Investigating Encryption within Android and iOS Mobile Devices and its Effects on Law Enforcement

Mobile devices have become ever more prevalent within the modern world and are integral to the lives of individuals who rely on these devices daily. In 2021, the current number of mobile phones recorded worldwide was 7.10 billion with 89.94% of people owning a mobile phone (Turner, 2019). In addition, the major mobile operating systems such as Android and iOS enjoy a strong market share as together, they both account for over 98% of the global smartphone market share (Stevanovic, 2020). Within mobile forensics, mobile devices yield significant insight into their users, making it a very valuable source of evidence. These devices are sought after during a criminal investigation as it may be the only source of evidence used to convict suspects within an investigation (Beckett, Buller, and Hughes, 2017). Data stored on these devices can be incredibly useful for law enforcement within a criminal investigation. Relevant information includes communication data such as contacts, call logs, messages, emails as well as application data with apps such as Facebook and WhatsApp. Due to the rapid acceleration in this technology, this has made efforts by law enforcement very difficult in accessing and retrieving data from these devices. One of these challenges are the built-in encryption features implemented within mobile devices, which can act as an obstacle to investigators that will need to access these devices. Encryption is used to protect data from being seen by converting it into a non-readable format which if accessed by a third party will be useless without the appropriate decryption key. These built-in encryption features function from the hardware layer to the software layer of the mobile devices (D3, 2017). Ever since the implementation of stronger encryption this has continued to frustrate law enforcement, leading to debate about whether it is right to have abilities that circumvent these features, such as a backdoor. This was most prevalent in the 2016 San Bernardino case between the FBI and Apple which sparked controversy over the access to encrypted data on mobile devices (Encryption Working Group, 2019). The phone, which was recovered from the terrorist in the deadly 2016 San Bernardino shooting, was programmed to delete all its data after ten failed passcode attempts which prompted the FBI to finally ask Apple to help with their investigation into circumventing the device's security features. Apple refused to bow down to the FBI's requests to access the phone because it would harm the security of their devices and their consumers who use them. This led the FBI to seek alternative help which allowed them to circumvent the phone's security features.

The aim of this essay is to compare encryption in Android and iOS mobile devices and how this ultimately affects the efforts of law enforcement in gaining access to data. This essay begins by comparing Android and iOS devices according to multiple factors, such as architecture, attacks, and the debate about the current state of encryption in mobile devices. This will ultimately inform how this affects efforts of law enforcement in accessing mobile devices which will be performed by consulting academic sources and technical documentation. Finally, it will conclude with a summary of the findings of this essay to answer how encryption is one of the key challenges facing law enforcement within the field of mobile forensics.

To understand encryption, it is necessary to discuss what encryption methods have been used on both platforms. Both Android and iOS possess technical documentation which provides information about their security features. Although the methods of encryption don't have to be limited to a specific platform, Android provides two main methods for encryption that are File-Based Encryption (FBE) and Full-Disk Encryption (FDE) (Android, 2019). FBE is available on Android 7.0 and above, with it being required on Android 10 and above. Files and directories are encrypted by the file system entirely instead of the whole disk. FBE comes with a feature called Direct Boot which means encrypted devices, when powered on, will go straight to the lock screen. Each user within the device has two storage locations that are accessible to essential and non-essential applications: Credential Encrypted (CE) storage and Device Encrypted (DE) storage. CE storage is set as a default storage location and only accessible after the user has unlocked the device. DE storage, however, is available during Direct Boot and after the device has been unlocked, meaning essential apps and services are available upon startup. This focus on usability for the user means it sacrifices some security. The separation of the storage means that multiple users are protected because it is not based on a single boot

