ADISA
ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

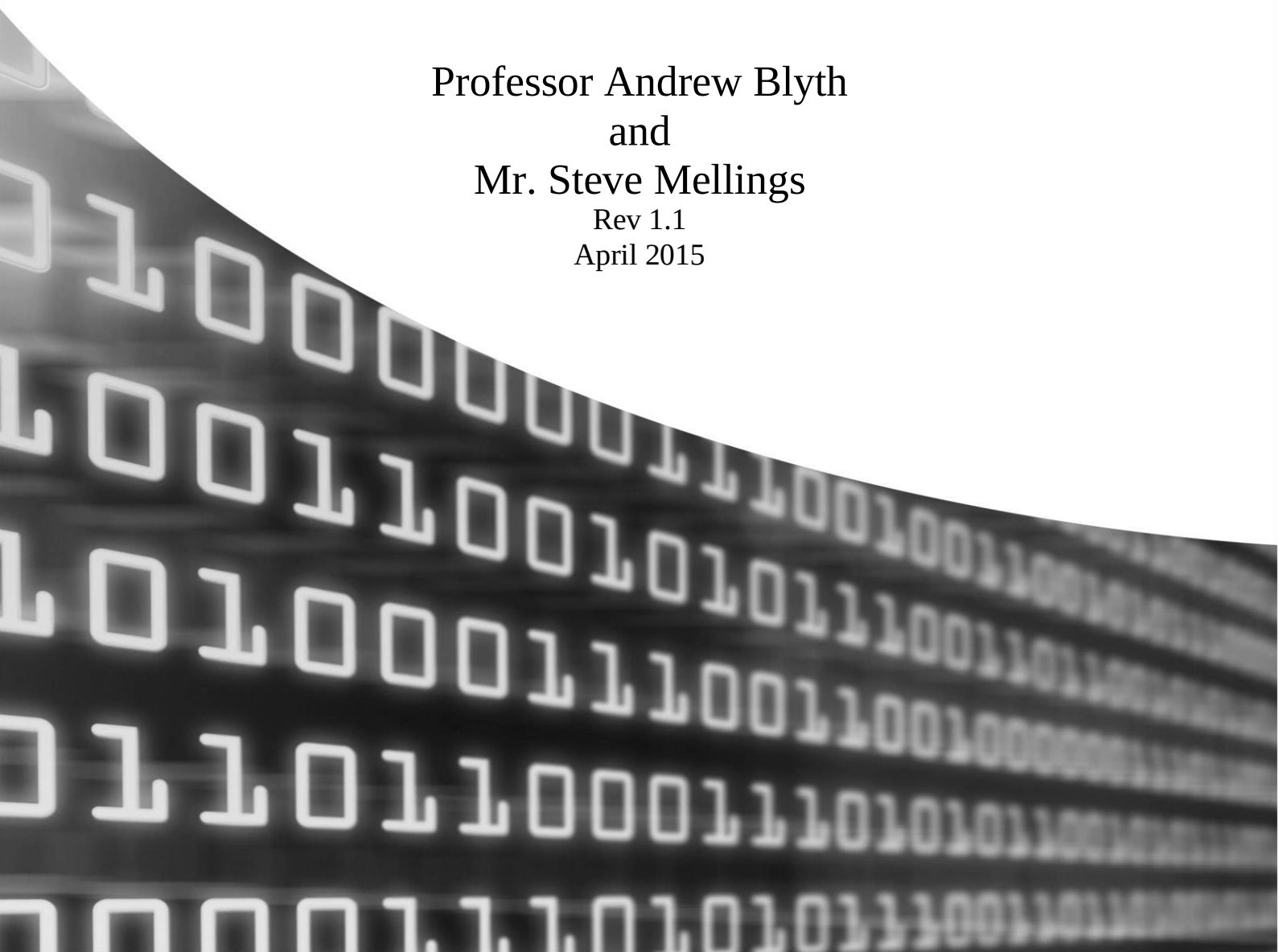
University of South Wales
Prifysgol De Cymru

WHITE PAPER

Forensic Analysis of Factory Reset Function as a permissible means of sanitising data on smartphones.

