Electronics and Electrical Engineering

http://www.aimspress.com/journal/ElectrEng

AIMS Electronics and Electrical Engineering, 4(3): 249–258.
DOI: 10.3934/ElectrEng.2020.3.249
Received: 31 March 2020
Accepted: 08 June 2020
Published: 22 June 2020

Review

Security and privacy challenges in the field of iOS device forensics

Dave Bullock[1], Aliyu Aliyu[1], Leandros Maglaras[1,2,*] and Mohamed Amine Ferrag[3]

[1] School of Computer Science and Informatics, De Montfort University, The Gateway, Leicester, LE1 9BH, UK

[2] Department of Informatics and Computer Engineering, University of West Attica, Greece

[3] Faculty of Mathematics, Computer Science, and Material Science, Guelma University, BP 401 GUELMA 24000, Algeria

* **Correspondence:** Email: leandros.maglaras@dmu.ac.uk.

Abstract: The purpose of this paper is to review existing research literature analyzing the existing challenges facing the forensics community during investigations involving iOS devices. The scope of this paper is to analyze the existing security and privacy challenges and review the research and techniques being developed to combat these challenges. Throughout this paper, examples, where techniques have been applied, are discussed and future topics of research are identified.

Keywords: iOS device forensics; cyber security; privacy issues

1. Introduction

Mobile devices are nowadays an essential part of our everyday life, as they are used for a variety of mobile applications [1]. Mobile device usage has grown in the UK over the last decade, with research from 2017 indicating that at least 41 million people now have access to a smartphone with over 10,000 models from as many as 3,000 manufacturers being available [2]. This continued adoption of mobile technology, manufacturers such as Apple and Samsung continuously release new software and updated hardware platforms to maintain their market appeal. Performance improvements to mobile devices are in line with Moore's Law [3], summarised as overall computer power doubling every two years. This can be seen when comparing the last three iPhone models, with the iPhone 6 having a base memory of 16GB which the iPhone 7 doubled and the iPhoneXR doubled again to 64 GB.Throughout these models, the chipset and processes have also increased from the original A8 chip to the A12 bionic chipset in the iPhone XR capable of 5 trillion operations per second.

As hardware has evolved, so have the underlying Operating Systems (OS) on devices, these include changes to security, access mechanisms, data formats and storage methods [4]. As mobile

devices have advanced technologically, the challenges facing forensic practitioners have increased. The aim of this article is to identify and review current security and privacy challenges facing the forensic community, with specific emphasis on iOS mobile devices and the challenges they pose forensic investigators. Existing challenges in forensics can be grouped into three main categories those being technical, legal and resource challenges [5]. Multiple types of extractions can be used to produce a forensic image of an iOS smartphone, that is a full copy of the data stored on the device. During a forensic investigation we aim to obtain the most complete record of data possible, while avoiding on the same time altering evidence in order to be able to use these on court. The most complete method for obtaining an acquisition on an iOS is a physical acquisition if possible, otherwise a logical acquisition is acceptable. The iOS device will most of the times need to be jailbroken in order to achieve this on modern iOS versions, although it is a process which changes the file system and potentially alters the evidence. This method gives access to lower level system functions [6]. An additional option for an acquisition on iOS is analyzing an iTunes backup file [7]. Most mobile forensic tools can open and analyze backup files, which has been found to contain some location-related files that also have some value for the investigators. The data available could assist in solving investigations related to kidnapping, missing persons, or organized criminal rings [8].

Several existing works try to address security and privacy issues as related to IoS [8, 9, 10, 11]. Especially the book [11] is a must read for individuals who are interested in the iPhone and other iOS devices and provides detailed methods on how to extract information from an iOS device. Most of the aforementioned works either focus on only one aspect of IoS forensics, e.g. dating or location applications or discuss digital forensics in general, including IoS security challenges in their research. The current article specifically try to analyse all security and privacy challenges that forensics investigators face when working with IoS devices, and discusses open future directions.

Our contributions in this work are:

- We analyze the existing security and privacy challenges that forensics investigators face when dealing with IoS
- We categorize those challenges into three main categories: tehcnical, legal and resources.
- We briefly compare Android to IoS security issues.
- We discuss open issues and propose some practical solutions that could help overcome existing obstacles.

