Implications of Circular Economy on Users Data Privacy:

A Case Study on Android Smartphones Second-Hand Market

D. Nguyen, S. Martinez & M. Khramova

Presentation by Juho Pörhönen,
Research Manager, Blancco Tech. Group

November 29th 2018

Motivations

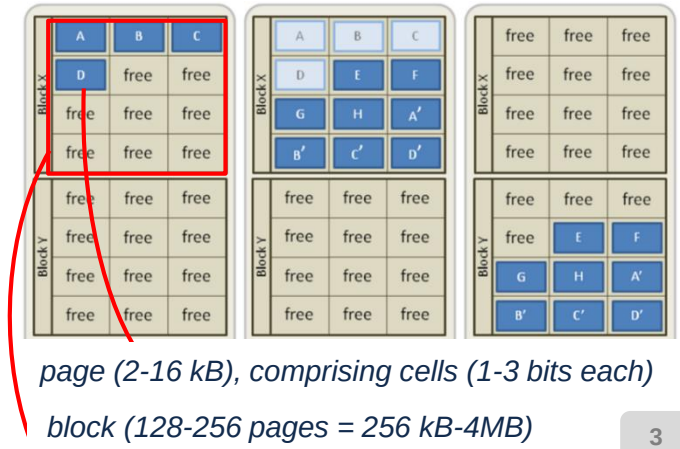
- According to an estimate, up to 89% of mobile devices end up in the landfill in US (in 2010) [1]
- Mobile devices contain rare metals [5] and recyclable components
- Second-hand phone market estimated to reach 222.6 million units by 2020 [10]
- Fear of personal data misuse is a major inhibitor for recycling of mobile devices [20, 22]
- Previous studies have focused on devices purchased from online trading platforms, such as Amazon, eBay, Craigslist, Gazelle [35, 37, 38]

Why Android?

- Dominance over the European mobile phone market (over 80% in 2017)
- Majority of Android devices still employ flash memory that is non self-encrypting
- Ecosystem is non-proprietary, making it easy to find out information on how to bypass the flash controller

About flash memory…

- Fundamentally different operation principle and hierarchical structure in comparison to conventional HDDs
- Inherent shortcomings:
  - Read operations (25-100 us latency) performed on "page" level
  - Write operations (250-1500 us) performed on page level, only if surrounding cells empty, otherwise the entire block first has to be copied, then erased and re-written
  - Erase operations (1500-5000 us) may only be performed on "block" level
  - NAND flash cells limited to only 10,000 write-cycles before they start losing charge
- Compensation by internal operations (run independently by the flash controller):
  - **Flash translation layer**: instead of erasing an entire block, only mapping is changed (eventually erased by "Garbage collection" function)
  - **Wear-leveling**: instead of overwrite, new blocks are written on least-used memory cells
  - **Over provisioning**: worn-out blocks may be moved to this "invisible" extra space



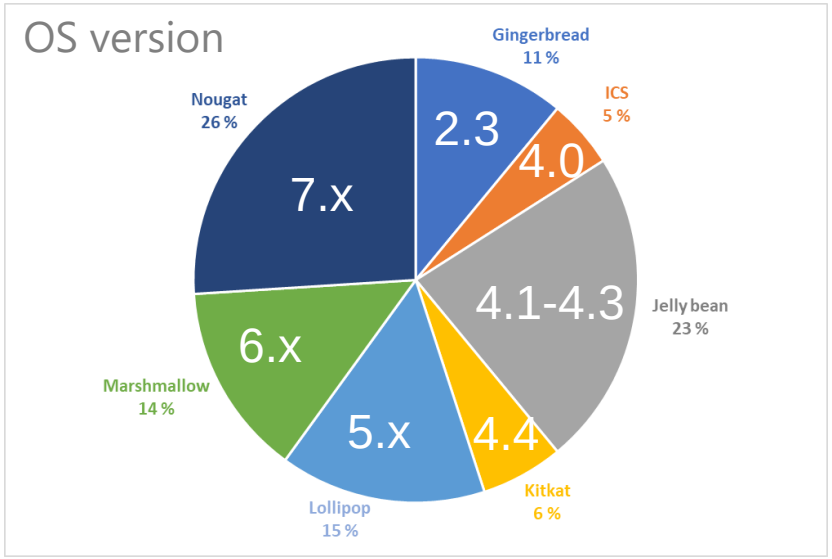
page (2-16 kB), comprising cells (1-3 bits each)

