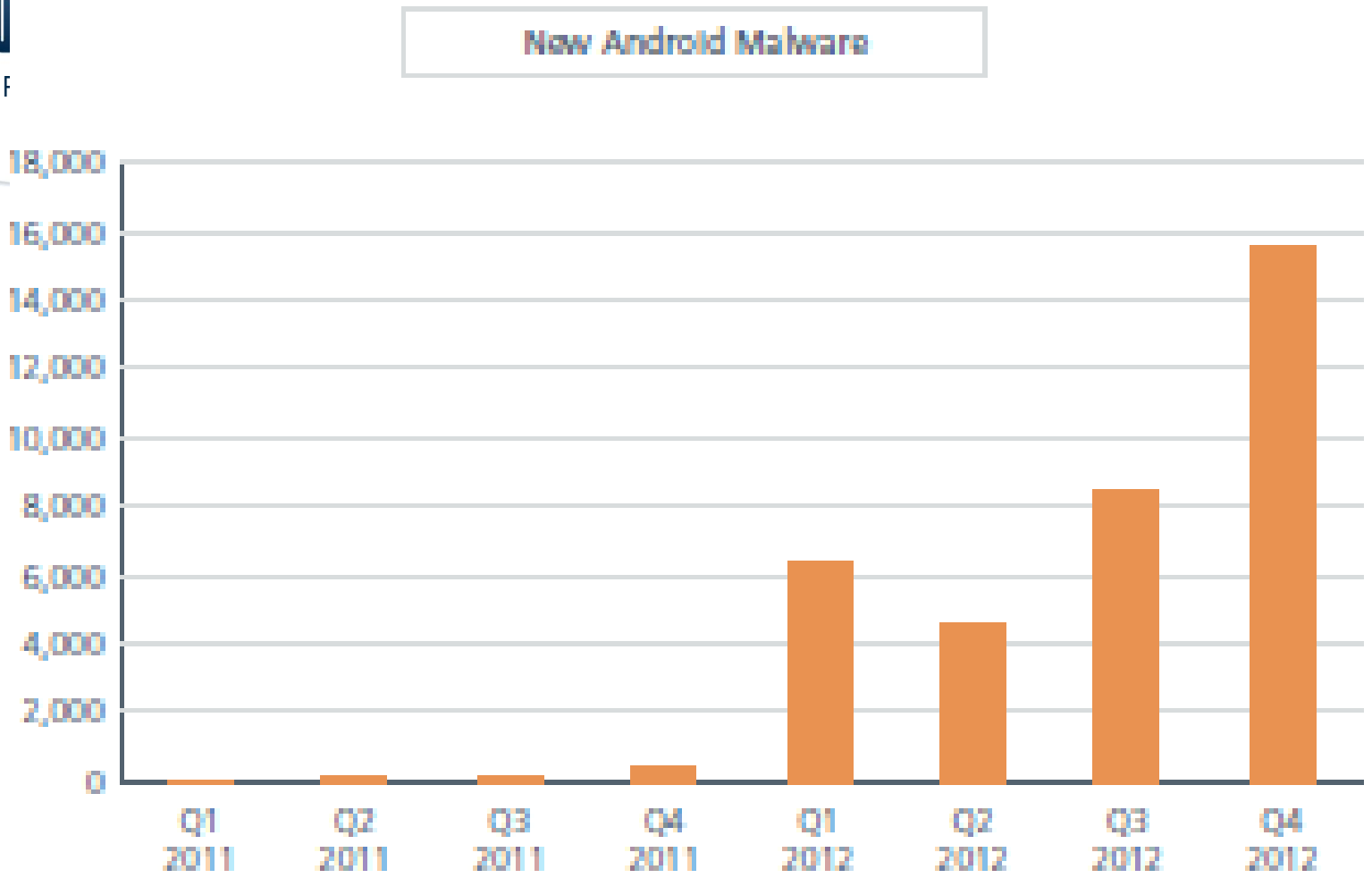
Plan

- ❑ Cryptographie
- ❑ Vie privée
- ❑ **Menaces, vulnérabilités, exploits, risques**
- ❑ Modèle de sécurité
- ❑ Ecosystème & sécurité
- ❑ Outils de sécurité
- ❑ Perspectives

