Investigation numérique & terminaux Apple iOS

Acquisition de données

Mathieu RENARD
ANSSI/LAM
mathieu.renard[à]ssi.gouv.fr

Constat

Démocratisation de l'usage terminaux mobile en entreprise
  - Stockage d'informations professionnelles
  - Sécurité, management des terminaux mal ou non maitrisé

Menaces
  - Accès illégitimes au données professionnelles / réseau de l'entité
  - Usurpation d'identité
  - Atteinte à la disponibilité du terminal

Risques accentués par le caractère mobile des terminaux (perte, vol)

Les terminaux mobiles sont des cibles de choix pour les attaquants

Investigation numérique iOS

Outils

Framework iPhoneDataProtection
  - Acquisition physique (iPhone 4 et inférieur)

iPhone Backup analyzer2
  - Analyse des sauvegardes iOS

Celebrite UFED
  - Solution commerciale
  - Acquisition physique (iPhone 4 et inférieur)
  - Acquisition Logique (backup & AFC)

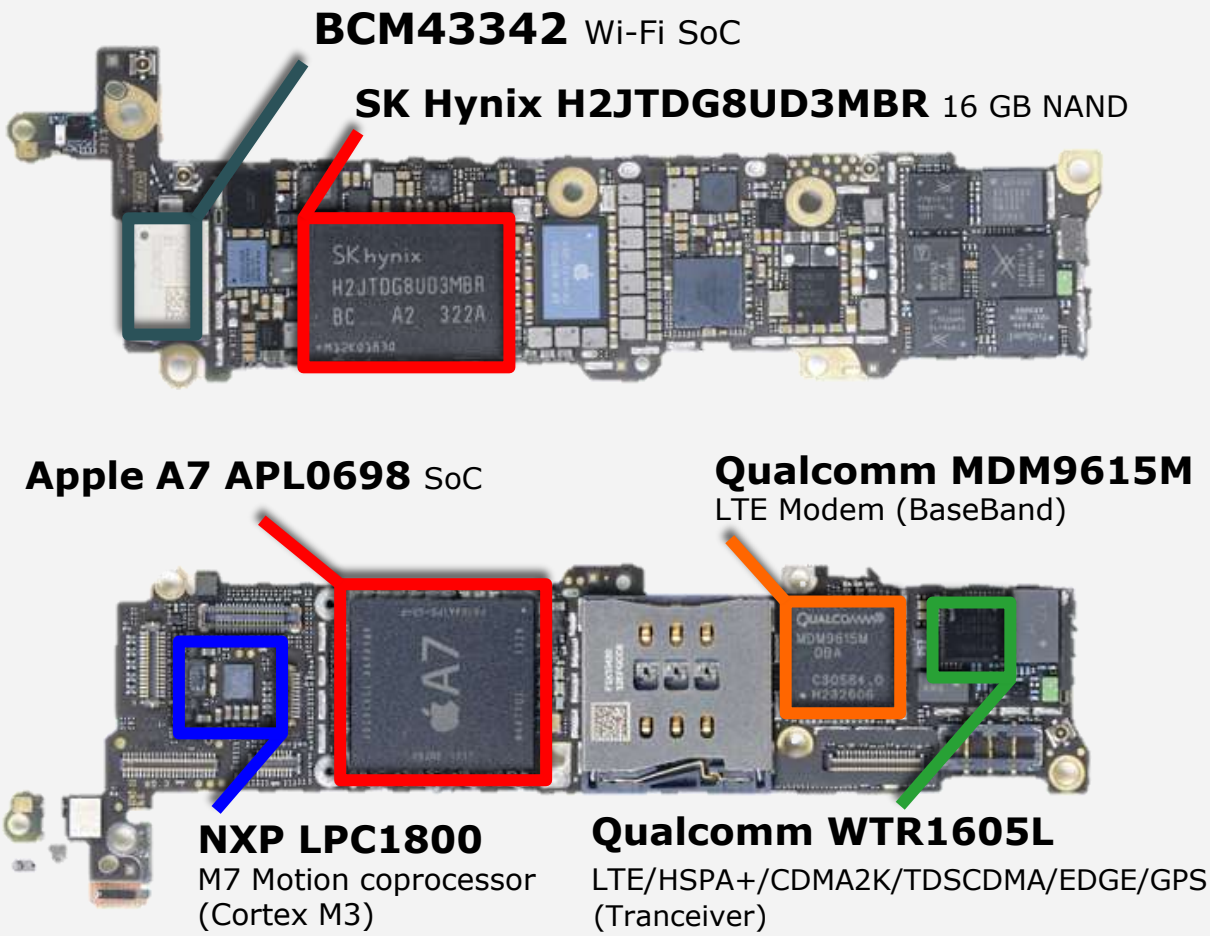
Investigation numérique & terminaux Apple iOS

