An Investigation into the Issues Law Enforcement Face With Mobile Device Security

Jack Clark
School of Design and Informatics
Abertay University
DUNDEE, DD1 1HG, UK

5th November 2019

Contents

1 Introduction **1**

1.1 Aim 1

2 Background **1**

3 Analysis **2**

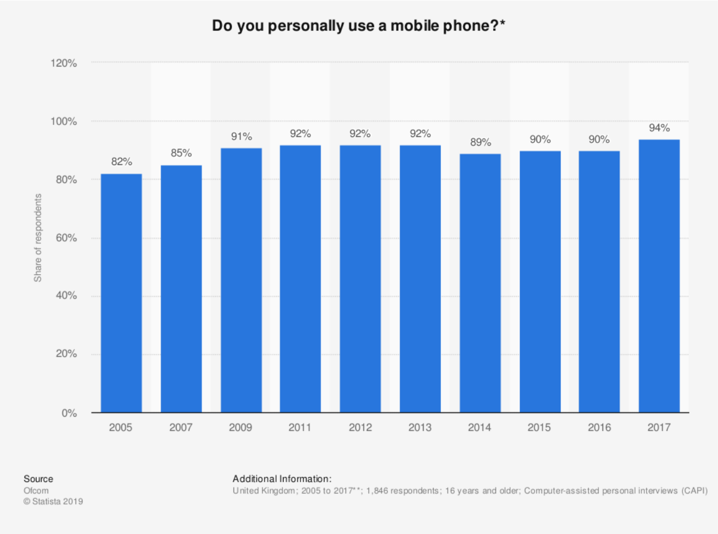
3.1 iOS Forensics 3

3.2 Ethics 7

4 Conclusion **7**

1 Introduction

The number of mobile devices in the UK has increased exponentially over previous years. From 2005, it was estimated that 82% of UK adults owned a smartphone, whereas in 2017 that number rose to 94% (See Figure 1).



Do you personally use a mobile phone?*

Source
Ofcom
© Statista 2019

Additional Information:
United Kingdom; 2005 to 2017**; 1,846 respondents; 16 years and older; Computer-assisted personal interviews (CAPI)

Figure 1: Adults That Use a Smarthphone in the UK (Statista 2019)

Alongside this increase, the technology and features inside these devices become more advanced year on year. With the increase of mobile devices, it is more likely that a person may be carrying one when a crime is committed, and so' it is now more likely than ever that the data on mobile devices is required for an investigation.

1.1 Aim

To discuss the challenges law enforcement face with:

- The security features of iOS devices
- Retrieving data from an iOS device for a forensic investigation
- The ethics of retrieving data from devices

2 Background

As previously stated, smartphones are becoming increasingly more secure. This increase of security is to thwart attempts by bad actors stealing and using a person's data, however, it can also hinder the effectiveness of law enforcement. For example, Apple introduced FaceID, a feature that implements facial recognition for the unlocking of a device, to their devices over the past years. In previous models, Apple implemented TouchID, a fingerprint sensor, which has since been replaced with FaceID. Both of these sensors are developed to increase the security of a device and protect the user's data. With a reported probability of another person unlocking your device at "1 in 50,000 with Touch ID or 1 in 1,000,000 with Face ID" both TouchID and FaceID are incredibly secure (*iOS Security Guide* 2019). Alongside the security of FaceID and TouchID, Apple have implemented restrictions on when a passcode will be required instead. This includes TouchID and FaceID failing to match a registered fingerprint or face (respectively) 5 times, a device being restarted or turned off and a device not being unlocked for 48 hours with either of the biometric options or a passcode(**Apple**). With the default suggested length of a passcode on an Apple device being 6-digits, and with the time-out features incorporated if a passcode is entered incorrectly consistently, it makes data retrieval difficult if a user is non-cooperative.

Alongside the time-out when a passcode is entered incorrectly too many times, the encryption of iOS is also tied to the passcode itself. Apple states that "the stronger the user passcode is, the stronger the encryption key becomes" (*iOS Security Guide* 2019). With iOS offering support for "six-digit, four-digit, and arbitrary-length alphanumeric passcodes" (*iOS Security Guide* 2019), the easiest way to increase the strength of the encryption and subsequently the security of a device is by using a longer passcode.

With iOS devices offering an "Emergency SOS" mode[1](*Use Emergency SOS on your iPhone* 2019), where a user can press a button multiple times to lock the device, disable biometrics and require a passcode, a device can be locked incredibly fast by a user. Again, this feature is designed to help users in the case of a person stealing a device or if a user is injured and needs emergency services, however, it can also be used by a person involved in a crime to disable the biometrics and force the passcode to be used.