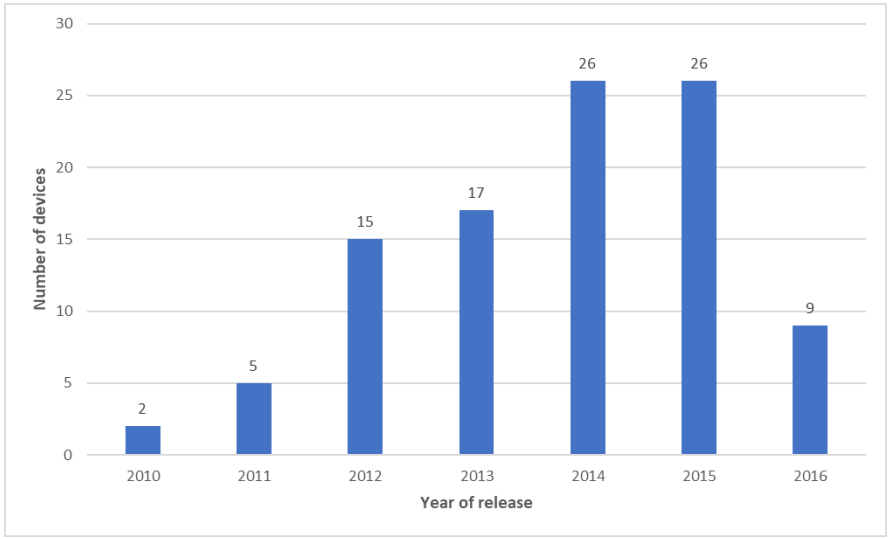
block (128-256 pages = 256 kB-4MB)

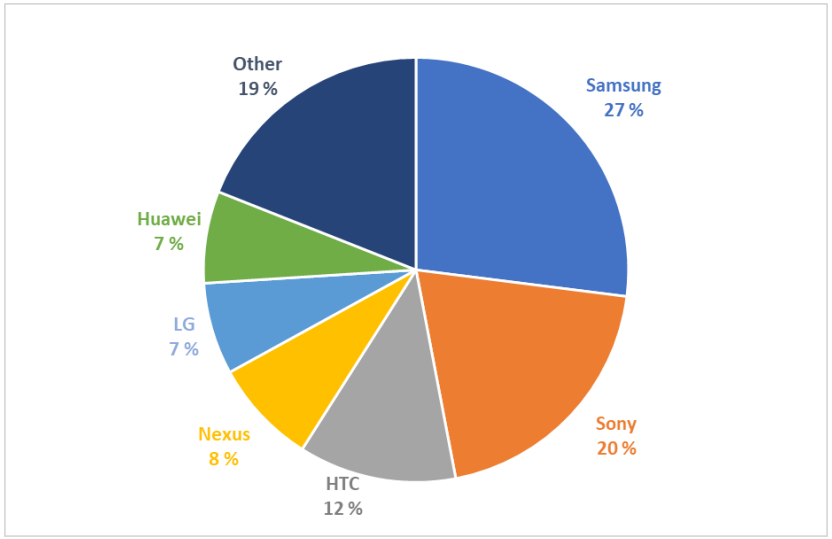
Source: "How Do SSDs Work?", Extremetech.com

Methodology (1/2)

- Sample set of 100 smartphones representative of the European second-hand market
- Smartphones acquired directly from three different IT Asset Disposition service providers between October 2016 and July 2017