- La liste d'outils d'investigation numérique pour iOS est limitée
- Aucun outil ne permet d'infirmer ou confirmer une compromission
- Nécessité de développer des méthodes et outils

iPhone
Architecture et sécurité

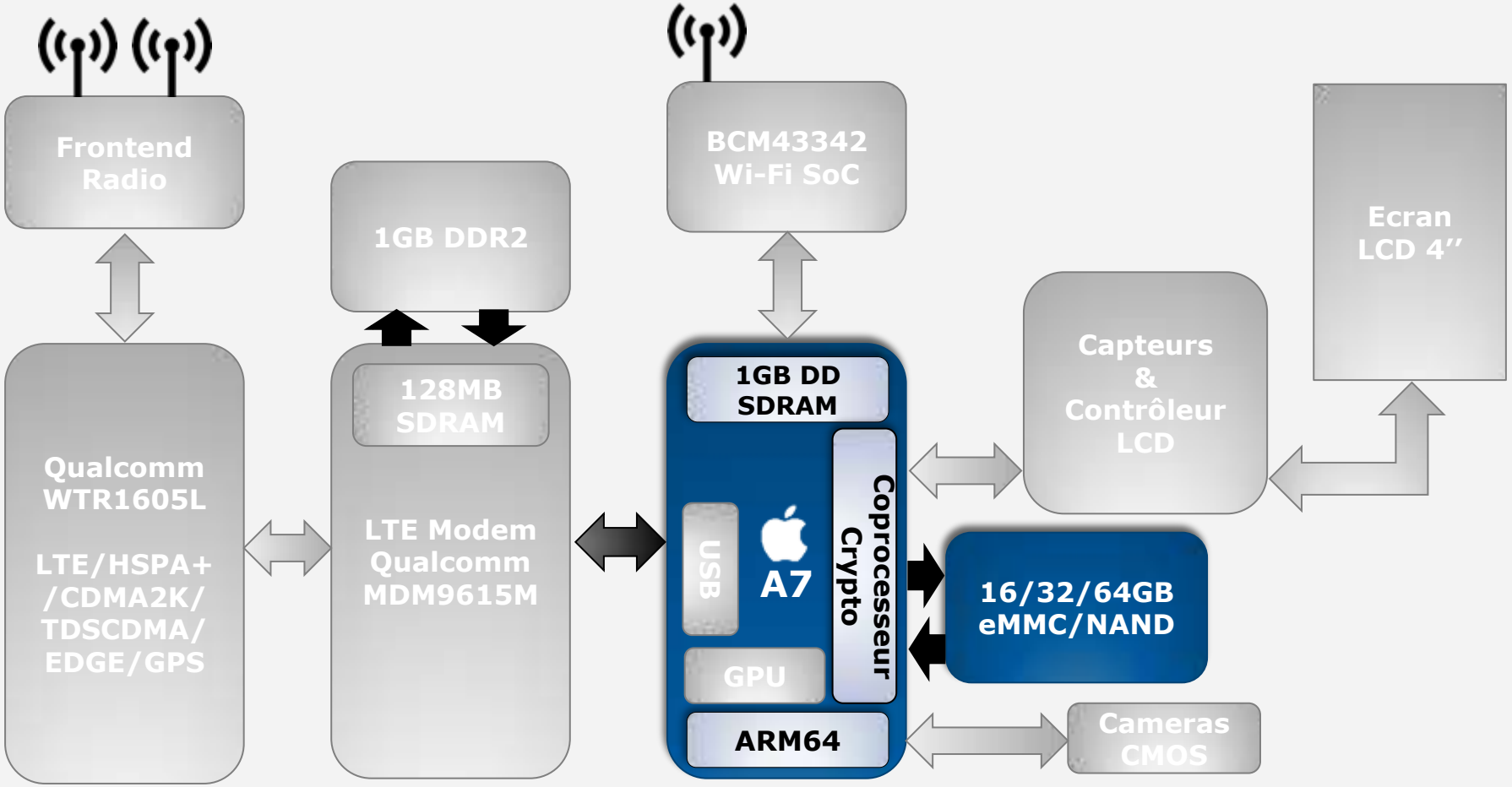
Architecture matérielle

Let's open the box



Architecture matérielle (Simplifiée)