The aforementioned security features can make it incredibly difficult for data retrieval from an iOS device. Typically when an iOS device is locked, for example, iPhone, the data is encrypted (*iOS Security Guide* 2019) and so law enforcement need to use methods first to extract the data and then decrypt it.

3 Analysis

There is a large number of academic sources that have performed forensics on iOS devices, however very little, sources directly from law enforcement. Due to this, research was performed on the issues that researchers have had and then compared to how this may affect law enforcement.

[1] As of iOS 11

3.1 iOS Forensics

As previously mentioned, smartphones include features to protect the data of the user. These features can prevent law enforcement from retrieving crucial data for an investigation, the most common of which is a passcode and biometric lock. The following work has developed techniques that can bypass these features and potentially assist law enforcement.

The paper *"Identifying back doors, attack points, and surveillance mechanisms in iOS devices"* (Zdziarski 2014) discusses the security features of iOS and how it has been developed to increase security, although managing to contain severe security flaws that may assist law enforcement. The paper discusses the security of iOS and how it has been developed, but goes into more detail regarding how some security omissions can be exploited fairly easily.

The paper presents techniques exploiting a feature that allows syncing of an iOS device to a computer to transfer data. When a device is synced, it creates a "trusted relationship with another device, where the client device is granted privileged, trusted access" (Zdziarski 2014), meaning that once an iOS device is synced with a computer, the computer is granted access to the files on the device. As stated in the paper, after being synced once, an issue arises where "the phone can be accessed over either USB or WiFi regardless of whether or not WiFi sync is turned on" (Zdziarski 2014), allowing a potential bad actor to gain access to the device data if the host is compromised.

Zdziarski further advances on this exploit by uncovering undocumented features of iOS that can be used by a bad actor. Many of these can be performed remotely from a compromised computer that has been synced with the device. The undocumented features can perform actions such as starting a packet sniffer on the device or starting "com.apple.mobile.file_relay" (Zdziarski 2014), a process on the iOS device that, if used correctly, can transmit valuable information back to the host.

It is clear that the author has performed thorough research into exploiting this vulnerability and the data that can be gathered would be incredibly useful for a forensic investigation. An issue with this, however, is that this method relies on the device being previously synced with a computer. To compound this further, law enforcement would need to gain access to said computer to then connect to the device, which could also have passwords and encryption which could delay or prevent access.

A further issue with the findings of this paper is that since the time of writing, Apple has addressed the security concerns from researchers regarding the undocumented control that can be accessed through the proposed method. Apple has stated that they offer "diagnostic capabilities to help enterprise IT departments, developers, and AppleCare troubleshoot issues" (*iOS: About diagnostic capabilities* 2019) and have further detailed the use of file_relay as a tool to be used by AppleCare to gather diagnostics data from a device and used internally at Apple (*iOS: About diagnostic capabilities* 2019).

The work *"Evaluating Digital Forensic Options for the Apple iPad"* (Hay et al. 2011) builds on other techniques for retrieving data from an iOS device. The paper discusses how to retrieve data using various methods: analysing an iTunes backup, similar to Zdziarski, using specialised software tools and jailbreaking the device, however, these methods assume that there is no passcode or biometrics. Although law enforcement may know the passcode to a device, it is still vital to perform forensic analysis as it can prove useful for a deep investigation which iOS, in itself, prevents.

There exists a vast array of software tools that can perform forensics on a device and this paper discussed three: Lantern, Mobilyze(*Mobilyze — BlackBag* 2019) and Oxygen Forensics Suite (*Oxygen Forensics - Mobile forensic solutions: software and hardware* 2019). Of the three discussed Lantern has been discontinued, however, the other tools have been developed further and support the latest devices. The author uses the tools to assess the device in question, an iPad[2], and evaluates the data that is retrieved using them. All tests were performed on the same iPad with the same data.

Throughout the testing of the tools, the following files were looked for:

- Documents, for example downloaded PDF and Word documents
- Media, such as music, photos and videos
- Mail and subsequent attachments
- Notes
- Contacts
- Safari and YouTube data
- Maps data, such as search history and pins
- Calendar data
- Installed Applications

The testing that was performed was very thorough. The information that was searched for is typically what would be required for a forensic investigation. Ultimately the tools proved to miss a fair amount of vital data that it was expected that they would discover.

Although the tools were lacking in some areas, they can still be a solution for law enforcement. If the passcode is known, then tools can typically gather data faster than what a human can. The authors stated that when they performed analysis on the device, it took "Lantern 7 minutes, Oxygen 17 minutes and Mobilyze 27 minutes" (Hay et al. 2011). The relatively short

[2] The existing tools the author uses supports most iOS devices

time that it takes for the tools to retrieve the data from the device could be important if it is a time-sensitive investigation, however other techniques discussed would be preferable if time is not as much an issue, as it managed to gather more data but took longer than the tools.