2. Technical challenges

As the cost of mobile devices has increased, manufacturers have built more robust security features into their devices to help protect customer data and aid in device location in the case of theft. Unfortunately, as these features have improved device security, they have significantly impacted forensic examinations and data acquisition which has led researchers like Jackson to question if digital forensics can keep pace [2]. In a mobile device forensic investigation, all acquired evidence should be taken into consideration, handled, and combined so as to reach a satisfactory conclusion [12]. Authors in [13] investigated file recovery by conducting a set of controlled experiments using different cloud services on iOS devices. Based on their analysis they discovered what kind of files could be recovered easier, and discovered that thumbnails could be the key for facilitating the investigation.

Apple first released the iPhone in 2007 including the first release of their Operating System iOS 1. This initial release had little security and was only updated when a community of hackers were identified developing and distributing unauthorised third-party applications [14]. The following updated iOS 2 release included the first evolution of the remote delete feature and an attempt to lock down their phones using encryption and digital signing [14].

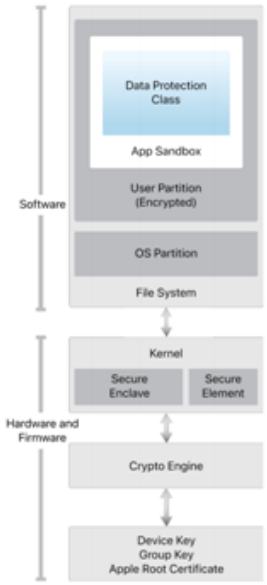

Figure 1. iOS security architecture.

As the iPhone has been developed and evolved, Apple have also released a number of other mobile devices including several variations of the iPhone, iPad and Apple Watch as well as numerous iOS releases. Each of these devices aims to protect customer data by combining encryption, secure boot and access mechanisms to support maximum security.

Initial guidance from the ACPO (The Association of Chief Police Officers of England, Wales and Northern Ireland) guidelines for digital evidence, advises first responders at a crime scene to isolate a mobile device from the network by powering it off [15]. This advice was initially aimed at protecting changes to a device and the possibility of a remote wipe command being received and processed. As the security mechanisms in mobile devices have evolved, this advice is no longer fit for purpose and can potentially have severe implications later in the investigation. Authors in [16] described 'cold booted' iPhone analysis as being one of the most difficult tasks a forensic examiner can encounter. Since iOS8 the data partition is encrypted with a key based on the user's passcode, the partition remains encrypted until the device passcode is entered. There are numerous privacy and legal challenges with this which are discussed later in the document. In another work [17], authors moved one step further and proposed an operational technique that allows digital forensic practitioners to recover deleted image files by referring to iOS journaling file system.

Researchers at MAGNET Forensics also describe additional implications of carrying out 'traditional' actions taken during device acquisition, with some not present in the Apple security documentation. This is that removing the sim card in an attempt to isolate network traffic from a

locked iOS 12 device, will also disable other potential unlock vectors including face and fingerprint recognition. Another traditional approach to device isolation is to place it in to a faraday bag, although necessary, researchers have accepted that this has an impact on the bypassing of biometric security measure such as fingerprints and face recognition [18, 19].

Although it is possible for biometric keys to be legally compelled to unlock a device, later iOS releases have security features which mean biometric unlocks may still not help forensic investigators. Delivered as part of iOS 12, are a number of scenarios which will disable fingerprint and face recognition and force the entering of a passcode to unlock the device. These scenarios include:

- If the mobile device has been powered on
- Hasn't been unlocked in more than 48 hours
- If the password hasn't been used in over 156 hours and facial recognition in 4 hours
- The device receives an unlock command
- After 5 unsuccessful attempts to match biometric security measures (Apple, 2019)

Echoing what was discussed above about cold booting iPhones, the new time-based restrictions could present a similar acquisition challenge. An example of this could be when these automatic security measures are activated before a crime scene was discovered and the forensic team accessed the device. This is a concern because as discussed by Mahalik, data is volatile and can quickly be deleted or transformed remotely, with more effort needed in the preservation of this data [20].