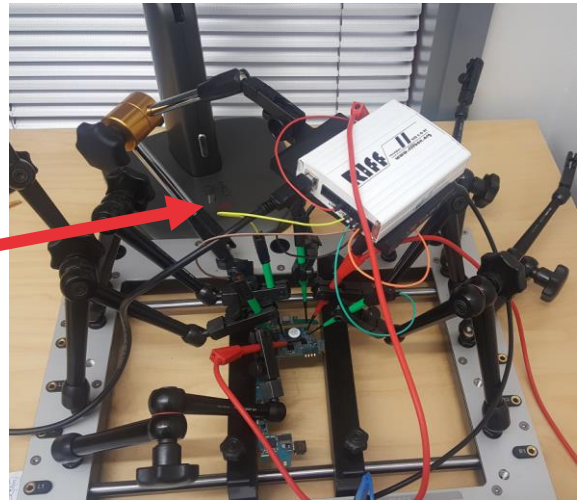




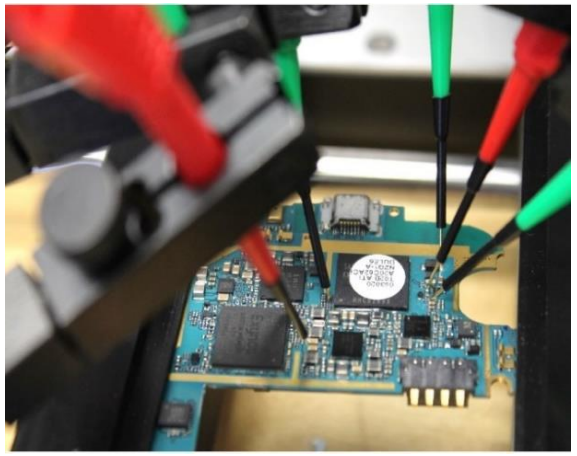


Methodology (2/2)

- Test procedure:
    1. Accessing files through user interface
    2. Acquiring a binary image of the memory
        i. Commercial forensic tools (non-invasive)
        ii. RIFF Box + JTAG Manager (invasive)
    3. Analysis of extracted image (-> logical data)
        - Commercial forensic tools or binary viewer
    4. Categorization of the logical data



- *Note: The used test setup is easily accessible at a low cost*
    - *RIFF Box 2: price on Amazon ~100€*
    - *Test stand: price online ~1000€*
    - *Commercial forensic software tools: free demo versions available online*
    - *JTAG mapping (pinouts) for various models also available on online tech forums*



Results

- Data was recovered from 19 out of the 100 devices
- This data was classified according to type and sensitivity
  - Non-critical: SMS, call logs and contacts from the carriers only
  - Critical: Corporate data and personal data identifying the previous user and/or location (also social media account information found)

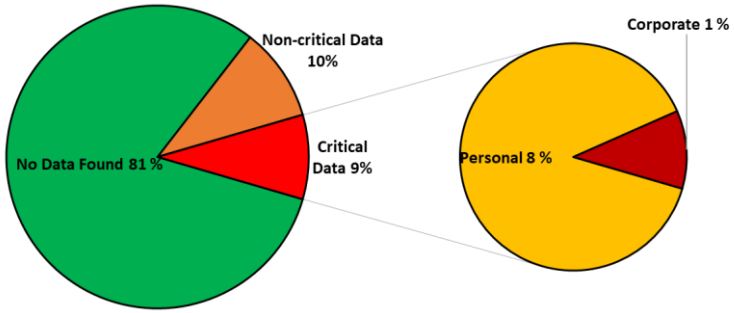


Table II
CLASSIFICATION OF RECOVERED DATA

Category	Data	Sensitivity
Entertainment	Music, Videos	Low
Photographic	Pictures	High
Documents	Excel, Word, PDF	Low
Messaging	SMS, MMS, WhatsApp	High
Call logs	Incoming, Outgoing	Low
Emails	Personal, Corporate	High
Internet	History, Cookies, Bookmarks	Low
Passwords	Accounts, Wi-Fi	High

Table III
ANALYSIS OF RECOVERED DATA

Type of data	Number of devices	Ratio
Browser	3	5.66%
Call logs	5	9.43%
Contacts	9	16.98%
Documents	3	5.66%
Emails	2	3.77%
Pictures	11	20.75%
MMS	2	3.77%
Music	1	1.89%
SMS	10	18.87%
Video	2	3.77%
WhatsApp	3	5.66%
Wi-Fi Passwords	2	3.77%

Conclusions

- While IT asset disposal (ITAD) facilities claim to implement a data sanitization process, a significant percentage (19%) of the devices still store user data
  - To be fair, this may result from human factors in the process
  - In comparison, our previous study [38] on second-hand mobile devices purchased from online trade platforms suggests that even higher percentage (35%) of the devices sold online in US, Germany and UK contain user data

- Critical data left behind (in 9% of the devices) includes personal information, making it possible to identify the previous user and his/her whereabouts in 7% of the cases, enabling identity theft and blackmailing
  - This data is accessible at a low cost and with little effort

- In conclusion, commonly used data sanitization processes need further investigation
  - Based on this study, the effectiveness of data recovery did not seem to depend on the OS version, as data was found up to OS 6.0 devices

References

[1] Green Aliance, A circular economy for smart devices Opportunities in the US, UK and India.