Another issue that law enforcement would face with using software tools is the cost. The price of one of these tools, for example Mobilyze is \$650.00 for verified law enforcement (*Mobilyze — BlackBag* 2019). In Scotland there are 13 Police Scotland division headquarters and, if a licence for each division were to be bought, the cost would be \$12,650 (£9802.42 at the time of writing). The cost would also increase as training would be required to use the software. As can be seen, software-based tools are very expensive, and if more licenses are required, then this cost would only rise.

As mentioned, the authors discussed analysing an iTunes Backup of the device. When a device is connected to a computer and synced with iTunes, it starts to create a backup of the device automatically. This feature is incredibly useful for a user as if they were to lose their device or have to erase it for some reason, this backup can be restored and no data will be lost (other than that from after the backup).

The authors discuss dissecting the backup that is stored on the computer. This method is found to be more effective than using the software-based tools, however, it takes more time. The downside to analysing an iTunes backup, however, is that the device ”should have been previously configured to not encrypt backups” (Hay et al. 2011), which is a feature that iTunes by default has turned off. If the backup has been encrypted, then this technique will not work.

The issue that law enforcement may face with this is that it relies heavily on the owner of the iOS device also having a computer that it has been synced to, similar to Zdziarski’s work.

The final technique that is discussed by the authors is jailbreaking the device. The act of jailbreaking is defined as ”modifications to iOS (also known as ”jailbreaking”) [to bypass] security features” (*Unauthorized modification of iOS can cause security vulnerabilities, instability, shortened battery life, and other issues* 2018). Although this modification is unauthorised by Apple, many users of iOS perform a jailbreak as it lifts restrictions that iOS places, typically for the security and usability of the device.

By jailbreaking a device, the security of it is lessened and applications can be installed freely, without the use of the App Store. A common package manager, similar to an App Store for jailbroken devices, is Cydia (*Cydia* 2018). Typically a jailbreak will include Cydia which will also automatically install some packages, an important one being OpenSSH. With this package installed a user can SSH into the iOS device as the root user (default password being ”alpine”), and access the entire filesystem of the device. With SSH access as the root user, the experience is very similar to any other UNIX system (for example, MacBook or iMac) where files can be accessed, viewed and downloaded. With a device that has been jailbroken, the entire filesystem can be imaged and then downloaded from the device. This allows for the data on the device to remain, partially, untouched and analysed on a separate device.

The authors make use of JailbreakMe (*JailbreakMe* n.d.), an effective Safari-based jailbreak for their testing. To execute the testing, the authors used the same device as when testing the software-based tools and searched for the same data.

The results of testing the jailbroken device show how powerful a jailbreak is. All the data that the authors searched for was found. In comparison to software tools, the search for files needs to be performed manually, so it will take considerably more time, however, the amount of data gathered is exceptionally more.

The main weakness with jailbreaking a device, however, is that it touches the filesystem. Currently, there is a jailbreak for up to iOS 12.4, and devices with an A12 processor or lower, called "unc0ver"[3] which is incredibly stable and comes bundled with Cydia. Although the jailbreak is readily available, to install it onto a device an Apple Developer account is required alongside the use of Cydia Impactor, a tool to install applications from out-with the App Store but tied to a developer account.

By installing the jailbreak, and then running it to actually jailbreak the device, data will be changed. This creates an issue for law enforcement as it can open an avenue for the argument that the data is no longer forensically sound. Although a jailbreak can be incredibly useful and gather a vast amount of data, it can very easily ruin an investigation.

A temporary solution to this issue would be performing a hash of the full filesystem after the jailbreak, image the device and work based on the image, however, the filesystem will have been changed due to the jailbreak. Alongside this, using a jailbreak such as unc0ver has its benefits as it is entirely open-source. Therefore it can be vetted and examined beforehand to check what will be altered. An ideal solution would be the development of a forensically sound jailbreak, for performing iOS forensics. The difficulty with this idea is that a jailbreak is performed by on purposely altering the filesystem.

The work by Hay et al. is incredibly useful and presents multiple techniques for retrieving data from a device, however, the paper makes no attempt to address techniques for retrieving data from a locked device. The paper would have been more useful if it had included this as it is very uncommon for a device not to have a passcode. At the same time, the paper discusses in great detail the process of jailbreaking a device, which can be complex and so is incredibly useful.

[3] https://github.com/pwn20wndstuff/Undecimus/

3.2 Ethics

Not only do law enforcement face issues with retrieving data from a physical device, but they also face issues regarding ethics. In 2015 there was a shooting in San Bernardino, California, where 14 people were killed and 17 injured (Inspector General 2018). The shooter was found to have an iPhone 5C on them at the time and the FBI requested that Apple be given a court order to assist the FBI in retrieving the data from the device.

