Discussing How Manufacturers' Focus on Device Security Can Hinder Mobile Forensic Investigations

Mairi MacLeod
CMP416: Digital Forensics
BSc(Hons) Ethical Hacking

This essay will address the issues that lie with manufacturers' focus on security. Specifically, how that presents a challenge to forensic analysts trying to gather evidence from mobile devices. Some of these security features addressed are; limiting the amount of accessable data when device is off, USB data connection being disabled and data encryption. This essay also looks into the differences between popular mobile devices and their operating systems. Along with how those differences may provide additional challenges for data extraction.

Mobile forensics is defined as "the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods" by the American government-owned organisation NIST (Ayers et al, 2014). Although mobile devices fall under the category of computers there are vast differences between traditional digital forensics and mobile forensics. The first of these differencies lies in the software used to gather data from the devices, with mobile forensics having less tooling options due to the difficulty of keeping up-to-date with all the new phone releases. As manufacturers are continuously releasing new mobile devices with updated hardware and software this makes it very difficult to maintain any form of tooling that can remain relevant after twelve months. Traditional digital forensics tends not to encounter this issue as hardware or software advancements that invalidate existing investigative methods are considerably less frequent and users tend not to replace computers or their components as frequently. Secondly, as will be mentioned more in-depth later in this paper, there are many unique complications with gathering data from a phone or tablet that are not present with a personal computer. These differences mean that investigators need to be trained separately in forensics for mobile devices before they can work on a case that requires data from such a device.

Although mobile phones have existed since the 1980s, smartphones really started their popularity in the late 2000s. This was in large part due to the introduction of the *iphone* and *Android* OS in 2007 and 2008 respectively. Both are classed as smartphones and often have very similar features but there are considerable differences between them. Popularity-wise *Android* has the lead boasting 87% of the global market share and there were around 1.4 billion being used in 2015. *Android* phones, often being the cheaper option, are more affordable for those on a lower income and thus increasing popularity in countries with a lower GDP per capita (Almehmadi and Batarfi, 2018 and MobileApps.com, 2020).

Android OS is a Linux-based operating system that is used by numerous phone manufacturers such as; Samsung, Huawei and Sony. The number of phones that use *Android* may also be a reason why it has the market share it does. As it was created from the Linux kernel much of it is open source and publicly available, the amount that is open source depends on the manufacturer as they may have patents or licenses for certain features. This is also why it is sometimes considered the more insecure out of the two OS' as it is far easier to create and download applications than on an *iphone*.

The *iphone* operating system is known as iOS and is currently on it's eleventh version. Created by Apple, in closed source for their *iPhone* and *iPad* products. As it is used exclusively on Apple devices it is famously not open source and applications not found on their 'app store' are not supported. Other phone operating systems are available, examples include *Symbian* and *Sailfish OS*, but *Android* and iOS are currently the most popular and widely used.

Due to the ever increasing popularity of smartphones and other mobile devices it is becoming more important for investigators to examine them for evidence. As the functionality and storage spaces increases in mobile users are storing more of their data on them, the days of phones being used exclusively for calling

and messaging are long gone. Modern devices act like a miniature computer and some of data that can be stored on a them includes; messages, images, browser history and location data. This functionality and portability has made phones the ideal devices for criminals and such devices have been used to assist with various crimes such as narcotics dealing, human-trafficking and child pornography (Almehmadi and Batarfi, 2018).

The acquisition of data there are five methods that can be used in mobile forensics; Manual, Logical, Hex Dumping and Joint Test Action Group (JTAG), chip-off and micro read. Often the first step attempted, manual acquisition is as the name implies where the investigator manually acquires data from the device. This can be done by taking photographs of the device, looking through e-mails, texts and contact lists as well as downloaded files and images. Unfortunately due to security features, such as passwords, very little data can actually be acquired at this stage of the investigation without the owner's consent. Logical acquisition uses software to extract the data stored on the device and send it to the forensic workstation for analysis. This stage is where most forensic tools operate and it works by sending commands to the device in order for it to send the data back.

Hex dumping and JTAG extraction methods will pull the raw data stored in flash memory of the device. Some tools are unable to gather all of the data stored in this area of memory and parsing it can be very time consuming. Hex dumping extraction software connects the device from a forensics workstation in order to send commands to gather the data stored in the flash memory. JTAG is similar but requires the device to be using JTAG-compliant components but can be used to gather data from devices that are locked or have deleted data. This uses a wired connection and creates an image from data stored in the microprocessor. The downside to JTAG over hex dumping is that it is far more invasive and requires some disassembly in order to access certain parts of the circuitry. If not done correctly the phone's CPU can be damaged and any further investigation impossible.