iPhone 5S



Mécanismes de sécurité iOS

En 30 secondes…

Secure Boot

Signature de code

Exploit mitigation

Applications Sandbox

iPhoneDataProtection

Investigation numérique & terminaux Apple iOS

Acquisition physique

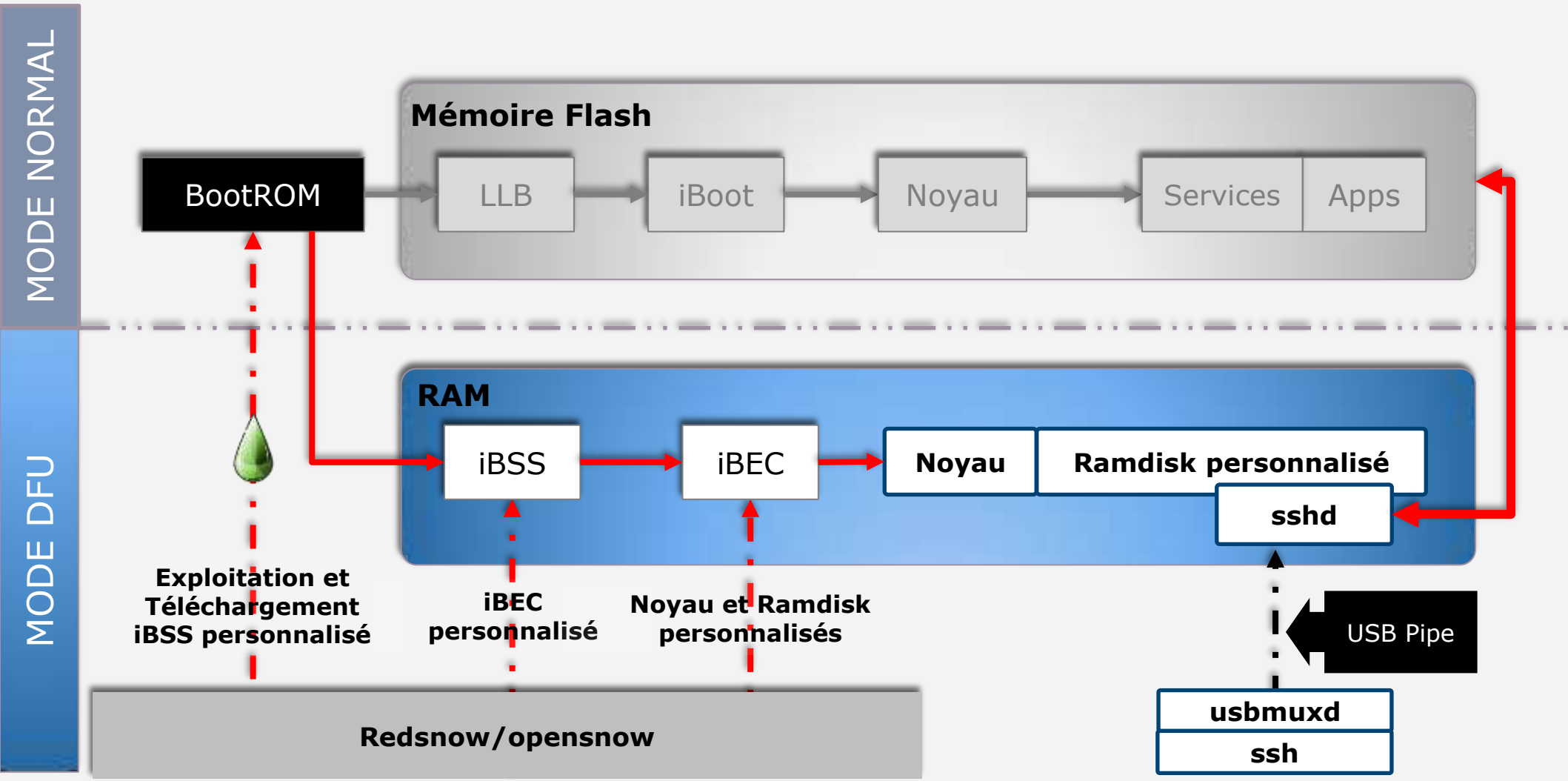
Vulnérabilités BootROM

Exécution de code via le mode DFU (device firmware update)
  - Le BootROM est en lecture seule
  - Fonctionne quelque soit la version d'iOS installée
  - Permet de charger le noyau et/ou ramdisk alternatif non signés
    - Technique similaire au boot sur un live CD/live USB
  - Accès en lecture au contenus de la NAND (API de bas niveau)

Exploits publics
  - Pwnage2 : iPhone 2G, iPhone 3G
  - Steaks4uce : iPod Touch 2G
  - Limera1n : iPhone 3GS, iPad 1, iPhone 4

Limera1n et analyse forensics

Acquisition d'une image de la flash NAND



Acquisition physique de données

Conclusion

- Lecture directe de la NAND
  - Acquisition du système de fichier complet
  - Récupération de fichiers effacés
- Framework iPhoneDataProtection
  - Maintenu par Jean Sigvald (Sogeti)
  - Acquisition d'une image de la flash NAND
  - Montage VFL/FTL pour accéder à l'état actuel de la partition de données
  - Construction d'une liste de toutes les versions disponibles de chaque bloc logique
- Possible uniquement sur iPhone < 4s et iPad < 2 (Vulnérabilité BootROM)
- **Aucune vulnérabilité publique pour les terminaux récents**