[5] Takahashi, K.I., M. Tsuda, J. Nakamura, K. Otabe, M. Tsuruoka, Y. Matsuno and Y. Adachi (2008), Elementary Analysis of Mobile Phones for Optimizing End-of-Life Scenarios, Journal of Environmental Science 20:1403-1408.

[10] IDC, Worldwide Market for Used Smartphones Forecast to Grow to 222.6 Million Units in 2020, According to IDC, FRAMINGHAM, Mass. November 21, 2016.

[20] M.J. Welfens, J. Normann, A. Seibt, Drivers and barriers to return and recycling of mobile phones, Case studies of communication and collection campaigns, Journal of Cleaner Production, 2015

[22] J. Ylä-Mella, R.L. Keiski, E. Pongracz, Electronic waste recovery in Finland: Consumers' perceptions towards recycling and re-use of mobile phones

[35] S. Diesburg, C.A. Feldhaus, M. Al Fardan, N. Ploof, J. Schlicht, Is Your Data Gone? Measuring User Perceptions of Deletion

[37] How Avast recovered 'erased' data from used Android phones, Avast 2014

[38] Privacy for sale. A study on data security in used mobile devices & hard drives, Blancco

blancco
technology group

Thank you for your attention!

Analysis of data remanence after Factory Reset, and sophisticated attacks on memory chips

D. Nguyen, S. Martinez & M. Khramova

Presentation by Juho Pörhönen,
Research Manager, Blancco Tech. Group

November 29th 2018

Motivations

- As data suggests, a significant percentage of the devices circulating in the European second hand market still store user data, even after going through the proper channels
- No up-to-date information available on effectiveness of common sanitization methods
    - The most common method being the reset function built into most operating systems

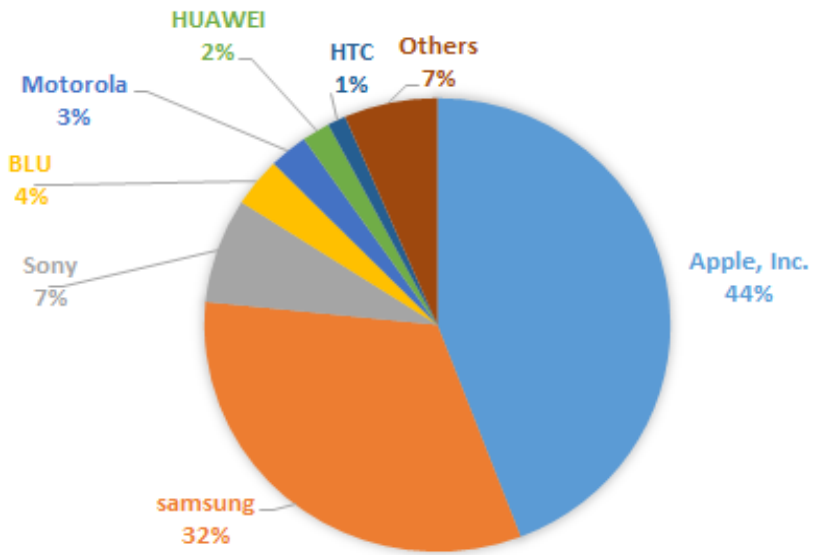
Why Android?

- Dominance over the European mobile phone market (over 80% in 2017)
- Provides in-built Factory Reset function, which is the "de facto" method for data sanitization
    - Previous studies from 2015 [8, 9] suggest this function is not sanitizing data properly, however, a sample set representative of the 2nd hand market was not provided

Period	Android	iOS	Windows	Others
2016 Q1	83.4%	15.4%	0.8%	0.4%
2016 Q2	87.6%	11.7%	0.4%	0.3%
2016 Q3	86.8%	12.5%	0.3%	0.4%
2016 Q4	81.4%	18.2%	0.2%	0.2%
2017 Q1	85.0%	14.7%	0.1%	0.1%

Methodology (1/2)