McAfee Threats Report



McAfee Threats Report



Samsung

- **Support URI « tel: » (ex. tel:0123456789)**
  - Clique sur le lien puis sur « appel »
- **USSD (Unstuctured Supplementary Service Data)**
  - *#06# → code IMEI (International Mobile Equipment Identity)
  - **04*0000*1111*1111# PIN 0000 → 1111
  - *2767*3855#
    - réinitialisation paramètres usine (Samsung)
    - aucune intervention utilisateur (pas de validation)
- **<frameset><frame src="%2306%23"/></frameset>**
  - Affiche IMEI
  - **L'attaque qui tue : code de réinitialisation**

Carrier IQ

- Collecte des informations sur l'appareil et les différentes actions de l'utilisateur
- Les envoie pour « améliorer l'expérience de l'utilisateur »
- Installé par différents opérateurs au USA
- De fait c'est un *rootkit*

Attaque de l'entremetteur

- **Principe (*Man in the middle*)**
  - Alice souhaite établir une communication avec Bob
  - Charlie intercepte cette demande et la transmet à Bob en se faisant passer pour Alice
  - Bob croyant répondre à Alice répond à Charlie
  - Charlie transfère la réponse à Alice
- **Impacts**
  - Confidentialité : Charlie voit tous les échanges
  - Intégrité : Charlie peut modifier à sa guise les échanges
- **Protections**
  - Chiffrement ne suffit pas, Charlie déchiffre et rechiffre
  - Authentification : Bob prouve moi que tu es bien Bob
  - Authentification mutuelle
- **Liaison sans fil, sans contact**
  - Interception facile
  - NFC

Plan

- ❑ Cryptographie
- ❑ Vie privée
- ❑ Menaces, vulnérabilités, exploits, risques
- ❑ **Modèle de sécurité**
- ❑ Ecosystème & sécurité
- ❑ Outils de sécurité
- ❑ Perspectives

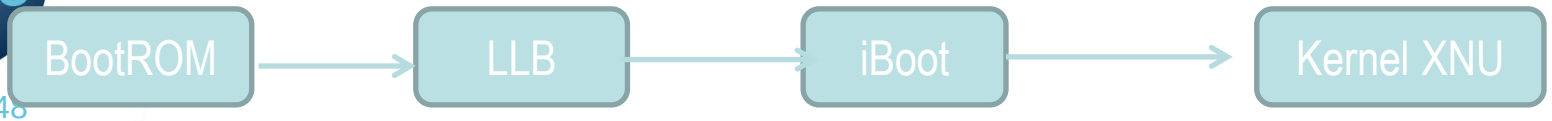
Baseband

- **Puce gérant la communication radio avec l'opérateur téléphonique**
  - Processeur
  - Système + logiciels
  - DSP
  - Fermé (milieu de la téléphonie)
- **C'est lui qui est démarré en premier**
  - Premières étapes du boot
  - Lance le processeur et le système (iOS, Android…)
- **Sécurité**
  - Problématique occultée
  - 2 mondes : téléphonie, informatique

Démarrage sécurisé

- ***Secure boot, trusted boot***
- **Objectifs**
  - Ne charger que des éléments (systèmes, applications) contrôlées et vérifiées
  - DRM, protection contre la rétroconception
- **Principes**
  - A chaque étape on vérifie la suivante avant de la charger
  - Signature et éventuellement chiffrement
  - Clé publique racine stockée en dur

iOS trusted boot



- **BootROM**
  - Non modifiable
  - Contient le certificat racine d'Apple
- **LLB Low Level Bootloader**
- **Images**
  - Conteneurs IMG3
  - Signées & chiffrées
- **Vérification signature de l'élément suivant avant de le charger**

Bac à sable (*sandbox*)

- **Permet d'exécuter les applications dans un environnement contrôlé**
  - Fichiers accessibles
  - Fonctions autorisées
  - Isolation des autres applications
  - Etc.
- **Une application malfaisante ou mal programmée ne doit pas pouvoir faire de dégâts ailleurs**
- **Un immense progrès**
  - Windows 95
  - chroot
  - MAC (*Mandatory Access Control*)
- **Non nécessairement exempt de failles**
  - Le but d'un exploit, s'échapper du bac à sable