Investigation numérique & terminaux Apple iOS

Acquisition Logique

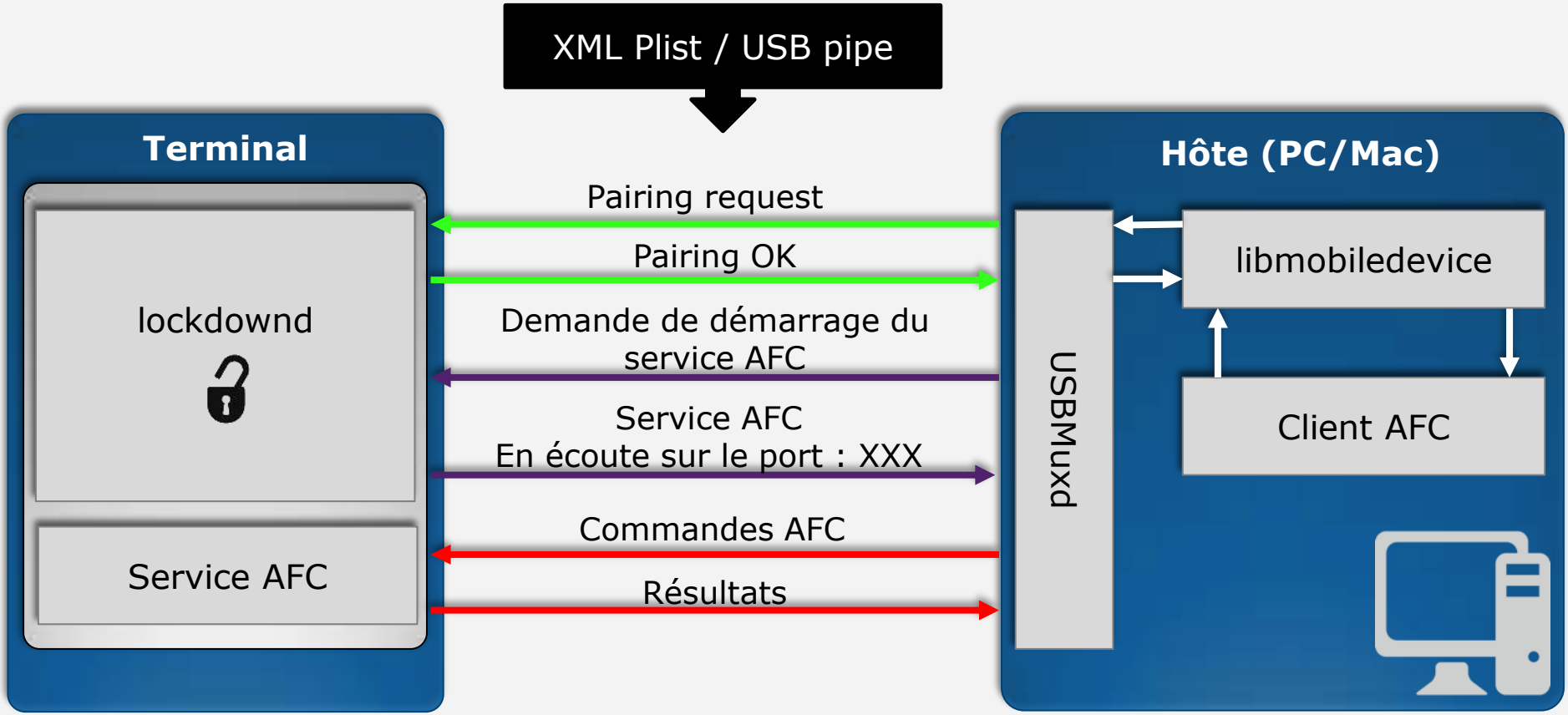
Communiquer avec un iPhone

Interfaces de communications USB

Configuration USB	Fonctions supportées
• PTP	• Transfert de fichiers multimédias
• iPod USB Interface	• Contrôle des fonctionnalités multimédias
• PTP • Apple Mobile Device	• Transfert de fichiers multimédias • Services iTunes
• PTP • Apple Mobile Device • Apple USB Ethernet	• Transfert de fichiers multimédias • Services iTunes • Interface réseau virtuelle

Communiquer avec un iPhone

Services iTunes



Investigation numérique et services iTunes

Backups
com.apple.mobilebackup
com.apple.mobilebackup2

Configuration & user databases
com.apple.mobile.file_relay

Fichiers & Medias
com.apple.afc
com.apple.mobile.house_arrest

Debugging & Instrumentation
com.apple.pcapd
com.apple.syslog_relay

Whats0n ?

DEMO: Démonstration d'acquisition Logique

Acquisition logique de données
Conclusion

- Requiert L'autorisation de l'utilisateur
  - Déverrouillage du terminal
  - Extraction et utilisation des fichiers générés lors de l'appairage

- Récupération des données stockées sur le terminal

- **Récupération de fichiers effacés impossible**

- **Acquisition du système de fichier complet impossible**

Investigation numérique & terminaux Apple iOS

Acquisition Logique « Intrusive »

./p0sixspwn


SECURITY
