Analysis of the forensic traces left by AirPrint in Apple iOS devices

Luis Gómez-Miralles, Joan Arnedo-Moreno

KISON Cryptography and Information Security for Open Networks

Universitat Oberta de Catalunya (UOC)

SMPE-2013

Barcelona, Spain

Introduction

Starting point: Mobile/Portable devices

- Exponential growth in last decade.
- Nowadays portable computers at our fingertips, capable of almost anything.

Introduction

Evolution of iOS devices in the last years

- 2007: iPhone and iPod Touch. Multi-touch interface, finger-based (no stylus).
- 2008: iPhone O.S. 2.0. App Store. Developers start coding applications extending the device capabilities.
- 2010: iPad, the rebirth of tablets. iPhone O.S. goes 'iOS'.
- 2011: iPad 2. iPhone 4S, Siri voice assistant.
- 2012: Siri comes to the iPad.

"Apple now gets about two-thirds of its revenue from iOS devices - a platform that didn't exist 5 years ago" *(Source: Augustine Fou, Marketing Science Consulting Inc.)*

Motivation

Regardless of debates, there are MANY iOS devices out there

- An iPad can replace a computer, or act as a glorified iPhone.
- A lot of personal data goes through the device.
- App based model (vs browser based).
- Closed system with undisclosed capabilities.

Who knows what's in there? iPad forensics!

Goals

Looking where nobody else has looked yet: AirPrint

- How does it work? No technical documentation!
- Reliably acquiring forensic traces.

We always assume the role of the "good guys" (for real!).

Apple AirPrint

- Introduced in iOS 4.2 (November 2010).

- Wireless, driverless printing (to AirPrint printers).

- Easy and simple for the user.

(a) **(b)** **(c)**

Analysis of forensic traces (1/3)

AirPrint use leaves some traces on device

- While printing, we monitored files, network connections, and processes.

- Spooler directory: `/var/mobile/Library/com.apple.printd/`
  - Created when printing for the first time.

- Temporary files (`1.pdf`, `2.pdf`, ...) appear here while printing.
  - The temp file is deleted as soon as the job has finished printing.

* Printing graphics (JPG at least) does NOT generate temp files.

Analysis of forensic traces (2/3)

Properties of AirPrint temp files

- The temp PDF files contain the document sent to the printer.

- When the queue is empty again (document printed, temp file deleted):
  - iOS 4: the counter is reset (a new job would generate a new `1.pdf`).
  - iOS 5: the counter keeps increasing until the device reboots.

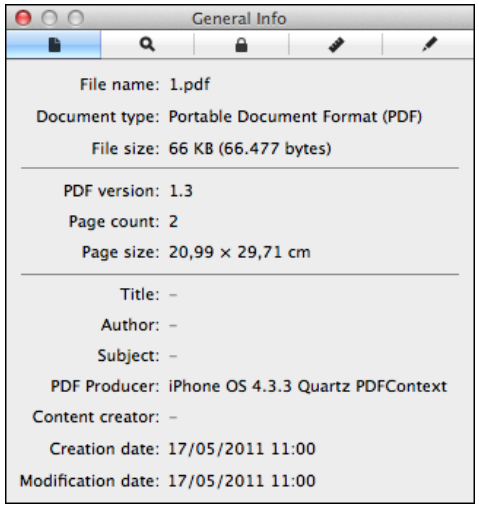
- If many copies are printed, the temp file contains an only copy of the document.

- If a page range is specified, the temp file contains only this page range.

* Exception when printing some native PDF files.

Analysis of forensic traces (3/3)

PDF metadata of temp files



- **'PDF Producer'**:
  iPhone OS x.y.z Quartz PDFContext
- **'Creation date'** == **'Modification date'**:
  Both indicate when the printing job was created.

Recoverability of Airprint traces (1/2)

Test series

iPhone 3G, iOS 4.2.1, no encryption.

1) Safari: print 4 web pages and 6 PDFs.

2) GoodReader: print 10 PDFs.

*3) Photos: print 10 photos.

4) Mail: print 5 messages and 5 attachments.

*5) Turn off. Wait for 30 sec. Turn on.

6) Safari: print 6 DOC and 4 XLS files.

*7) Mail: download 15 MB, repeat step 5.

*8) App Store: download 50 MB.