In iOS 11.4.1 Beta versions, Apple introduced a new default security setting which disables USB data traffic after the device has been locked for over an hour [21]. Further research by the forensic community identified the iPhone will only charge itself after an hour, unless the passcode to unlock the device is entered every hour. However, they discovered that certain accessory cables can delay the timer for up to seven days, helping forensic teams prolong the time needed between entering the passcode enabling device imaging [22].

Apple have also enabled a mode called "S.O.S Mode", this is entered by pressing a button on the side of the device 5 times in quick succession. This will temporarily disable the touch id and require a passcode to unlock the device, so if a biometric access has been compelled by the court the investigators would still need a passcode to access the device [23]. This is something which could potentially be invoked accidentally, for example if a device isn't packaged correctly and the button is hit during transport.

Although the forensic and security community have found a number of techniques to counter the constant security updates by Apple to their devices, there are still fundamental security features that could thwart an investigation. For example, in an attempt to protect a device and its customer's data, Apple have included a setting which will completely wipe the data of the device if an incorrect passcode is entered 10 times [24]. This is a feature to discourage a brute force attack which was possible with earlier version of iOS.

When a device is locked, researchers identified a mechanism to extract limited information using a pairing record or a Lockdown file. This does assume you have access to a machine that the device has previously been connect to. This file enables examiners to extract information from the device and for certain tools to perform limited logical acquisition. This technique was then complicated by the release of iOS 11.3 as Apple implemented a seven-day expiry time limit on the files. This was also discussed by Afonin who identified the potential impact if the timeline for acquiring devices to being ready for investigation isn't quick enough,then the records will expire before they can be used [23].

Companies like Apple have been working steadily to improve the security of mobile devices through encryption [25]. Apple have integrated encryption into the hardware and firmware of their devices (See Figure 1). There is a dedicated Advanced Encryption Standard (AES) 256-bit crypto engine which resides between the device flash storage and the main system memory [26]. On later models, the flash storage system is on a dedicated isolated bus that is only granted access to the user data through the DMA crypto engine. These security mechanisms are not available through the Joint Test Action Group (JTAG) or other debugging mechanisms available to forensic investigators as keys are fused into the secure enclave and encryption processor during manufacturing.

With the challenge of well implemented encryption, the forensic community have developed a technique known as jailbreaking to gain access to devices [27]. This technique enables forensic examiners to circumvent the restrictions placed on a device by Apple by side loading a piece of code to escape the inbuilt iOS security features such as sandboxing,changing the underlying operating system. This allows the installation of applications such as an SSH server enabling bit for bit copies of the device to be made.

Scholars also identifies the risk of using a 'rooted' jailbreak and discusses the advantages of using a 'rootles' jailbreak to prevent data being written to the root data partition of a device [16]. When reviewing the forensic soundness of this technique, authors describe the unavoidable changes to the device, the inherit difficulty of cleanly removing the jailbreak and the initial risk of exposing the device to an internet server. This approach does appear to be in complete contrast to the principle outlined by the ACPO guidelines for avoiding actions which change data on the target device.

The aggressive nature with which Apple releases software and security updates could potentially impact the successfulness of this technique. The ability to side load unsigned code was specifically targeted during a recent round of Apple updates. This was also the case with a vulnerability identified by security researchers. Scholars discovered a method to break into an iPhone using the Bluetooth Airdrop feature [28]. Apple have also taken the approach to release significant bug bounties for identified weaknesses in their devices and iOS releases, thus helping to bolster their internal testing and patch vulnerabilities (See Table 1).

Table 1. Apple security bounty payments.

Category	Maximum payment (USD)
Secure boot firware components	200.000
Extraction of confidential material protected by the secure enclave	100.000
Execution of aritrary code with Kernel privileges	50.000
Unauthorized access to iCloud account data on Apple servers	50.000
Access from a sandboxed process to user data outside of the sandbox	25.000

3. Legal challenges

In 2014 Apple introduced encryption by default which prevented them from unlocking devices as the encryption key is based on the user's passcode. This was following the Apple ethos of privacy being a "fundamental human right", stating great experiences don't have to be at the expense of privacy and security. Law enforcement and security firms at the time raised concerns about not being able to access

key evidence on Apple devices describing them as "Warrant Proof" [29].