ADVISORY
INSECURITY AHEAD

Jailbreak Avertissement

Ceci n’est pas une incitation à l'exploitation ou au Jailbreak

Jailbreak
  - Désactivation des fonctionnalités de sécurité des terminaux
  - Augmentation de la surface d’attaque
  - Augmentation du risque de compromission

L'ANSSI incite systématiquement les éditeurs à corriger toutes vulnérabilités identifiées, dans les plus brefs délais

Les utilisateurs sont invités à appliquer les correctifs dès leurs publications

Jailbreak Avertissement

Ceci n’est pas une incitation à l'exploitation ou au Jailbreak

Jailbreak
  - Désactivation des fonctionnalités de sécurité des terminaux
  - Augmentation de la surface d’attaque
  - Augmentation du risque de compromission

L’ANSSI incite systématiquement les éditeurs à corriger toutes vulnérabilités identifiées dans les plus brefs délais

Les utilisateurs sont invités à appliquer les correctifs dès leurs publications

LE JAILBREAK NUIT GRAVEMENT À LA SÉCURITÉ DES TERMINAUX

Investigation numérique et Jailbreak

- Investigation Numérique
  - Collecte et identification de preuve
  - Traçabilité des actions réalisées
  - Reproductibilité de l'analyse

- Jailbreak
  - Désactivation des fonctionnalités de sécurité
  - Modifications persistantes
  - Absence de documentation des modifications

- **Incompatibles avec les objectifs de l'investigation**
  - Conservation de la preuve

