

Forensics, Malware and Penetration Testing

Mobile forensics

David Oswald

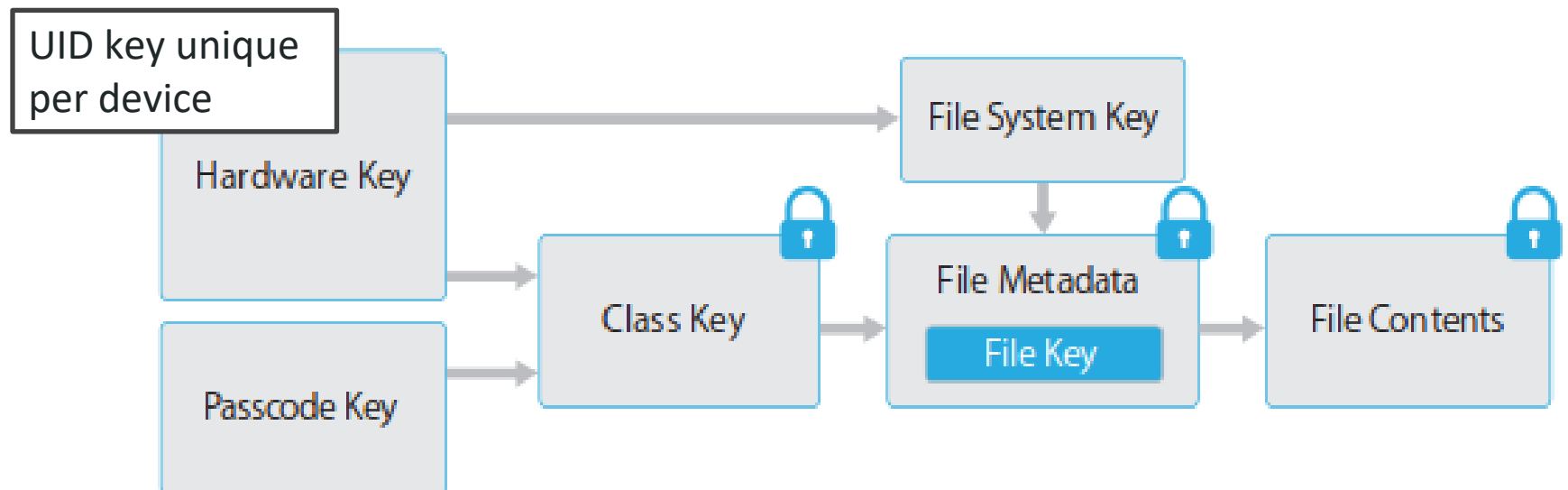
University of Birmingham

d.f.oswald@cs.bham.ac.uk



Full-disk encryption (FDE) on iOS

iOS supports FDE much longer (and better), proper binding to user (sometimes) and real hardware secret



Passcodes on iOS

- Passcodes (4-digit, 6-digit, alpha-numeric) are used for key derivation in secure enclave processor (SEP)
- Passcodes can only be brute-forced online (on the actual device)
- 80 ms delay between attempts, in addition increasing delays:

Delays between passcode attempts	
Attempts	Delay Enforced
1-4	none
5	1 minute
6	5 minutes
7-8	15 minutes
9	1 hour

https://www.apple.com/business/docs/iOS_Security_Guide.pdf

iOS FDE - Summary

- Very mature system, hard to break if passcode complex enough
- 4-digit passcode could be (manually) bruteforced with “NAND mirroring” in approx. 1 day
- “GrayKey”

<https://arxiv.org/ftp/arxiv/papers/1609/1609.04327.pdf>



Figure 15. iPhone 5c with logic analyzer



<https://blog.malwarebytes.com/wp-content/uploads/2018/03/GrayKey.png>

How does iOS store data, anyway?



iOS file system

- In general, iOS *shares many characteristics* with Android from the app's point of view
- Unix-like system (in this case XNU)
- Frequent use of `sqlite` (or the XML-based `plist`) for app-local and system-wide storage
- Jailbreak gives **full root access** and therefore access to root directory /
- Currently jailbreakable version: iOS 10.2

<https://www.theiphonewiki.com/wiki/Jailbreak>

Example: iPhone 3GS (ancient)