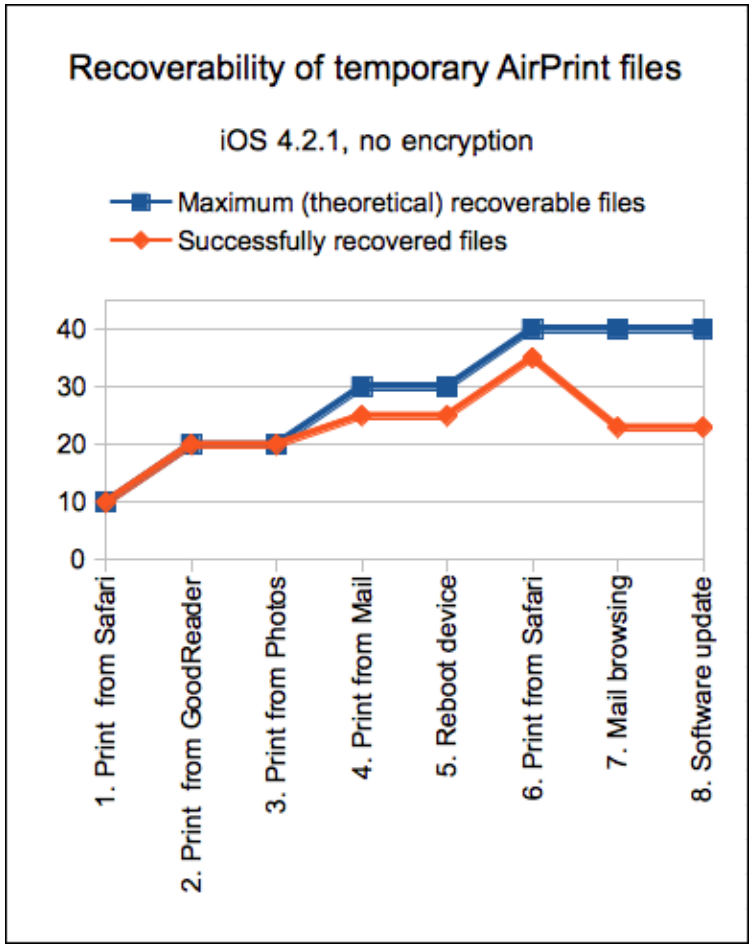
(*) == Tests that do NOT create AirPrint temp files.

Recoverability of Airprint traces (2/2)

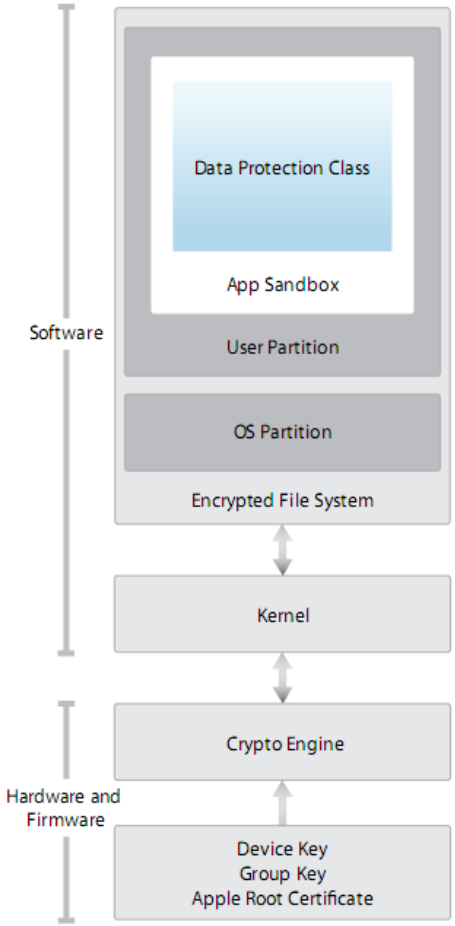
Carve PDFs with `photorec`.

Recoverable: Most artifacts were successfully recovered (even after rebooting). This confirms that AirPrint temp files are flushed to disk.

Persistant: These artifacts do not seem likely to overwrite each other's disk area.



Current challenge: IOS encryption



Now, iOS devices offer hardware-based encryption.

- Per-file encryption keys.
- Quick Summary: Carving is useless :-(

Good news: iphone-dataprotection

- Bruteforce attack on device keys.
- We still have to look into it.

Analysis of the forensic traces left by AirPrint in Apple iOS devices

Luis Gómez-Miralles, Joan Arnedo-Moreno

KISON Cryptography and Information Security for Open Networks

Universitat Oberta de Catalunya (UOC)

SMPE-2013

Barcelona, Spain