On receiving the court order, Apple declined to adhere to it as it states that it "violates its First Amendment right" and "could create a permanent way to bypass iPhone password protection for law enforcement officials" (Khamooshi 2016). The feedback from other large technology companies, in particular in Silicon Valley, support Apple in this fight for the same reasons.

This scenario highlights an ethical issue that law enforcement can face with devices that are involved in an investigation. If the data can not be retrieved however it is deemed important enough, then law enforcement can contact manufacturers to ask to decrypt the information on the device, similar to the San Bernardino case. But at the same time, the general public may purchase devices for the reason being that they are secure, and if a company complies to the request to decrypt data, it can create the belief that devices are no longer secure.

At the beginning of 2019, Forbes published a report based on a court ruling regarding law enforcement forcing people to unlock their devices (Brewster 2019). The court ruling stated (United States District Court 2019)

> "that if a person cannot be compelled to provide a passcode because it is a testimonial communication, a person cannot be compelled to provide one's finger, thumb, iris, face, or other biometric feature to unlock that same device."

The ruling, therefore, shows that law enforcement has to face ethical issues when dealing with investigations. They are not allowed to force a person to give the passcode to unlock the device, regardless of how vital it is for the investigation.

4 Conclusion

In conclusion, law enforcement faces multiple issues when faced with performing forensics of mobile devices. These include retrieving data from a device, with and without the passcode and ethical issues regarding retrieving the passcode for the device. The works by Zdziarski and Hay et al. show that there are techniques and methods to retrieve data from iOS devices, however, when these in itself creates an issue for law enforcement due to forensic integrity of data and security being increased by developers. Alongside this, if the data can not be recovered from a device due to it being locked by a passcode or biometrics, law enforcement in the United States are not allowed to force a person to give this information. Ultimately, there are ways for law enforcement to tackle these issues, however they come along with compromises.

References

Brewster, Thomas (Jan. 2019). *Feds Can't Force You To Unlock Your iPhone With Finger Or Face, Judge Rules.* Available at: `https://www.forbes.com/sites/thomasbrewster/2019/01/14/feds-cant-force-you-to-unlock-your-iphone-with-finger-or-face-judge-rules` (Accessed: 04 November 2019).

Cydia (2018). Available at: `https://cydia.saurik.com` (Accessed: 04 November 2019).

Hay, Andrew et al. (2011). "Evaluating Digital Forensic Options for the Apple iPad". English. In: vol. 361. Advances in Digital Forensics VII. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 257–273. ISBN: 9783642242113. DOI: `10.1007/978-3-642-24212-0_20`. URL: `https://hal.inria.fr/hal-01569561`.

Inspector General, Office of the (Mar. 2018). *A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation.* Tech. rep.

iOS Security Guide (2019). Available at: `https://www.apple.com/business/docs/site/iOS_Security_Guide.pdf` (Accessed: 31 October 2019).

iOS: About diagnostic capabilities (2019). Available at: `diagnosticcapabilitiestohelpenterpriseITdepartments, developers,andAppleCaretroubleshootissues` (Accessed: 2 November 2019).

JailbreakMe (n.d.). Available at: `https://jailbreak.me` (Accessed: 04 November 2019).

Khamooshi, Arash (Mar. 2016). *Breaking Down Apple's iPhone Fight With the U.S. Government.* Available at: `https://www.nytimes.com/interactive/2016/03/03/technology/apple-iphone-fbi-fight-explained.html` (Accessed: 04 November 2019).

Mobilyze — BlackBag (2019). Available at: `https://www.blackbagtech.com/products/mobilyze/` (Accessed: 04 November 2019).

Oxygen Forensics - Mobile forensic solutions: software and hardware (2019). Available at: `https://www.oxygen-forensic.com` (Accessed: 04 November 2019).

Statista (2019). *Do you personally use a mobile phone?* Available at: `https://www.statista.com/statistics/300378/mobile-phone-usage-in-the-uk/` (Accessed: 31 October 2019).

Unauthorized modification of iOS can cause security vulnerabilities, instability, shortened battery life, and other issues (2018). Available at: `https://support.apple.com/en-gb/HT201954` (Accessed: 04 November 2019).

United States District Court (Jan. 2019). *ORDER DENYING APPLICATION FOR A SEARCH WARRANT*. Available at: `https://assets.documentcloud.org/documents/5684083/Judge-Says-Facial-Recognition-Unlocks-Not.pdf` (Accessed: 04 November 2019).

Use Emergency SOS on your iPhone (2019). Available at: `https://support.apple.com/en-us/HT208076` (Accessed: 31 October 2019).

Zdziarski, Jonathan (Mar. 2014). "Identifying back doors, attack points, and surveillance mechanisms in iOS devices". English. In: *Digital Investigation* 11.1, pp. 3–19. DOI: `10.1016/j.diin.2014.01.001`.