Example from a jailbroken iPhone 3GS (iOS 6.1.6)
(ancient but the principles have not changed)

```
iPhone:/ root# ls -la
total 22
drwxr-xr-x 16 root    admin    884 Mar  6 17:05 ./
drwxr-xr-x 16 root    admin    884 Mar  6 17:05 ../
d-wx-wx-wx  2 _unknown _unknown  68 Feb  2 2013 .Trashes/
----- 1 root    admin    0 Feb  1 2013 .file
drwx----- 2 root    admin    170 Feb 26 18:22 .fsevents/
lrwxr-xr-x  1 root    admin    32 Feb 25 18:31 Applications -> /var/stash/_c
aNeXw/Applications/
drwxrwxr-x  2 root    admin    68 Feb  2 2013 Developer/
drwxrwxr-x 13 root    admin    646 Feb 25 18:24 Library/
drwxr-xr-x  3 root    wheel    102 Feb  2 2013 System/
lrwxr-xr-x  1 root    admin    11 Mar  6 17:05 User -> /var/mobile/
drwxr-xr-x  2 root    wheel   1972 Feb 25 18:51 bin/
drwxr-xr-x  2 root    wheel    68 Oct 28 2006 boot/
drwxrwxr-x  2 root    admin    68 Feb  2 2013 cores/
dr-xr-xr-x  3 root    wheel   1503 Mar  6 17:04 dev/
lrwxrwxrwx  1 root    wheel    12 Feb 25 18:22 etc -> private/etc//
drwxr-xr-x  2 root    wheel    68 Oct 28 2006 lib/
drwxr-xr-x  2 root    wheel    68 Oct 28 2006 mnt/
drwxr-xr-x  4 root    wheel   136 Feb  2 2013 private/
drwxr-xr-x  2 root    wheel   646 Feb 25 18:30 sbin/
lrwxrwxrwx  1 root    wheel    16 Feb 25 18:22 tmp -> private/var/tmp//
drwxr-xr-x  8 root    wheel   340 Feb 25 18:25 usr/
lrwxrwxrwx  1 root    wheel    12 Feb 25 18:22 var -> private/var//
iPhone:/ root#
```


Example: iPhone 3GS (ancient)

System application storage

```
iPhone:/User/Library root# ls
Accounts/           Keyboard/           SoftwareUpdate/
AddressBook/        Logs/              Spotlight/
AggregateDictionary/ Mail/               SpringBoard/
Application\ Support/ Maps/               SyncedPreferences/
Assets/             MediaStream/        TCC/
BulletinBoard/      MobileInstallation/ VoiceServices/
Caches/             Notes/              Voicemail/
Calendar/           OTALogging/         WebClips/
Carrier\ Bundle.bundle@ Operator\ Bundle.bundle@ WebKit/
ConfigurationProfiles/ Passes/              com.apple.iTunesStore/
Cookies/            Preferences/          com.apple.itunesstored/
Cydia/              SMS/
FairPlay/           Safari/
iPhone:/User/Library root# ls AddressBook/
AddressBook.sqlitedb      AddressBook.sqlitedb-wal      AddressBookImages.sqlitedb-shm
AddressBook.sqlitedb-shm  AddressBookImages.sqlitedb    AddressBookImages.sqlitedb-wal
iPhone:/User/Library root#
```

Example: iPhone 3GS (ancient)

Address book is sqlite

```
iPhone:/User/Library/AddressBook root# sqlite3 AddressBook.sqlitedb
SQLite version 3.7.13
Enter ".help" for instructions
sqlite> select first,last from ABPerson;
Hans|Dampf
|
sqlite> .quit
iPhone:/User/Library/AddressBook root#
```

Example: iPhone 3GS (ancient)

Maps has binary file + plist

```
iPhone:/User/Library/Maps root# ls -la
total 36
drwxr-xr-x  3 mobile mobile   204 Feb 25 19:07 ./
drwxrwxrwx 37 mobile mobile  1326 Feb 26 12:56 ../
-rw-r--r--  1 mobile mobile    79 Oct 31 17:36 Bookmarks.plist
-rw-r--r--  1 mobile mobile 14974 Feb 25 19:06 History.mapsdata
drwxr-xr-x  3 mobile mobile   102 Feb 25 19:06 ReportAProblem/
-rw-r--r--  1 mobile mobile 15322 Feb 25 19:07 SearchResults.dat
iPhone:/User/Library/Maps root# grep -a Birmingham History.mapsdata
Birmingham
"University of BirminghamZ    EdgbastonZ
BirminghamZB15 2TTZEnglandz
Birmingham2
Great BritainrUniversity of BirminghamrUniversity of Birmingham    EdgbastonJ
+441214143344Bhttp://www.birmingham.ac.uk
Curzon StreetZCity University - School of Acting2ZMillennium PointZ
BirminghamZB4 7XGZEnglandz1
Birmingham2
+441213317220Bhttp://www.bcu.ac.uk/actingBirmingham City University - School of Acting
"#University of Birmingham - The Vale2ZEdgbaston Park RoadZ
BirminghamZB15 3SZEnglandz
Birmingham2
Great BritainrEdgbaston ParkBark EdgbastonJston PB,;J@RÖ_Û~#University of Birm
+441214143344Bhttp://www.birmingham.ac.uk/
```

Example: iPhone 3GS (ancient)