Contrôle d'accès

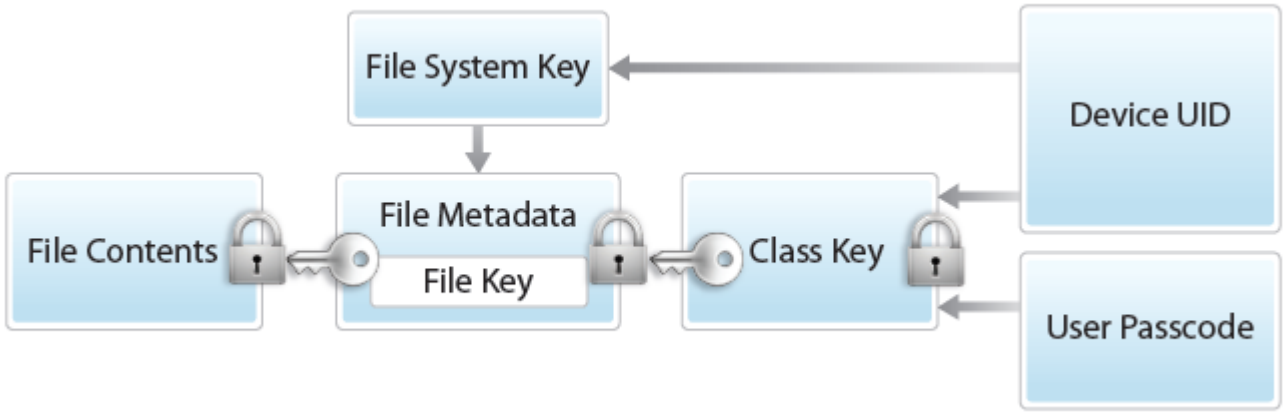
- **Discretionary Access Control – DAC**
  - Contrôle d'accès discrétionnaire
  - Un sujet avec une certaine autorisation d'accès est capable de transmettre cette permission à n'importe quel autre sujet
  - Exemple : droits d'accès sur les fichier sous Unix
- **Role-Based Access Control –RBAC**
  - Contrôle d'accès à base de rôles
  - Décision d'accès est basée sur le rôle auquel l'utilisateur est attaché
- **Mandatory Access Control – MAC**
  - Contrôle d'accès obligatoire
  - Décisions de protection ne doivent pas être prises par le propriétaire des objets concernés mais imposées par le système
  - Exemple : SELinux

Modèle sécurité iOS

- **Sandbox : politique pour TrustedBSD (MAC)**
- **Trusted boot**
- **Processeur cryptographique matériel AES 256**
  - Clés AES stockées en dur dans le processeur
    - UID : unique pour chaque appareil
    - GID : partagée par tous les appareils du même modèle
      - Sert à déchiffrer les images IMG3 (boot)
- **Mémoire NAND**
  - Zone effaçable (sans wear-leveling) → stockage de clés
  - Chiffrée par le contrôleur DMA
    - Clé dérivée de UID
    - Empêche de lire directement la puce NAND

iOS chiffrement des fichiers

- 1 clé AES par fichier, stockée dans un bloc lui-même chiffré par un dérivé de la clé UID et éventuellement du mot de passe



iOS classes de protection

- **Complete protection**
  - UID + mot de passe
  - App mail, launch images, location data
- **No Protection**
  - UID seulement
- **Protected Unless Open**
- **Protected Until First User Authentication**

iOS keychain

- **Sert à stocker des secrets (mots de passe, clés)**
- **SQLite database**
  - Protégé par UID
  - Eventuellement pour certains éléments par le mot de passe
- **Classes de protection**
  - Analogues à celles des fichiers

Modèle sécurité Android

- **Basé sur GNU/Linux**
  - Libc Google → Bionic
- **Applications**
  - Java avec JVM Dalvik
  - Possibilité d'intégrer du code natif
    - Ouvre des possibilités pour des exploits

Modèle sécurité Android

❑ Signature numérique

- ➢ Toute application doit être signée
- ➢ Coût modique d'acquisition d'un certificat
- ➢ Vérifications quasiment nulles
- ➢ Certificats expirent après 22/10/2033

❑ Cloisonnement

- ➢ 1 uid par application
- ➢ 1 gid pour toutes les applications signées par le même certificat
  - elles peuvent aussi partager le même uid → applications malfaisantes « k-aires »

Modèle sécurité Android

❑ Révocation

- ➢ Kill switch : élimine à distance des app identifiées par leur certificat
- ➢ Nécessite une connexion réseau