Analyse des Jailbreaks evasi0n7 et p0sixpwn

- Identification des modifications réalisées sur le système
- Identification de techniques utilisables dans le contexte forensique
- Application des techniques de Jailbreak à l'analyse forensique
  - Réduction de l'impact sur le système
  - Maitrise et traçabilité des modifications
- Activation temporaire d'une copie déverrouillée du service
  - Permet d'acquérir l'intégralité des fichiers
  - Impact sur le système variable en fonction de la version d'iOS
  - Impact maîtrisé

Débridage du service AFC

iOS 6.x.x - MobileStorageMounter

com.apple.mobile_image_mounter
  - Service utilisé pour monter des images DMG signées
  - Montage des outils de développement
  - Montage des outils de mise à jour OTA iOS 6

Race condition dans « MobileStorageMounter »
  - Vulnérabilité identifiée par Comex
  - Leak du code d'exploitation (2013)
  - Réutilisation du code par ./p0sixspwn (2013)
  - Autorise le montage d'une image DMG non signée

Débridage du service AFC

iOS 6.x.x : Race condition & MobileStorageMounter

Montage d'une image DMG
  - Téléchargement de l'image dans /var/mobile/Media
  - Calcul de l'empreinte
  - Vérification de la signature
  - Déplacement l'image dans une zone non accessible
  - Montage de l'image

Absence de verrou entre le calcul de l'empreinte et le montage
  - Possibilité de remplacer l'image après vérification

Débridage du service AFC

iOS 6.x.x ./p0sixSpwn style

Création d'une image personnalisée
  - Fichier de configuration d'un service AFC personnalisé
    - Exécution depuis le répertoire racine (option « -d / »)
    - Autorisation d'accès aux fichiers spéciaux (option « -S »)

Téléchargement de l'image signée et de l'image personnalisée

Remplacement de l'image singé par une image personnalisée

Demande de démarrage du service AFC débridé

ShareUnl0ck

DEMO: Acquisition Logique « intrusive » iOS 6.x.x

Débridage du service AFC

Le cas d'iOS 7.0.x - Eléments de contexte

com.apple.afc
- Service de transfert de fichiers
- Service géré par /usr/libexec/afcd
- Utilisé par iTunes lors des phases de synchronisation
- Accès limité aux contenus du répertoire /var/mobile/Media
- Possibilité d'accès aux contenus des applications tierces

Activation temporaire d'une copie déverrouillée du service
- Démarrage du service AFC à l'aide de lockdownd impossible
- Vulnérabilités utilisées par les Jailbreaks précédant corrigées
- Système de fichier en lecture seul
- Impossible de créer un exécutable dans un répertoire contrôlé par l'utilisateur
- Afcd Initialise sa propre sandbox lors du démarrage
  - /usr/lib/system/libsystem_sandbox.dylib

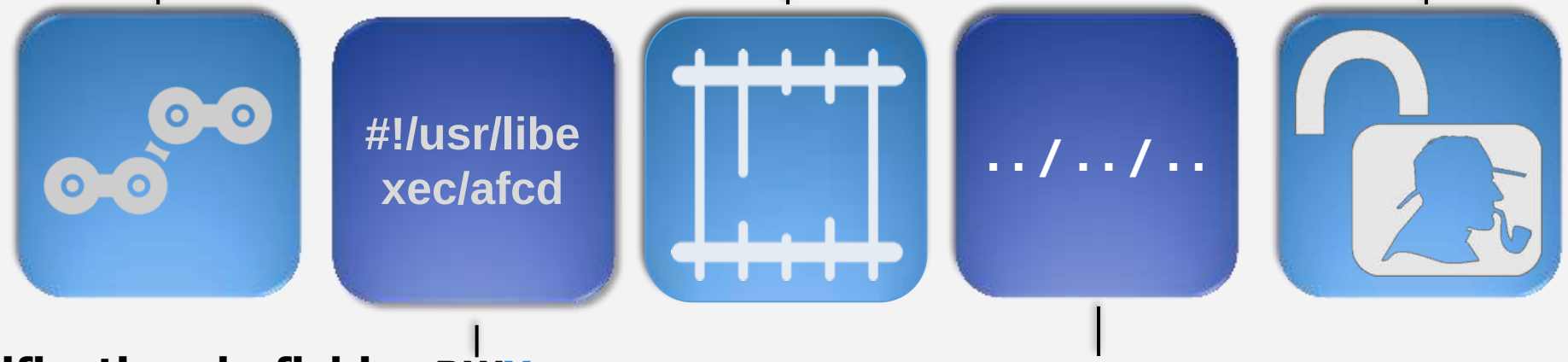
Débridage du service AFC

iOS 7.0.x – Not yet another evasi0n…

Contournement de la sandbox afcd
- Création d'une bibliothèque : ShareUnl0ck.dylib