Professor Andrew Blyth
and
Mr. Steve Mellings

Rev 1.1
April 2015



Abstract

The goal of this paper is to examine the assertion that the factory reset function as specified and supported by BlackBerry, Apple and Android (HTC/Samsung) erases data such that a threat actor function at risk level 1/2 is unable to recover any data. The research method utilised to explore this hypothesis is a quantitative one, where by structured data was placed on a device, the factory reset was then performed on the device and finally the device was analysed using standard COTS (commercial off-the-shelf) tools.

Introduction

The growth of the Internet and high-speed networking has created the ability for people to access many different types of content on mobile devices, such as mobile phones and tablets. While this increased usage has allowed people to work in a more agile manner, it has created security concerns relating to the management, and ease of access, of the content on these devices.

Applications such as British Gas' Hive allow a user to manage their home heating from a smartphone. Applications such as MySafe allow a user to manage their home security, while applications such as Facebook, Twitter, and Google allow people to manage their social media and repository of significant personal information. Research has shown that residual data can be found on phones in the second hand market [4,5], and that through this data it is possible to identify user behaviour [1,2].

Although best practice has emerged for mobile phone forensics [6], it is true to say that no best practice has emerged for the data sanitisation of mobile phones. While studies have been undertaken examining the forensic recovery techniques for particular operating systems such as Microsoft Windows [3], no studies have been performed examining the ability of the factory reset function to forensically erase data.

This has resulted in many claims being made relating to the ease with which data can be recovered from a mobile phone [3] after the in-built factory reset function has been invoked. The goal of this paper is to explore the ability to forensically recover data from various 3G/4G devices with a view of offering businesses and users advice on how best to protect their personal information when such handsets are disposed of.

A sample of 24 handsets was supplied by the hardware partner. These handsets represented the most common makes and models found in the disposal channel at present and also represented the three main operating systems in place, namely BlackBerry, iOS, and Android. In this paper we will examine the ability of the factory reset to render the data unrecoverable using standard forensic tools. The following is a table of the devices that were analysed.

Mobile Phone Make/Model	Mobile Phone Make/Model
BlackBerry Bold Touch 9900	BlackBerry Torch 9810
BlackBerry Curve 8320	BlackBerry Pearl 8120
BlackBerry Curve 8900	BlackBerry Torch 9800
BlackBerry Curve 9320	BlackBerry Pearl 8110
BlackBerry Curve 8520	BlackBerry 8800
BlackBerry Curve 8310	BlackBerry Pearl 9105
BlackBerry Bold 9700	Apple iPhone 3G
Apple iPhone 3GS	Apple iPhone 4
Apple iPhone 4S	Apple iPhone 5

Apple iPhone 5C	Apple iPhone 5S
HTC Wildfire	HTC Wildfire S
Samsung Galaxy Ace 2 i8160	Samsung i8190 Galaxy S III Mini
HTC ChaCha	Samsung i9100 Galaxy S II

Table 1 – Makes and Models of 3G/4G Devices

To facilitate in the measurement of the ability to recover data from a device it is important that we benchmark the forensic capability against which the handset will be tested. For the purposes of this paper the ADISA Threat Matrix was utilised and Threat Actor Capability and Compromise Methods Levels 1 and 2 were used as the forensic benchmark.

Risk Level	Threat Actor Capability and Compromise Methods
1	Casual or opportunistic threat actor only able to mount high-level non-invasive and non-destructive software attacks utilising freeware, OS tools and COTS products.
2	Commercial data recovery organisation able to mount non-invasive and non-destructive software attacks and hardware attacks.
3	Commercial computer forensics organisation able to mount both non-invasive/non-destructive and invasive/non-destructive software and hardware attack, utilising COTS products.
4	Commercial computer forensics organisation able to mount both non-invasive/non-destructive and invasive/destructive software and hardware attack, utilising COTS products.
5	Government-sponsored organisations using advanced techniques to mount all types of software and hardware attacks with unlimited time and resources to recover sanitised data.

