Security Analysis of Android Factory Resets

Laurent Simon
lmrs2@cam.ac.uk
https://www.cl.cam.ac.uk/~lmrs2/
Talk outline

- Background
- Methodology
- Results
- Practical recovery
- FR alternatives
Background

- Second-hand phone market growth
  - 57M, 2014 (Gartner)
  - 2/3 second life, 2015 (Gartner)
  - 150-250M traded by 2018

- Data recovery success reported
  - Avast, BBC news, etc
Secure Deletion

- **Logical Sanitisation**: data cannot be recovered via standard hardware interfaces like standard eMMC commands
- **Digital Sanitisation**: data cannot be recovered via any digital means, including the bypass or compromise of the device’s controller or firmware, or via undocumented drive commands
- This talk: *logical sanitisation*
Data Storage Locations

- **Data partition** mounted on /data
  - Sensitive info, ext4 (eMMC), yaffs2 ("raw flash")

- **Internal (primary) "SD card"**: mounted on /sdcard
  - Music, pictures, FAT, emulated (FUSE)

- **External SD card**: removable
  - Same as internal one, FAT
  - Secondary SD card, or primary if no internal one
Data Storage Locations

- /data       /sdcard (primary)
- /data
- /data       /sdcard (primary)
Flash Memory - Overview

- Unlike HDDs, Solid State Storage (SSD) supports a limited number of erase cycles (10000)

  $\Rightarrow$ memory management, wear-leveling algo

  blocks used by file system

<table>
<thead>
<tr>
<th>data 1</th>
</tr>
</thead>
</table>

- clean blocks
  - data'
  - data”

- to-be-erased dirty blocks
Flash Memory - Overview

- Unlike HDD, Solid State Storage (SSD) support a limited number of erase cycles (10000)

=> memory management, wear-leveling algo

![Diagram showing blocks used by file system and clean blocks vs to-be-erased dirty blocks]
Flash Memory – File Systems

- Software: flash-aware file system yaffs2
- Hardware: eMMC (logical view for OS)

File system

MTD device

Block device

Device driver

Controller

Flash memory
How to securely delete?

- **Yaffs2**: Exposed via `ioctl(fd, MEMERASE, blk_num)`

- **eMMC**: special commands to send to the chip
  Exposed via:
  - `ioctl(fd, BLKDISCARD, blknum)`
  - `ioctl(fd, BLKSECURITYDISCARD, blknum)`
Talk outline

- Background
- Methodology
- Results
- Practical recovery
- FR alternatives
Phone Acquisition

Proportion of devices (%)

- June 2013
- Our sample
- March 2014

<table>
<thead>
<tr>
<th>OS</th>
<th>June 2013</th>
<th>Our sample</th>
<th>March 2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Froyo (v2.2.x)</td>
<td>31M</td>
<td>0M</td>
<td>0M</td>
</tr>
<tr>
<td>KK (v4.4)</td>
<td>0M</td>
<td>0M</td>
<td>0M</td>
</tr>
<tr>
<td>GB (v2.3.x)</td>
<td>341M</td>
<td>0M</td>
<td>0M</td>
</tr>
<tr>
<td>ICS (v4.0.x)</td>
<td>233M</td>
<td>379M</td>
<td>0M</td>
</tr>
<tr>
<td>JB (v4.1-3)</td>
<td>379M</td>
<td>0M</td>
<td>0M</td>
</tr>
<tr>
<td>Other</td>
<td>0M</td>
<td>0M</td>
<td>15M</td>
</tr>
</tbody>
</table>
Setup

• Overwrite "bit-by-bit" partitions (data, primary and secondary SD card) with identifying patterns
  • Bit-by-bit = lower level possible (dd-like)
  • Identifying patterns = unique ID
• Factory Reset
• Pattern recovery and identification
- Background
- Methodology
- Results
- Practical recovery
- FR alternatives
Results: Data partition