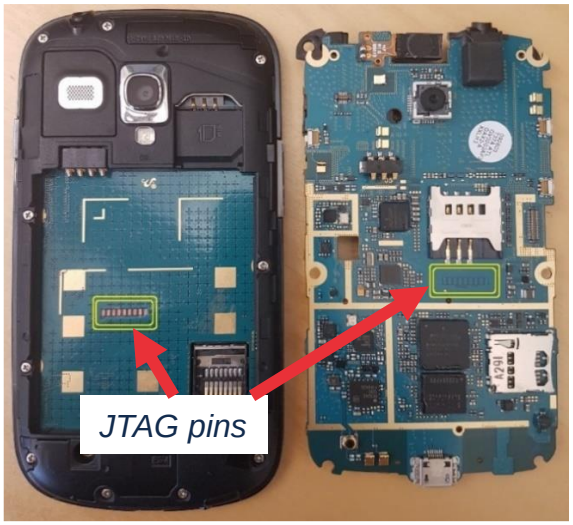
- Sample set of 68 Android smartphones representative of the European second-hand market
  - From every vendor we picked up the most popular models
  - phones purchased from 2nd hand phone re-furbishers



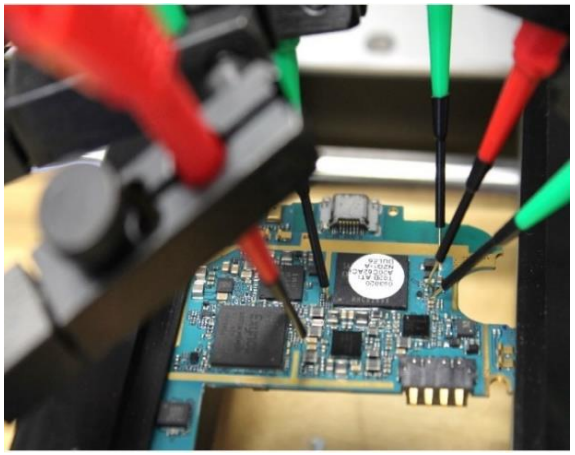
	Model	OS version		Model	OS version
1.	AG Mobile Chrome Selfie	4.4.2	35.	Samsung Galaxy S III I9300	4.3
2.	AG Mobile Ghost	5.0.2	36.	Samsung Galaxy S III I9300	4.1.2
3.	Asus Memo Pad HD7 (ME173X) 16GB	4.2.2	37.	Samsung Galaxy S III Mini i8190	4.1.2
4.	Asus Zenpad	5.0.2	38.	Samsung Galaxy S III Mini i8200N	4.2.2
5.	CAT B15	4.1.2	39.	Samsung Galaxy S Plus	2.3.6
6.	FairPhone 2	6.0.1	40.	Samsung Galaxy S2 I9100	4.1.2
7.	HTC Desire 310	4.2.2	41.	Samsung Galaxy S4 I9505	5.0.1
8.	HTC Desire 620	4.4.4	42.	Samsung Galaxy S4 Mini I9195 LTE	4.2.2
9.	HTC Desire C	4.0.3	43.	Samsung Galaxy S5 (SM-G900F)	5.0
10.	HTC Desire S	4.0.3	44.	Samsung Galaxy S5 Mini G800F	5.1.1
11.	HTC Desire X	4.1.1	45.	Samsung Galaxy S6 (SM-G920F)	6.0.1
12.	HTC One M7	5.0.2	46.	Samsung Galaxy Tab 3 7.0 (SM-T211)	4.4.2
13.	HTC One M8	6.0	47.	Samsung Galaxy Trend 2	4.4.2
14.	HTC One Mini 2	4.4.2	48.	Samsung Galaxy XCover	2.3.6
15.	Huawei Ascend G620S	4.4.4	49.	Samsung Galaxy Y Pro (GT-B5510)	2.3.6
16.	Huawei Y6	5.1.1	50.	Samsung i8160 Galaxy Ace 2	4.1.2
17.	Lenovo IdeaTab 2	4.4.2	51.	Samsung S5830 Galaxy Ace	2.3.6
18.	LG G flex2 (LG-H955)	5.1.1	52.	Samsung XCover II (S7710)	4.1.2
19.	LG G2 (LG-D802)	4.2.2	53.	Sony Xperia Go	4.1.2
20.	LG G3 D855	5.0	54.	Sony Xperia J	4.1.2
21.	LG G4 H815	6.0	55.	Sony Xperia M2	5.1.1
22.	LG V10 32GB	6.0	56.	Sony Xperia M2 Aqua	5.1.1
23.	Motorola Moto G (XT-1039)	4.4.4.	57.	Sony Xperia SL	4.1.2
24.	Motorola Moto G 3rd	6.0.1	58.	Sony Xperia SP	4.3
25.	Motorola Moto G4	7.0	59.	Sony Xperia Tipo	4.0.4
26.	Motorola Moto X 2nd	5.0	60.	Sony Xperia U	2.3.7
27.	Nexus 1	2.3.6	61.	Sony Xperia Z1	5.1.1
28.	Nexus 4 (LG-E960)	5.1.1	62.	Sony Xperia Z1 Compact	5.1.1
29.	OnePlus One (A0001)	6.0.1	63.	Sony Xperia Z2	5.1.1
30.	Samsung A5 (SM-A500FU)	6.0.1	64.	Sony Xperia Z3 Compact	5.0.2
31.	Samsung Galaxy Note N7000	4.1.2	65.	Xiaomi Redmi 3	5.1.1
32.	Samsung Galaxy Note3 (SM-N9005)	5.0	66.	ZTE Blade	2.3.5
33.	Samsung Galaxy Note4 (SM-N910F)	6.0.1	67.	ZTE Blade V6 Lite	5.1
34.	Samsung Galaxy S	2.3.6	68.	ZTE Skate	2.3.5