Table 2 - Threat Actor Capability and Compromise Methods

Methodology

The Methodology

A number of devices of each type were received and checked for functionality. Prior to the start of the experiment each device was given a full battery charge and was then placed onto a stable (known) state via the execution of the factory reset function. The following defines the test methodology:

- Using the standard forensic toolset a forensically sound image of the device was taken.
- A sim card was placed into the handset to allow the handset to fully function as a 3G/4G device. Some handsets were locked to a specific network operator so the following list of network operators were used - O2, EE, Vodafone. The handset was then powered on and allowed to create a network connection. The handset was connected to a Wi-Fi network using a set of predefined credentials.
- Data was then placed on the phone as follows, using the internal applications for each device:
    - Using the internal camera, a series of 25 predefined photos were taken.
    - Using the internal camera, a series of five predefined videos were taken.

    - Using the internal contacts application a series of 10 predefined contacts were placed on the device.
    - Using the internal calendar a series of 10, one hour in length, appointments were scheduled.
    - Using the internal SMS/MMS messaging application, a series of 10 predefined messages were sent and received.
    - Using the internal Phone application, a series of five predefined phone calls were made.
    - Using the Wi-Fi connection and the internal Internet Browser application a series of two predefined Google searches were made, and for each search one click through was made.
    - The device was then connected to the computer and a known WAV file uploaded to the device. Using the internal audio player the WAV file was played to ensure the validity of the file.
- Once all of the data had been placed on the device, the device underwent a power cycle. At that stage a forensically sound image was taken of the device. This image was then utilised to ensure that all of the data placed on the device was present.
- Then for each type of device the factory reset function was executed in accordance with the manufacturer's guidelines, and at the end of this the device was power cycled.
- The device was then forensically imaged to produce a forensically sound image, and each image was analysed as follows:
    - Using Cellbrite UFED Physical Analyzer Version 3.8.7.7, the image was inspected for the presence of the following data types:
        - Images/Movies, Calendar, Contacts, Audio, SMS/MMS and Phone.
    - Using Cellbrite UFED Physical Analyzer Version 3.8.7.7, the image was then data mined for the following data types:
        - Images/Movies, Calendar, Contacts, Audio, SMS and Phone.
    - Using data carving tool Blade Version 1.9.12045.05, the forensic image was analysed for the following data types:
        - Compressed Files (GZIP, RAR and ZIP), File Types (PDF and RTF), E-Mail Types (Outlook and Microsoft Mail), Microsoft Office (2003 and 2007).
        - Sound Files (MP3 and WAV), Movies (Flash, AVI, MPEG and Windows Media), Internet (HTML and XML).

The Imaging Process

The image of each device was conducted in accordance with a strict set of rules. Each device was treated as a forensic artefact and processed accordingly. The imaging progress was such that each device was connected to Cellbrite UFED (version 2.2.5.4) via the correct physical data connector. Then, via a USB connector, the UFED device was connected to the PC running Windows 7. The UFED device functions as a client providing data from the phone to the imaging software running on the PC (UFED Logical Analyzer 3.8.7.7.). The UFED device functions as a write blocker ensuring that no data is written back to the device. Where possible each device was physically imaged, and when a physically image was not possible then a logical image of the device was taken.

Results

Mobile Phone Make/Model	Data Acquisition Method	Data on Phone
BlackBerry Bold 9900	Physical	No
BlackBerry Torch 9810	Physical	No
BlackBerry Pearl 8120	Physical	No
BlackBerry Curve 8900	Physical	No
BlackBerry Curve 8320	Physical	No
BlackBerry Torch 9800	Physical	No
BlackBerry Curve 9320	Logical	No
BlackBerry Pearl 8110	Physical	No
BlackBerry 8800	Logical	No
BlackBerry Curve 8310	Physical	No
BlackBerry Pearl 9105	Physical	No
Apple iPhone 3G	Physical	No
Apple iPhone 3GS	Physical	No
Apple iPhone 4	Physical	No
Apple iPhone 4S	Physical	No
Apple iPhone 5	Physical	No
Apple iPhone 5S	Physical	No
Apple iPhone 5C	Physical	No
Samsung i8160	Physical	Yes
Samsung i8190	Physical	Yes
HTC Wildfire S	Physical	Yes
HTC Wildfire	Physical	Yes
HTC ChaCha	Physical	Yes
Samsung i9100 Galaxy S2	Physical	Yes

Table 3 – Makes and Modules of 3G/4G Devices

The data recovered from the Android devices included the following:

- Phone Book/Contacts.
- SMS, MMS and IM.
- Calendar.
- Call Logs.
- Pictures, Video, Audio/Music.
- Apps and App Data.

