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
  - (primary)

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

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

=> memory management, wear-leveling algo

blocks used by file system

data 1

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

blocks used by file system

data 2

clean blocks
to-be-erased dirty blocks

data’ data” data 1
Flash Memory – File Systems

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

File system

<table>
<thead>
<tr>
<th>Device driver</th>
<th>N</th>
<th>N+1</th>
<th>N+2</th>
<th>N+3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flash memory</td>
<td>N</td>
<td>N+1</td>
<td>N+2</td>
<td>N+3</td>
</tr>
</tbody>
</table>

yaffs2

MTD device

<table>
<thead>
<tr>
<th>MTD device</th>
<th>N</th>
<th>N+1</th>
<th>N+2</th>
<th>N+3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block device</td>
<td>N</td>
<td>N+1</td>
<td>N+2</td>
<td>N+3</td>
</tr>
</tbody>
</table>

Mapping after overwrite of block N

Original block mapping

[Diagram showing the mapping and interaction between the device driver, controller, and 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
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

- Devices with insecure deletion (%)
  - Froyo (v2.2.x)
  - GB (v2.3.x)
  - ICS (v4.0.x)
  - JB (v4.[1-3])

- Data sizes:
  - 295M
  - 138M
  - 53M

- Commands used:
  - ioctl(MEMERASE)
  - ioctl(BLK SEC DISCARD)
Results: Data partition (Cont'ed)

- Upgrade from GB (2.3.x) to ICS (4.0.x)
  - ioctl(BLKSECDISCARD) return errno 95 EOPNOTSUPP
- 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): 0M
- GB (v2.3.x)
  - ioctl(BLKSEC DISCARD): 295M
- ICS (v4.0.x)
  - ioctl(BLKSEC DISCARD): 138M
- JB (v4.[1-3])
  - ioctl(BLKSEC DISCARD): 53M
Results: Primary SD card

Devices with insecure deletion (%)

<table>
<thead>
<tr>
<th>Device</th>
<th>Froyo (v2.2.x)</th>
<th>GB (v2.3.x)</th>
<th>ICS (v4.0.x)</th>
<th>JB (v4.[1-3])</th>
</tr>
</thead>
<tbody>
<tr>
<td>Format</td>
<td>100</td>
<td>74</td>
<td>138</td>
<td>159</td>
</tr>
<tr>
<td>ioctl</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BLKDISCARD</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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%

username@gmail.comcom.googleAFcb4KRs88NZlzN-r6qHrSHGF1Twyh...TKw==
c1DQAAAJ4AAABQPfQhNXLTDDYDLgHoIFDdDIEoJBokYr_6ad0WeSr2kVpK4...B-0pd
androidmarketDQAAAJ8AAAD1NNQaeO_yxfgN MtSvnQVangE3DAat1KtTo...INkZV
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
- Ony 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"
Conclusion

- Android FR in messy state
- Android code, vendors' customisations and lack of proper testing
- Mostly available on the second-hand market
- 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/