Methodology (2/2)

- In-house test procedure:
    1. Acquiring a binary image of the memory
        i. Commercial forensic tools (non-invasive)
        ii. RIFF Box + JTAG Manager (invasive)
    2. Analysis of extracted image (-> logical data)
        - Commercial forensic tools or binary viewer
    3. Categorization of the logical data

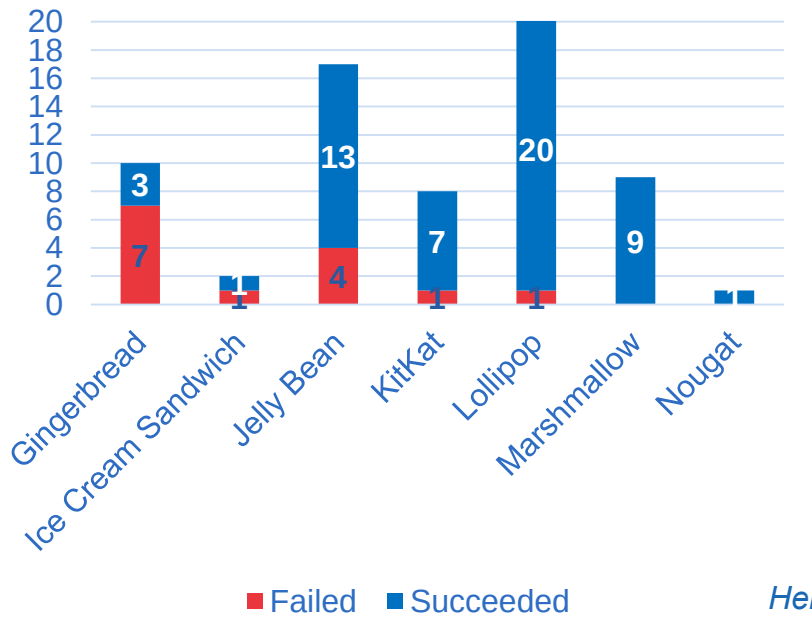


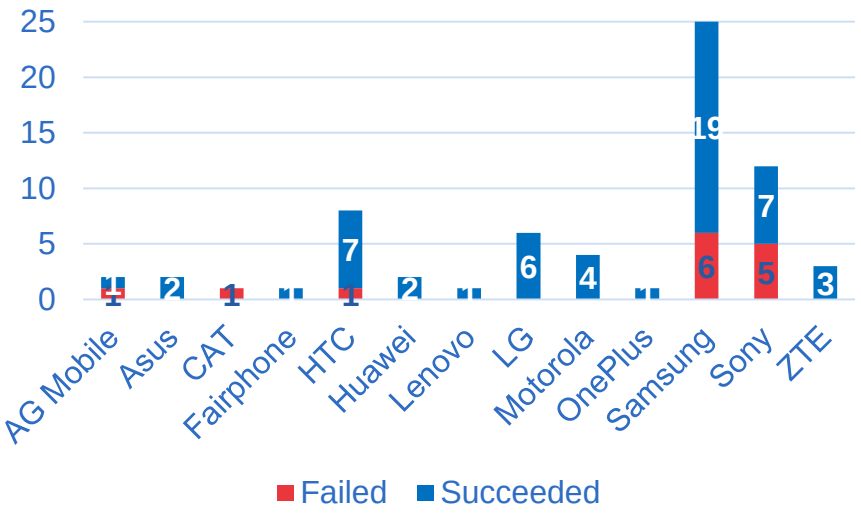
- Forensic laboratory testing
    - Two smartphones of the most popular model where we no data was recovered in-house were sent out to an external laboratory for sophisticated analysis