Création d'un fichier RWX
- ShareUnl0ck

Exécution de ShareUnl0ck
- Débridage de afcd



Modification du fichier RWX
- Remplacement de ShareUnl0ck par un shebang

Chargement de ShareUnl0ck.dylib au démarrage de ShareUnl0ck
- Modification de com.apple.mobile.installation.plist

Débridage du service AFC

Obtention d'un fichier disposant des droits RWX

« installd »
  - Service en charge de l'installation des applications

Directory traversal dans installd
  - Requiert l'utilisation d'une application signée par Apple
  - Extraction de l'application
  - Téléchargement du contenu du paquet de l'application sur le terminal
    - /var/mobile/Media/
  - Modification du chemin de l'exécutable dans le fichier info.plist
    - CFBundleExecutable = ../../../../../../var/mobile/Media/myapp.app/myapp
  - Reconstruction du paquet de l'application
    - CustomApp.ipa
  - Installation de l'application modifiée
    - Installd => chmod +x ../../../../../../var/mobile/Media/myapp.app/myapp

Débridage du service AFC
Configuration du service AFC

Modification du fichier exécutable déployé dans /var/mobile/media

```
#!/usr/libexec/afcd -S -d / -p 8888
```

A ce stade, le service AFC est toujours soumis
  - A la politique d'isolation du système

Le service afcd initialise sa propre sandbox
  - /usr/lib/system/libsystem_sandbox.dylib

Possibilité d'interposer une bibliothèque spécialement conçue pour interdire l'initialisation de la sandbox

Débridage du service AFC

Contournement de la Sandbox

Re-exportation des fonctions à l'aide de « LazyBindings »
  - Technique introduite dans evasi0n (iOS 6)
  - Présentation détaillée sur le blog de QuarksLab

Contournement de la signature de code
  - S_ATTR_LOC_RELOC définis pour toutes les sections exécutables
  - +x retiré de chaque section exécutables :
    - Après vérification du header
    - Mais avant le mappage en mémoire pour vérification de la signature

MACH-O Kung Fu

http://blog.quarkslab.com/evasi0n-jailbreak-precisions-on-stage-3.html
http://geohot.com/e7writeup.html

Débridage du service AFC

Modification des variables d'environnement

Chargement de la bibliothèque non signée
  - Utilisation de la variable d'environnement DYLD_INSERT_LIBRARY
  - Lecture du contenu du fichier com.apple.installation.plist
    - /private/var/mobile/Library/Cache/ com.apple.mobile.installation.plist
    - Contient les paramètres de lancement des applications
    - Téléchargeable via le service : com.apple.mobile.file_relay

Modification du contenu du fichier com.apple.installtion.plist
    - Impossible en fonctionnement nominal

Débridage du service AFC

Modification des variables d'environnement

« installd »
  - Service en charge de l'installation des applications Apple iOS signées
  - Non soumis aux règles d'isolation imposées par la sandbox

Race condition dans « installd »
  - Extraction du contenu d'un fichier zip sur le système
  - L'extraction du contenu de la charge active dans le répertoire :
    - ../../../var/mobile/Library/Caches/
  - Permet d'actualiser com.apple.mobile.installation.plist
  - Requiert un accès au répertoire « /tmp »

Débridage du service AFC

Chargement de la bibliothèque non signée

com.apple.afc
  - Service géré par /usr/libexec/afcd
  - Utilisé par iTunes lors des phases de synchronisation
  - Accès limité aux contenus du répertoire /var/mobile/Media
  - Possibilité d'accès aux contenus des applications tierces
  - Intègre des fonctions en charge d'interdire le « directory traversal »

Directory traversal & afcd
  - Lors de la création d'un lien symbolique afcd compte le nombre de ../
  - Interdiction d'accès aux fichiers situés à l'extérieur du répertoire racine
  - Le déplacement du lien dans un répertoire de niveau inférieur permet de contourner ce mécanisme de protection