In 2015, an iPhone belonging to Syed Farook who killed fourteen people in a terrorist attack in the United States of America [30]. The FBI required access to the device as part of their investigation and the now infamous court case between the FBI and Apple ensued. The FBI request to Apple included disablingor circumventing the auto erase feature and automating passcode attempts. Apple actively refused to obey a court order to unlock the terrorist device and stated that building a "back door" into its devices for law enforcement would set a dangerous precedent [31]. Apple were supported in their stance by large technology companies including Microsoft and Google. During this time, research published by the security company TrailOfBits detailed how Apple could circumvent their security processes and comply with the FBI request by building a customised version of iOS to counter the software restrictions.

Apple do have the ability to provide cryptographic keys to aid in the unlocking of iCloud accounts, where any requests for such keys would need to be submitted through the American legal system. In 2018, researchers at Reuters reported on how Apple would host Chinese user's iCloud encryption keys in a data centre in China [32]. This seems contrary to the privacy statement Tim Cook made, where the risk of losing access to a lucrative Chinese market weren't enough to keep the keys in America despite numerous human rights concerns.

4. Resources challenges

Apple have a culture of secrecy and employees inside the business often don't known what other teams are working on [33]. As discussed by MAGNET forensic researchers, this approach can often lead to undocumented security restrictions which need to be firstly identified, researched and countered by the forensic community. This has a knock-on impact, where available jailbreaks wont often be available for a substantial period of time following an iOS release, thus impacting the investigation schedule.

During the legal battle between the FBI and Apple, the case was dropped as the FBI announced they had gained access to the locked phone through the discovery of a bootloader vulnerability by the Israeli company 'Cellebrite' [34]. Cellebrite have not divulged any information about how they have circumvented the Apple security restraints but have acknowledged that their capability will work on iPhones and iPads running iOS 5 to iOS 11. The secrecy about the vulnerability prevents this technique from being shared, this is due to the risk of competitive disadvantage or Apple actively patching the security hole.

Another company Grayshift has produced a similar tool called "GrayKey" with a similar stance on security and keeping the details of their capability secret. GrayKey takes advantage of an unknown exploit in the secure enclave processor, the hardware which handles the iPhone encryption [35]. Graykeys' ability to exploit Apple products must use an inbuilt, difficult or impossible to patch vulnerability, as the release of GrayKey and the setting up of Grayshift as a company wouldn't be warranted. Joseph fox noted the dramatic decrease in price where Cellebrite charged $200,00$ for an unlock subscription which has now dropped to $15,000$. Privacy advocate Joseph Hall expressed concern as there is nothing to indicate or restrict Grayshift selling products to only democratic or 'friendly' countries.

Apple are actively attempting to prevent tools like GrayKey from unlocking devices with frequent

patch releases and new security features such as the USB restricted mode. The struggle between Apple and the security community has become an arms race with companies trying to either protect their capability for commercial gain, or collect bug bounties. The secret nature of these companies does call into question the potential forensic soundness of their approach to access a device.Although in 2019 MAGNET Forensics announced a partnership with Garyshift. This partnership doesn't disclose the unlocking methodology to the community for review, but it does indicate that with forensic practitioners involved the process will be as forensically sound as possible.

5. Discussion

This article discusses the challenges posed to a forensic investigation on iOS devices. The initial challenges lie in the ability of the forensic community and first responders to be able to identify an iOS device and understand how to properly isolate the device from the network. The ACPO guidelines and legal frameworks to force users to divulge their passwords have been updated in recent years. Due to the rate of change with mobile device, these areas of legislation and technical guidance will need constant reviewing to ensure they match the pace of change and remain relevant.

In a recent article [36] discovered vulnerabilities on Android applications in regards to the recovery of authentication credentials from the volatile memory. Also in [8] authors discovered forensic artifacts from two popular third-party location sharing applications for both iOS and Android devices, proving that iOS has similar security and privacy issues as related to Android devices.