Results

- User data was recovered from devices up to Android OS 5.0.1 (Lollipop)
  - 10 out of 14 devices failing to erase data after Factory Reset use eMMC, which represents vast majority of the market
  - Otherwise the amount of recovered data varies depending memory type, phone model, OS version, manufacturer





Here "failed" means failed factory reset in terms of data erasure.

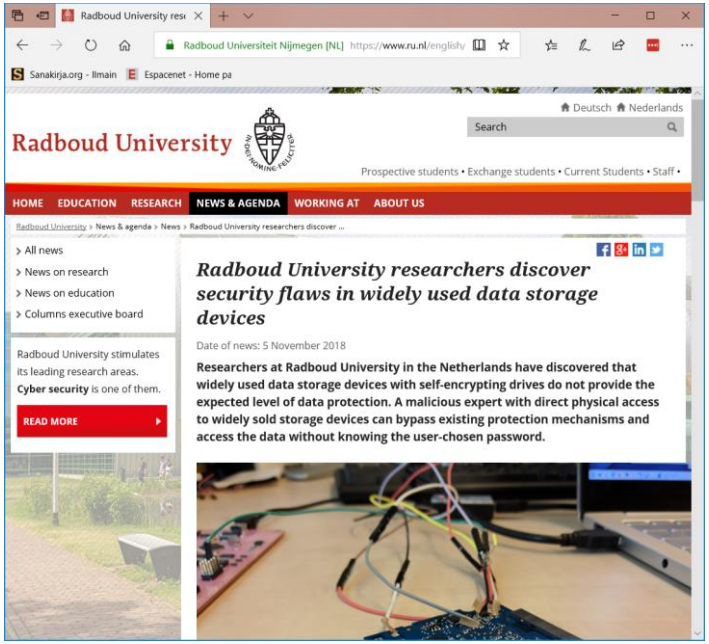
Conclusions

- Factory Reset is failing to permanently erase user data on the smartphones running on Android OS 2.3 (Gingerbread) to 5.x (Lollipop)
  - Results suggest that data is more easy to recover from older Android versions (but not impossible on later ones either)
  - Further, results suggest that data is more easy to recover from old NAND technology (OneNAND > eMMC > UFS)

- Also, data not accessible otherwise may be accessed by bypassing the controller
  - Access to data that hidden by the controller (e.g. removed block mapping information)

Further discussion

- Android OS 6 employs hardware encryption, depending on the device performance [1], while Android OS 7 always employs hardware encryption [2]
- **Will the data privacy issue in second-hand devices be resolved, as hardware encryption becomes commonplace?**
  - No. Encrypted data still exists on the device, unless it is erased. Recovering the data "only" requires an extra step of recovering the encryption key from the flash controller



This vulnerability was demonstrated with BitLocker used in conjunction with self-encrypting SSD, however, the same principle also applies to other security systems that rely on self-encrypting flash memory (AES-128/256 algorithm)!

References

[1] Android 6.0 Compatibility Definition. 2015. Available at:

https://source.android.com/compatibility/6.0/android-6.0-cdd

[2] Android 7.0 Compatibility Definition. 2015. Available at:

https://source.android.com/compatibility/7.0/android-7.0-cdd

[8] ADISA, "Forensic Analysis of Smartphone Factory Reset Function," 20 05 2015. Available:

https://www.informationsecuritybuzz.com/articles/forensic-analysis-of-smartphone-factory-reset-function/

[9] L. Simon and R. Anderson, "Security Analysis of Android Factory Resets," 2015. Available:

https://www.cl.cam.ac.uk/~rja14/Papers/fr_most15.pdf

blancco
technology group

Thank you for your attention!