- Froyo (v2.2.x)
- GB (v2.3.x)
- ICS (v4.0.x)
- JB (v4.[1-3])

Devices with insecure deletion (%)

- ioctl(MEMERASE)
- ioctl(BLK SEC DISCARD)

295M
138M
53M
Results: Data partition (Cont'ed)

- Upgrade from GB (2.3.x) to ICS (4.0.x)
  - `ioctl(BLKSECDISCARD)` return `errno` 95 `EOPNOTSUPPORT`
- 2007 eMMC standard has compulsory support for logical sanitisation
- HTC Sensation XE correctly wipes data partition in Bootloader mode but not for Android Factory Reset
Results: Data partition

- Froyo (v2.2.x):
  - ioctl(MEMERASE)

- GB (v2.3.x):
  - ioctl(BLKDISCARD)

- ICS (v4.0.x)
  - ioctl(BLK SEC DISCARD)

- JB (v4.[1-3])
  - IOCTL(BLK SEC DISCARD)

- Devices with insecure deletion (%):
  - 0M
  - 295M
  - 138M
  - 53M
Results: Primary SD card

<table>
<thead>
<tr>
<th>Devices with insecure deletion (%)</th>
<th>30M</th>
<th>340M</th>
</tr>
</thead>
<tbody>
<tr>
<td>Froyo (v2.2.x)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>GB (v2.3.x)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICS (v4.0.x)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>JB (v4.[1-3])</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

format() for (format())

ioctl(BLKDISCARD) for (ioctl(BLKDISCARD))

138M

159M
Results: Secondary SD card

Not supported in AOSP code
Talk outline

- Background
- Methodology
- Results
- Practical recovery
- FR alternatives
Practical Recovery

- Contact (Facebook, Phonebook, WhatsApp, etc)
- Conversation (emails, SMSs, Facebook & WhatsApp chats, etc)
- Browsing history
- Credentials (Facebook cookies, etc)
- Multimedia
Practical Recovery (Cont'ed)

• Android (master) auth token(s)
• Master token can be used to get other tokens from Google
• Tokens recovered 100% of the time, master one 80%
Talk outline

- Background
- Methodology
- Results
- Practical recovery
- FR alternatives
Alternatives to built-in FR

- Overwrite bit-by-bit: one pass enough to provide logical sanitisation
- Filling unallocated space (create files) to overwrite: discarded because:
  - Extra level of indirection
  - File systems vary (ext4, FAT, FUSE, Samsung's proprietary RFS)
Alternatives to built-in FR (Cont'ed)

- Full Disk Encryption (FDE), >= ICS only (v4.0.x)
  => not possible on GB (2.3.x) vulnerable devices
- Only support for data partition
- Encryption key stored encrypted using user's PIN in so called "crypto footer"
  - Crypto footer not sanitised with flawed FR
  - Crypto footer allows PIN brute-force
- Android lollipop (5.x): default encryption has hardcoded password "default_password"
Alternatives to built-in FR (Cont'ed)

• Mobile Anti-Virus (MAV) apps with "remote wipe" function

• 10 most downloaded Mobile Anti Virus (MAV) apps on Google Play
  • AVG, Lookout, Avast, Dr.web, Norton, McAFeef, Kaspersky, TrustGo, TrendMicro, Avira

• Mostly use built-in Factory Reset through Android API => not an alternative
Example: Lookout implementation

- Overwrites files and unlinks them
- Dev assume file update occurs "in-place"
- On Galaxy S Plus, FAT-formatted primary SD: >90% data recoverable
- Details about other apps' implementation available in paper on my webpage.
Conclusion

- Android FR has problems but getting better
- Android code, vendors' customisations and lack of proper testing
- Mostly available on the second-hand market NOW
- Paper provides engineering design suggestions to reduce this problem in future handsets. Have a look!
Thanks!

Laurent Simon

lmrs2@cam.ac.uk
https://www.cl.cam.ac.uk/~lmrs2/