Chip-off is where the flash memory chip is physically removed from the device and put into a reader where contents extracted in the form of a binary image file. This is a difficult method of data extraction and investigators must be well trained and careful as to not damage the storage, which would jeopardise their ability to retrieve any data. Chip-off is truely a last resort as it destroys the device from which the chip is removed. Micro reading is even more low level than chip-off and reads the data from a device using an electron microscope which monitors the NAND and NOR chip. Due to the complexities of this approach it is very rarely performed and only as a last resort for very high profile cases (Ayers et al, 2014).

An important part of forensics is knowing where data is stored and what data is important. Most *Android* phones have six memory partitions, the most critical for forensics being /user data and /recovery. The former stores messages, contact information and data created by applications. /recovery as the name suggests is used to boot the phone into recovery mode when an error occurs when trying to start the device and allows the user to backup their data. This folder is not altered by applications when the phone is not being used in recovery mode so the data found inside is more difficult to change or remove. Due to this state being one where alteration or corruption is significantly reduced makes it very attractive for imaging the device. However, in order to retrieve the information stored in /user data the investigator must start the device normally and this can impact the integrity of some of the data (Almehmadi and Batarfi, 2018). With Apple devices due to the lack of knowledge surrounding the internal workings of iOS, understanding the file system is considerably more difficult. Other mobile OS and even different implementations of *Android* can also have different file structures which makes a one size fits all approach for imaging impossible.

Mobile device companies are very hesitant to provide backdoors or potential exploits for their devices, even to governments or for very serious cases. This is due to the fear that once created they may be exploited by malicious actors to steal their customers money or data. This means that researchers and investigators must try to come up with their own methods of data extraction whilst manufacturers continue to improve the security of their devices.

Due to the complexity of some of the data extraction methods, especially those which investigate the physical components of a device, keeping up-to-date with new phone releases can be difficult. With the large amount of time required to train a person in these methodologies it can be a considerable

undertaking to ensure that they can perform them on the most recent of devices. There are constantly new devices being put on the market, with some companies releasing multiple phones a year. Tooling used cannot be expected to updated as and when the components used in these devices are therefore it can be months or years before the equipment and training is available or even affordable. OS' tend to be updated less frequently but the security updates can provide additional challenges in data retrieval. A security feature on modern iOS devices disables USB data connections anywhere from an hour to seven days after a device has been locked unless USB connections have been accepted in the settings. *Android* phones allow for sudo access via the USB debugging mode, however this also requires the device to be unlocked in more recent phones.

Android and other more open source mobile OS are almost infamous for their lack of application verification. This allows for malware or other malicious applications to be installed which can be used to remove or corrupt data when the device has been confiscated. Although this is not the manufacturer making data extraction more difficult with security improvements it is still relevant to this essay. Their decision to not have checks in place for what applications are being installed on a device can hamper a forensics investigation. iOS also provides problems for data extraction due to their encryption methods. On Apple devices all data can be encrypted, including backups, which can result in having to use time consuming brute-forcing decryption in order to retrieve the information (Chernyshev et al, 2017).

'Impact of *Android* Phone Rooting on User Data Integrity in Mobile Forensics' discusses the concept of 'rooting', a form of privilege escalation on an *Android* device, a similar concept to 'jailbreaking' an *iphone* (Almehmadi and Batarfi, 2018). So called because the investigator gains root, or sudo, access to the device's file system. One difficulty with this methodology lies in the reliance on firmware security vulnerabilities that allow an investigator to gain the desired privilege level. As mentioned previously, software updates are fairly frequent which can patch previously exploitable vulnerabilities.

This paper mentions how device manufacturers strive to make their devices as secure as possible in order to protect their customers' data. In recent years consumers are becoming more aware of data privacy especially with the introduction of stricter legislation such as the European Union's General Data Protection Regulation in 2018. This shift in demand motivates manufacturers to provide more secure phones to gain a competitive advantage over others. Although all *Android* phones use the same base operating system each manufacturer makes minor changes in order to differentiate their devices from competitors'. These often vary the modules used for accessing non-volatile memory, where most of the data investigators want to collect exists. This is why rooting is important, so that all memory modules can be accessed and data extracted.

'Importance of rooting in an *Android* data acquisition' introduces tools that can root a mobile device that is connected to a computer although many of them are designed for older *Android* versions and may not be as effective on more modern phones. Some of the tools this author lists must be installed onto the device which is not acceptable in a criminal investigation as the evidence provided from an altered device is legally inadmissible. (Boueiz, 2020) Both authors agree that rooting is very important to ensuring that all of the data is extracted from a device, provided it is done in a forensically sound manner. They also both conclude that a difficulty in this methodology lies in the differences in *Android* OS versions and security features implemented by manufacturers.