Results Summary and Conclusions

In summary, the factory reset function, when performed on the sample of BlackBerry and Apple devices, erases the user data from the device such that using standard forensic tools and techniques it is impossible to recover the data. This concludes that from a data sanitisation point of view the factory reset function, when performed on BlackBerry and Apple devices, is sufficient. It can be speculated that this is due to the fact that both BlackBerry and Apple control both the hardware and software platforms for their devices and as such, the software platform will be integrated into the hardware platform so as to support specific functions.

However, the story with the Android devices is very different. The research findings show that the factory reset function, when performed on certain Android devices is not sufficient and that data can be recovered. In fact, the data recovered would indicate that even multiple factory resets would not be enough to erase all of the data. The reason for this conclusion is that forensic analysis of the Android devices showed that some of the devices still contained data from instant messaging services, and from the test methodology point of view no instant messaging services data was placed on the phone. It can be speculated that the poor performance of the Android devices is that as Android runs on multiple hardware platforms, the developers of Android are unable to integrate their software platform into the hardware such that specific hardware features cannot be utilised.

Best Practice Recommendations when Disposing of Smart Phones

The act of sanitising data is the final stage in the smartphone disposal process but the greatest issue is how to ensure the device actually makes it to the point where it is sanitised. As such it is recommended that the risk from poor asset management is viewed as an equal threat to the failure of a particular sanitisation technique. For this reason this paper includes some further best practice recommendations to follow when disposing of smartphones.

For low volume disposal processes such as individual users, then the factory reset function on the BlackBerry and Apple devices tested would be viewed as acceptable to protect personal data. For low volume disposal processes on Android handsets it is recommended to look at alternative external sanitisation methods such as proven software overwriting tools or physical destruction of the device. Both of these options introduce different risks as currently there are no government approved mobile phone overwriting solutions, so a specification would be required which shows evidence of independent testing having been done on the chosen overwriting software. The software provider should also offer indemnity insurance against product failure and the company undertaking that on your behalf should also offer further assurances and provide a detailed audit trail. For physical destruction, there is an environmental and health and safety impact of the batteries (removable and integrated), which needs to be considered. Seek expert advice on the best means of destroying your device before simply applying a DIY destruction process.

For higher volume disposal projects such as from a business, the same logic listed above would apply, but the difficulty in tracking devices to be assured that the reset has been done on **every** handset would introduce a process variability which would leave a potential exposure against regulatory requirements. It is recommended to seek a specialist company to perform a controlled collect, audit and sanitise service such that all devices, regardless of the operating system, are inventoried using the IMEI number, undergo a sanitisation technique which offers indemnity assurance, and which results in an audit trail to show that the process was successful.

References

1. G. Grispos, W.B. Glisson, J.H. Pardue and M. Dickson (2014). *Identifying User Behavior from Residual Data in Cloud-based Synchronized Apps*. **Conference on Information Systems Applied Research (CONISAR 2014)**, 6–9 November 2014, Baltimore Maryland, USA.

2. W.B. Glisson and T. Storer, (2013). *Investigating Information Security Risks of Mobile Device Use within Organizations*, **AMCIS,** 2013.

3. G. Grispos, T. Storer, W.B. Glisson, *A comparison of forensic evidence recovery techniques for a windows mobile smart phone*, **Journal of Digital Investigation**, Volume 8, Issue 1, 2011, pp. 23–36.

4. T. Storer, W.B. Glisson and G. Grispos, (2010), *Investigating information recovered from re-sold mobile devices*, **ACM Privacy and Usability Methods Pow-Wow** (PUMP) Workshop, 2010.

5. P. Owen, P. Thomas and D. McPhee (2010), *An Analysis of the Digital Forensic Examination of Mobile Phones*, **Fourth International Conference on Next Generation Mobile Applications, Services and Technologies (NGMAST)**, 2010.

6. R. Ayers, S. Brothers and W. Jansen, (2014), *Guidelines on Mobile Device Forensics: Recommendations of the National Institute of Standards and Technology*, **NIST Special Publication 800–101**, Revision 1, 2013.

Acknowledgements

The test hardware utilised during this research project was kindly provided by ShP Limited of Morecambe, United Kingdom.