First responders should be aware of the potential security restrictions and time-based changes that may impact the device, even if they have been isolated correctly. Although some of the mechanisms Apple have implemented in their devices to protect the device from theft are in the correct way, Apple should work closer with law enforcement to help isolate a device correctly. Building 'backdoors' into their software is something which should not happen, but maintaining a mechanism or service which could be used by Law enforcement seems like a sensible balance between privacy and security. An example of such a model is that of Sensorvault [37] which is been described as a boon for Law enforcement agencies. As Law enforcement agencies are going through extreme measures such as leveraging on super computers [38]. A sort of partnership/collaboration can be feasible. The mechanism being proposed is that of a model that is similar to what Google is doing. It has an internal database that contains records of users' historical geolocation data [39]. And it is being used by law enforcement agencies. The LEA obtain a geofence warrant and then search for all devices within the vicinity of a crime and after looking at those devices' movements and narrowing those devices down to potential suspects or witnesses. It then asks Google for the information about the owners of those devices for further investigations. There is a balance of privacy and security here as the identity of users are not revealed as they are just identified with numbers. It is only revealed as and when needed hence with this sort of mechanism or service. Apple can adopt a similar model for its iOS.

The secrecy with which Cellebrite and Grayshift protect their approach, seems to be the start of a new trend in how forensic and security companies will operate. As it has been demonstrated that Apple will actively try to identify and patch the exposed security vulnerabilities. The secrecy is necessary for maintaining market share and a viable product. This has an impact to the wider forensic community as techniques and forensic soundness cannot be verified. There doesn't appear to be any legal restrictions on who these products can be sold to.

Finally, the battle between new releases of iOS and jailbraking methods will continue. The new version of the jailbraking tool "unc0ver" will be able to break every iOS device including the 13.5 recently released version by taking advantage of a zero-day kernel exploit. Although there are many things that need to be improved, the use of open source tools for Digital forensics is considered important. With the Advantage of access to source code, use of open source tools can be beneficial for Digital Criminology researchers to use appropriately and more tools beyond commercial. The source code analysis allows examiners to know exactly what is happening on the device for analysis and how, as well as present both the program and the source code in court during the trial.

6. Conclusions

The main challenges facing the forensic community can be grouped into three categories, technical, legal and resource all playing a critical role. As device manufacturers compete for market share based on their security features and their pledge to keep customer data 'secure', techniques such as those developed by Cellebrite and Grayshift will need to adapt as Apple will eventually be able to successfully block them. Cheaper alternative mechanisms for jailbreaking devices are already noting the delay between iOS releases and the availability of jailbreaks. Researchers have also noted the difficulty in cleanly removing jailbreaks which calls the forensic soundness of these approaches into question as they go against the ACPO guidelines.

Acknowledgments

We thankfully acknowledge the support of the CONCORDIA H2020 (GA no. 830927) EU project.

Conflict of interest

Authors declare no conflict of interest.

References

1. Ferrag MA, Maglaras L, Derhab A (2019) Authentication and authorization for mobile iot devices using biofeatures: Recent advances and future trends. *Secur Commun Netw* 2019: 1–20.
2. Jackson W (2014) Can digital forensics keep up with smartphone tech.
3. Waldrop MM (2016) The chips are down for moore's law. *Nature News* 530: 144.
4. Ferrag MA, Maglaras L, Derhab A, et al. (2020) Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues. *Telecommun Syst* 73: 317–348.
5. Al Fahdi M, Clarke NL, Furnell SM (2013) Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions. *2013 Information Security for South Africa*, 1–8.
6. Barmpatsalou K, Damopoulos D, Kambourakis G, et al. (2013) A critical review of 7 years of mobile device forensics. *Digit Invest* 10: 323–349.
7. Husain MI, Baggili I, Sridhar R (2010) A simple cost-effective framework for iphone forensic analysis. *International Conference on Digital Forensics and Cyber Crime*, 27–37.