❑ Permissions

- ➢ Manifeste décrit les permissions requises par l'app
- ➢ L'utilisateur peut accepter ou refuser l'app mais pas modifier les permissions
- ➢ Qui est capable d'effectuer un choix éclairé ?
- ➢ Un vendeur de matériel, opérateur peut ajouter des permissions à l'Android standard
  - ○ *pm list permissions*

Plan

- ❑ Cryptographie
- ❑ Vie privée
- ❑ Menaces, vulnérabilités, exploits, risques
- ❑ Modèle de sécurité
- ❑ **Ecosystème & sécurité**
- ❑ Outils de sécurité
- ❑ Perspectives

Ecosystème

- Fabricants de matériels
- Fabricants de l'OS (Google)
- Opérateurs téléphoniques, circuits de distribution
- Développeurs d'applications
- Fournisseurs de contenus et de services (régies publicitaires, services en ligne, etc.)

Problématique des mises à jour

- **Multiplicité des acteurs**
  - Fournisseur OS
  - Fabricant du matériel
  - Opérateur téléphonique
- **Obsolescence très rapide des produits**
  - Sortie de produits pas encore au point
  - Impossibilité d'installer la dernière version sur un matériel un peu ancien
- **Quand, où effectuer les mises à jour ?**
  - Débit réseau
  - Environnements non sûrs (points d'accès malfaisants)

Publicité dans les applications

- **Fortes similarité dans le code des applications liées à l'intégration d'outils pour monnayer la publicité**
  - Part importante du code (~80%)
  - Nombre réduit de fournisseurs
  - Très consommateur de ressources (batterie)
  - Sécurité ?
  - Respect de la vie privé ?
- **Modèle économique**
  - Gratuit ou très bon marché
  - Se rémunère en vendant les informations personnelles récupérées
- **Plagiat, vol**
  - Récupère des applications payantes
  - Les modifie légèrement en ajoutant de la publicité voire du code malfaisant

Plan

- ❑ Cryptographie
- ❑ Vie privée
- ❑ Menaces, vulnérabilités, exploits, risques
- ❑ Modèle de sécurité
- ❑ Ecosystème & sécurité
- ❑ **Outils de sécurité**
- ❑ Perspectives

Antivirus PC

❑ Antivirus

- ➢ Essentiellement signatures
- ➢ Un peu de comportemental, heuristique
- ➢ Intercepte des fonctions systèmes (*hook*)

❑ Limites

- ➢ Explosion du nombre de codes malfaisants et donc de signatures
- ➢ Ressources consommées
- ➢ Polymorphisme des virus
- ➢ Délais de prise en compte des nouveaux virus
- ➢ 68% des attaques ciblées (APT) ne sont vues qu'une fois (source FireEye)

Antivirus smartphone

- **Antivirus smartphone**
  - Tous les codes sont signés et parfaitement identifiés
    - Vérifications en amont
    - Listes noires ou/et blanches d'applications
  - Applications dans un bac à sable
    - Limite les risques
    - Un antivirus ne peut intercepter les fonctions systèmes (sauf jailbreak ou noyau modifié)
- **Marketing**
  - Assez illusoire en matière de sécurité
  - Peut diminuer la sécurité
  - Faux antivrus qui ne sont que des applications malfaisantes
- **Gestions des applications**
  - Listes blanches, listes noires
  - Réputation

Outils de sécurisation

- ❑ Pas de *silver bullet*
- ❑ La sécurité est un processus pas un produit (Bruce Schneier)
- ❑ Approche globale
- ❑ Présentation suivante sur le BYOD

Plan

- ❑ Cryptographie
- ❑ Vie privée
- ❑ Menaces, vulnérabilités, exploits, risques
- ❑ Modèle de sécurité
- ❑ Ecosystème & sécurité
- ❑ Outils de sécurité
- ❑ **Perspectives**

Convergence PC → smartphones

- **Intégration dans les dernières versions (Windows 8, Mac OS X Mountain Lion)**
  - Interface
  - Modèle des applications distribuées dans une place de marché
  - Bac à sable
  - Signature généralisée du code
  - Secure boot

Est-ce si différent ?

- **Reproduction des erreurs classiques**
- **Les grands principes de sécurité restent toujours valables**
  - Appréciation des risques
  - Respect des bonnes pratiques
- **Progression dans les modèles de sécurité**
  - Regret que l'on ne soit pas allé plus loin
- **Aggravation de la menace**
  - Applications malfaisantes