Débridage du service AFC

Mise à jour du cache et démarrage du service

Rechargement des caches
  - com.apple.mobile.installation.plist,…
  - Utilisation du service com.apple.diagnostique_relay
  - Redémarrage le système

Lancement du service AFC débridé
  - Lancement de l'application modifiée par l'analyste

ShareUnl0ck

ShareUnl0ck

DEMO: Acquisition Logique « intrusive » iOS 7.0.x

Acquisition logique « intrusive »
Conclusion

- Requiert L'autorisation de l'utilisateur
  - Déverrouillage du terminal
  - Extraction et utilisation des fichiers générés lors de l'appairage
- Récupération des données stockées sur le terminal
- Acquisition du système de fichier complet
- Récupération de fichiers effacés impossible

iOS Forensics
Résultats

Analyse différentiel d'un système Jailbraké

Acquisition d'une image de référence
  - A partir d'un firmware Apple
  - A partir d'un terminal Apple

Comparaison des images
  - Identification des fichiers connus (Liste blanche / Liste noire)
  - Context Triggered Piecewise Hashing (CTPH)
    - Initialement développé par Andrew Tridgell : détection de spam
    - Transposé au monde du forensics par Jesse Kornblum
    - Outils : ssdeep, binwally

CTPH

Identification des modifications sur un terminal Jailbreaké

25 differs etc/fstab
25 differs private/etc/fstab
>>> unique target/var/mobile/Media/.evasi0n7_installed
>>> unique target/var/mobile/Media/jailbreak.log
>>> unique target/private/var/tmp/evasi0n-started
[..]
>>> unique target/System/Library/LaunchDaemons/com.evad3rs.evasi0n7.untether.plist
>>> unique target/System/Library/LaunchDaemons/com.saurik.Cydia.Startup.plist
>>> unique target/System/Library/Caches/com.apple.xpcd/xpcd_cache.dylib
>>> unique target/System/Library/Caches/com.apple.dyld/enable-dylibs-to-override-cache
[..]
>>> unique target/tmp/evasi0n-started
>>> unique target/pri/vate/var/mobile/Media/.evasi0n7_installed
>>> unique target/private/var/mobile/Media/jailbreak.log
>>> unique target/evasi0n7
>>> unique target/evasi0n7-installed

CTPH

Limites

L'analyse des périphériques n'est pas prise en charge
  - Réalisation d'une analyse manuelle
  - Identification de deux périphériques suspects

/dev/hax-ptsd
/dev/hax-test

L'image du noyau n'est pas modifiée
  - Evasi0n patch le noyau lors du démarrage

100 matches System/Library/Caches/com.apple.kernelcaches/kernelcache

Investigation numérique et iOS
Compatibilité

Compatibilité des méthodes d'acquisitions

Modèle	Acquisition physique (sans jailbreak)	Acquisition logique
iPhone ≤4	**Oui**	**Oui** (Equipement déverrouillé)
iPhone ≥ 4s	Non	
iPad 1	**Oui**	
iPad ≥ 2	Non	
iPad ≤ 2	**Oui**	

Version	Acquisition logique non intrusive	Acquisition logique intrusive
iOS < 7.0.6	**Oui**	**Oui**
iOS > 7.0.6	Non	

Conclusion

Conclusion 1/2

- Acquisition physique des données
  - Méthode la plus pertinente
  - autorise la récupération du contenu de certains fichiers effacés
  - S'affranchis des API du système
  - Ne s'applique qu'aux terminaux utilisant le processeur Apple A4 ou plus

- Acquisition logique « non intrusive »
  - compatible avec toutes les versions de terminaux en circulation
  - Inadaptée dans le cadre de la recherche de preuves de compromissions

Conclusion 2/2

Acquisition logique « intrusive »

- Permet de contourner les limites de la méthode « non intrusive »
- S'appuie sur l'exploitation de vulnérabilité
- Utilise les API du système
- Entraine des modifications
- Extraction du système de fichiers possible

Limites

- Acquisition et l'analyse de la mémoire RAM impossible
- Acquisition du code exécuté par le « Baseband » impossible
- Analyse des applications provenant de l'App Store impossible
- Repose sur les API du système

Merci de votre attention

Questions ?