A paper written by Chernyshev et al discusses the wide array of OS that are available and how these can offer additional challenges to investigations. They mention how criminals are aware of the limitations of forensic tooling; how they tend to only support the most popular operating systems and devices. For example, popular tools for extracting data only started providing support for phones using the *Windows OS* in 2015. As a result of this they choose to use phones with obsolete or older operating systems such as *Blackberry* or *Symbian* to increase the chance that their data will not be extracted. Boueiz's paper affirms this and explains that even the tools they describe for rooting a device are limited in their effectiveness against more modern phones.(Boueiz, 2020)

The difficulties of extracting data on a device with modern security features in place is discussed in the paper 'Challenges of acquiring mobile devices while minimizing the loss of usable forensics data' (Herrera, 2020). In this paper they discuss the danger of forensic investigators using their 'common sense' in

investigations; switching off the device or removing the SIM card. All of these would be seen as logical mitigations against remote commands being sent to delete or alter data on the device but with modern phones this is not the case. The danger lies in the device's security settings that can prevent access to data if any of the aforementioned are performed. For example, in current *iphones* once the device is turned off the state changes to Before First Unlock (BFU) from After First Unlock (AFU) and in this state the amount of data is severely limited. It is therefore recommended that the device is put into airplane mode, however this requires the phone to be unlocked and it is not often the investigator has access to the passcode. Even more low level data extraction techniques such as Chip-Off have been made more difficult in recent years by manufacturers desire for providing their users with better security.

iphone devices are also known to not always block Bluetooth connections in this mode so the phone can potentially be accessed remotely regardless if airplane mode is on or not. Although the author admits that they are not always one hundred per cent effective, their suggested method of preventing remote access and connections to a device is a Faraday cage or bag. These are made of metal or wire mesh and are designed to block all electromagnetic fields, including WiFi. In 2018 researchers created malware called Odini and Magneto that use manipulates the CPU's magnetic field in order to send and receive data from outside the Faraday bag (Advanced Cyber-Security Research Lab, 2018). These softwares suggest that there are no airtight methods to preventing a motivated person from accessing their device and investigators can only attempt to do so.

It is understandable why mobile device manufacturers wish to create more secure phones but this inevitably adds complexity to investigators trying to extract data for a criminal investigation. The ethical debate of security versus privacy is relevant here; should phone manufacturers provide investigators backdoors to access all of the data on a device or is there too much risk of this being abused?

In conclusion there is no easy answer to what should be done to assist data extraction for forensics investigations as any solution may have negative impacts in the longer term. By increasing device security criminals will find it easier to hide key evidence of their crimes but everyday people will be less likely to have sensitive data stolen or leaked publicly. The only happy medium is to focus on research into data extraction methodologies and increase the training budget of mobile forensics teams to allow them to stay up-to-date with the current technologies. This is especially important for older devices and less common OS' in order to mitigate the risk of crucial evidence not being found due to the tools not supporting the phone.

References

Advanced Cyber-Security Research Lab (2018). *Air-Gap Research Page*. [online] Available at: https://cyber.bgu.ac.il/advanced-cyber/airgap (Accessed 13 November)

Almehmadi, T. and Batarfi, O. (2018). *Impact of Android Phone Rooting on User Data Integrity in Mobile Forensics*. International Journal of Advanced Computer Science and Applications, 9(12).

Ayers, R. et al. (2014). *Guidelines on Mobile Device Forensics*. [online] Available at: https://www.nist.gov/publications/guidelines-mobile-device-forensics (Accessed: 30 October)

Boueiz, M. (2020). *Importance of rooting in an Android data acquisition*. 8th International Symposium on Digital Forensics and Security (ISDFS), Beirut, 2020, doi:10.1109/ISDFS49300.2020.9116445.

Chernyshev, M. et al. (2017).*Mobile Forensics: Advances, Challenges, and Research Opportunities*. IEEE Security and Privacy, [online] 15(6), pp.42–51. Available at: https://ieeexplore.ieee.org/abstract/document/8123468 [Accessed 17 Nov. 2020].

Herrera, L. (2020). *Challenges of acquiring mobile devices while minimizing the loss of usable forensics data.* IEEE Security and Privacy. doi:10.1109/ISDFS49300.2020.9116458.

MobileApps.com (2020). *Android vs iOS Market Share 2020: Stats and Facts* [online]. Available at: https://www.mobileapps.com/blog/android-vs-ios-market-share (Accessed: 05 November)

Ranjan, N. et al,(2016) *Android phone forensic: Tools and techniques*. International Conference on Computing, Communication and Automation, Noida, 2016, pp. 605-610, doi: 10.1109/CCAA.2016.7813792.