Photos in DCIM folder

```
iPhone:/User/Media/DCIM/100APPLE root# ls -la
total 1208
drwxr-xr-x  2 mobile mobile    102 Feb 25 19:03 ./
drwxr-x---  4 mobile mobile    136 Feb 25 19:03 ../
-rw-r--r--  1 mobile mobile 1236988 Feb 25 19:03 IMG_0001.JPG
iPhone:/User/Media/DCIM/100APPLE root#
```

Some wifi info in

```
/iPhone:/Library/Preferences/SystemConfiguration root# ls -la
total 20
drwxr-xr-x  2 root wheel   238 Mar  6 17:10 ./
drwxr-xr-x  3 root wheel   136 Feb 25 18:18 ../
-rw-r--r--  1 root wheel   767 Mar  6 17:04 NetworkInterfaces.plist
-rw-r--r--  1 root wheel    59 Mar  6 17:04 OSThermalStatus.plist
-rw-r--r--  1 root wheel    78 Oct 31 17:36 com.apple.mobilegestalt.plist
-rw-r--r--  1 root wheel 1180 Mar  6 17:04 com.apple.wifi.plist
-rw-r--r--  1 root wheel 2986 Mar  6 17:04 preferences.plist
iPhone:/Library/Preferences/SystemConfiguration root#
```

Example: iPhone 3GS (ancient)

Keychain folder

```
iPhone:/Library/Keychains root# ls -la
total 180
drwxr-xr-x  2 _securityd wheel   204 Mar  6 17:20 ./
drwxr-xr-x 30 root      wheel  1156 Feb 25 18:22 ../
-rw-----  1 _securityd wheel 16384 Feb 25 18:08 TrustStore.sqlite3
-rw-----  1 _securityd wheel 16384 Mar  6 17:05 caissuercache.sqlite3
-rw-----  1 _securityd wheel 98304 Mar  6 17:04 keychain-2.db
-rw-----  1 _securityd wheel 53248 Mar  6 17:20 ocspcache.sqlite3
```

Plists in XML format

```
ClientTruth.plist      PayloadManifest.plist  PublicInfo/
MCDataMigration.plist  ProfileTruth.plist     UserSettings.plist
iPhone:/User/Library/ConfigurationProfiles root# cat UserSettings.plist
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTD/
PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
  <key>assignedObject</key>
  <dict/>
  <key>restrictedBool</key>
  <dict>
    <key>allowAccountModification</key>
    <dict>
      <key>value</key>
      <true/>
    </dict>
  </dict>
  <key>allowAddingGameCenterFriends</key>
  <dict/>
  <key>allowAccountModification</key>
  <dict/>
  <key>restrictedBool</key>
  <dict/>
  <key>assignedObject</key>
  <dict/>
</dict>
</plist>
```

iOS Summary

- Logical acquisition difficult if locked
- Cellebrite offers special services:

<https://cellebrite.com/en/advanced-services/>

Supported Devices

Apple Samsung Huawei Other Android

Data access and collection for the latest Apple iOS devices including all iPhone models (iPhone 4S to iPhone 12), iPad, iPad mini, iPad Pro, and iPod touch, running iOS 5 to iOS 14.7.1.

After-First-Unlock (AFU) access to locked iPhones up to iPhone 12, running iOS 11.3 to 14.3 (must keep device alive after seizure!)

Limitations may apply.

Checkra1n / checkm8

- Checkm8 bootrom exploit (CVE-2019-8900) is unpatchable and affects iPhone X and older, iPads up to 7th gen, etc
<https://blog.malwarebytes.com/mac/2019/09/new-ios-exploit-checkm8-allows-permanent-compromise-of-iphones/>
- With physical access, attacker can bypass various system protections for forensics purposes, see e.g. <https://blog.elcomsoft.com/2020/06/checkra1n-unc0ver-jailbreak-today/>
- Integrated in major iOS forensics tools like <https://www.elcomsoft.com/eift.html>

iOS Summary

- Logical acquisition difficult if locked
- Cellebrite and other companies offer special “mail-in” services
- Once content acquired, analysis similar to Android (sqlite etc)
- Various (unknown) possibilities for forensic imaging, e.g. unpublished software and hardware vulnerabilities, backups, ...



hashcat

advanced
password
recovery


hashcat

Forums

Wiki

Tools

Events

 Search

 Help

Hello There, Guest!  [Login](#) [Register](#) 

Current time: 03-07-2017, 09:35 AM

hashcat Forum › Announcements › hashcat

hashcat v3.40

hashcat v3.40

[Thread Modes](#)

03-03-2017, 06:18 PM

[#1](#)



atom

Administrator



Posts: 4,473
Threads: 206
Joined: Apr 2010

Welcome to hashcat v3.40 release!

The major changes are the following:

- Added support to crack iTunes backups: <https://hashcat.net/forum/thread-6047.html>
- Added support to crack LUKS volumes: <https://hashcat.net/forum/thread-6225.html>
- Added support for hccapx files: <https://hashcat.net/forum/thread-6273.html>