8. Bays J and Karabiyik U (2019) Forensic analysis of third party location applications in android and ios. *arXiv preprint arXiv:1907.00074*.
9. Troutman C and Mancha V (2020) Mobile forensics. *Digital Forensic Education* 61: 175–201.
10. Knox S, Moghadam S, Patrick K, et al. (2020) What's really 'happning'? a forensic analysis of android and ios happn dating apps. *Comput Secur* 94: 101833.
11. Hoog A and Strzempka K (2011) *iPhone and iOS forensics: Investigation, analysis and mobile security for Apple iPhone, iPad and iOS devices*. Elsevier.
12. Barmpatsalou K, Cruz T, Monteiro E, et al. (2018) Current and future trends in mobile device forensics: A survey. *ACM Comput Surv (CSUR)* 51: 1–31.
13. Huang CT, Ko HJ, Zhuang ZW, et al. (2018) Mobile forensics for cloud storage service on ios systems. *2018 International Symposium on Information Theory and Its Applications (ISITA)*, 178–182.
14. Long J (2016) The evolution of ios security and privacy features.
15. Reiner R (1991) *Chief constables*. Oxford: Oxford University Press.
16. Todesco L (2015) Attacking the xnu kernel in el capitan. *Black Hat EU*.
17. Ariffin A, DOorazio C, Choo KKR, et al. (2013) ios forensics: How can we recover deleted image files with timestamp in a forensically sound manner? *2013 International conference on availability, reliability and security*, 375–382.
18. Blanch JL and Christensen SS (2018) Biometric basics: Options to gather data from digital devices locked by a biometric key. *US Att'ys Bull* 66: 3.
19. Ferrag MA, Maglaras L, Derhab A, et al. (2018) Taxonomy of biometric-based authentication schemes for mobile computing devices. *2018 3rd international conference on pattern analysis and intelligent systems (PAIS)*, 1–8.
20. Mahalik H, Tamma R, Bommisetty S (2016) *Practical Mobile Forensics*. Packt Publishing Ltd.
21. Edge C and Trouton R (2020) The evolution of apple device management. *Apple Device Management*, 1–54.
22. Fox-Brewster T (2018) The feds can now (probably) unlock every iphone model in existence.
23. Afonin O (2017) New security measures in ios 11 and their forensic implications.
24. Lutes KD and Mislan RP (2008) Challenges in mobile phone forensics. *Proceeding of the 5th International Conference on Cybernetics and Information Technologies, Systems and Applications (CITSA)*.
25. Castro D and McQuinn A (2016) Unlocking encryption: Information security and the rule of law. *Information Technology and Innovation Foundation*.
26. Bédrune JB and Sigwald J (2011) iphone data protection in depth. *Vortrag von der HITB-SecConf*.
27. Hyrynsalmi S, Koskinen J, Hyrynsalmi SM (2019) A review of ethical discussions on platforms and ecosystems. *Proceedings of the Third Seminar on Technology Ethics 2019* 2505: 9–19. In: Proceedings of the Third Seminar on Technology Ethics 2019.

28. Martin J, Alpuche D, Bodeman K, et al. (2019) Handoff all your privacy–a review of apple's bluetooth low energy continuity protocol. *Proceedings on Privacy Enhancing Technologies* 2019: 34–53.
29. Otte SJ (2017) Whether the department of justice should have the authority to compel apple inc. to breach its iphone security measures. *U Cin L Rev* 85: 877.
30. Hack M (2016) The implications of apple's battle with the fbi. *Network Security* 2016: 8–10.
31. Stephan K (2017) Apple versus the feds: How a smartphone stymied the fbi. *IEEE Consumer Electronics Magazine* 6: 103–104.
32. Nellis S and Cadell C (2018) Apple moves to store icloud keys in china, raising human rights fears. Available from: https://www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raisinghuman-rights-fears-idUSKCN1G8060.
33. Lashinsky A (2012) *Inside Apple: The secrets behind the past and future success of Steve Jobs's iconic brand.* Hachette UK.
34. Simao AMDL, Sicoli FC, de Melo LP, et al. (2011) Acquisition of digital evidence in android smartphones. *9th Australian Digital Forensics Conference*, 116.
35. Lorenzo F, McDonald JT, Andel TR, et al. (2019) Evaluating side channel resilience in iphone 5c unlock scenarios. *2019 SoutheastCon*, 1–7.
36. Ntantogian C, Apostolopoulos D, Marinakis G, et al. (2014) Evaluating the privacy of android mobile applications under forensic analysis. *Comput Secur* 42: 66–76.
37. E. G. Warrants (2019) The great debate. Available from: https://egrove.olemiss.edu/cgi/viewcontent.cgi?article=1000&context=greatdebate.
38. Anagnostopoulos L, Zeadally S, Exposito E (2016) Handling big data: research challenges and future directions. *The Journal of Supercomputing* 72: 1494–1516.
39. Wang X, Shamsi F, Okshtein Y, et al. (2014) Clustering geofence-based alerts for mobile devices. US Patent 8,755,824.

AIMS Press