time password. The introduction of Android 9.0 also released support for metadata encryption. This acts with FBE and means a single key that is present at boot time encrypts content not already encrypted by FBE (Android, 2019). FDE encrypts data at the disk level using a single encryption key; once decrypted, all data can be accessed. The encryption key is combined with the passcode to protect the encrypted files. Android's FDE is based on 'dm-crypt' - a transparent disk encryption subsystem available within the Linux kernel - with the type of algorithm used being 128-bit Advanced Encryption Standard (AES) along with Cipher-Block Training (CBC) and ESSIV: SHA256. The use of FDE prohibits the main functionality of the device from being carried out until credentials have been given (Android, 2019). On the other hand, iOS devices use a file encryption methodology called Data Protection (Apple, 2021) as well as a feature known as a Hardware AES Cryptographic Accelerator. The Data Protection feature on iOS devices is enabled whenever a device passcode is set. Each file that is created, the Data Protection system creates a 256-bit per-file key and gives it to the Advanced Encryption Standard (AES) hardware engine which uses the key it has been provided with to encrypt the file while it is being processed to storage (Apple, 2021). It allows the device to respond to incoming phone calls but also creates a high level of encryption of user data. Applications such as Messages, Photos and third-party apps, by default, employ Data Protection (Apple, 2021). As well as using Data Protection as an encryption mechanism, it also employs the use of a hardware AES cryptographic accelerator to encrypt data held in flash memory (Mohamed and Patel, 2015). The AES accelerator holds two keys, the device unique ID (UID) key and the device group ID (GID) key, which are both AES 256-bit keys. The UID key means that the form of cryptography allows it to be linked to a specific device. If the memory was to be removed from one device to another, the data would still not be able to be read as the filesystem is protected by the UID key (Mohamed and Patel, 2015). To date, several studies have investigated the security mechanisms within mobile devices. According to Mohamed, I. and Patel, D (2015), their research into Android outlined that iOS's defenses were more secure. Several key security features were discussed such as iOS's ability to prevent the decryption of data while in locked mode and remote wiping capabilities, which can be performed through Mobile Device Management (MDM). Other key issues were Android's ability to allow users to make security decisions. This could affect law enforcement progress as phone settings such as file encryption can be activated as well as a passcode (Mohamed and Patel, 2015). Passcode authentication can be bypassed using jailbreaking but can be hampered by if the device has been configured to wipe its data after ten passcode attempts. However, the authors fail to successfully conclude the paper as it omits key details on whether iOS or Android possess more efficient encryption. On the one hand, it does seem to suggest that, on an overall level, iOS could be more secure for its resistance to attack but lacks a discussion on encryption, with the author's statement about iOS possessing a stronger security approach against attacks meaning there is uncertainty about whether this applies to attacks on its encryption methods. In addition, they state that mobile security is still very much a concern. A more recent study investigated security features within Android and iOS using similar features described by Mohamed, I. and Patel, D (2015). According to Garg, S. and Baliyan, N (Garg and Baliyan, 2021), research already carried out into security features between these two platforms was not comprehensive enough. This literature highlighted that due to Android's open-source nature it is more vulnerable to attacks. The complex nature of encryption systems used by Android and iOS can pose a threat to attacks and in this case law enforcement. However, previous research has established that these can be overcome but it is by no means a simple process. Between 2007 and 2014, iOS possessed 408 vulnerabilities with many of them possessing a lower severity. In addition, the U.S. The Department of Homeland Security conducted a report into mobile devices and found that 0.7% of malware targeted iOS (Mohamed and Patel, 2015). The same report also showed that 79% of malware existed on Android devices. In addition, 30 vulnerabilities were disclosed about Android between 2009 and 2013 (Mohamed and Patel, 2015). Although this study provides insight into the vulnerabilities present on both platforms, it lacks specific focus on attacks affecting encryption and is also dated as it was conducted in 2013. Garg, S. and Baliyan, N. (2021) performed a similar set of comparisons in a more recent study. In particular, the vulnerabilities affecting iOS and Android between 2007 and 2019 which for Android was 2563 while iOS had 1655. Common vulnerabilities listed in this study include 'gain privileges' (obtaining root or admin rights), 'bypass something' (circumventing authentication methods) and more. According to Garg and Baliyan (2021), between 2015 and 2019, the distribution of vulnerability types reported for 'gain privileges' was 96% on Android while on iOS it was 4%. This pales in comparison to the vulnerability 'bypass something' which recorded 48% on Android and 52% on iOS. Vulnerabilities that could be related to breaking encryption could be further clarified

as there is lack of it in this paper. The data presentation of some results appears ambiguous particularly in the distribution of vulnerability types in which it was seen that the unidentified vulnerabilities reported comments such as 'Jailbreaking in iOS' and 'Open-source nature of Android' (Garg and Baliyan, 2021).

Jailbreaking can be used as a method of exploiting a locked mobile device to allow root access to the system, with it being referred to as rooting on Android devices. It can be one of the main threats that undermines encryption as described in a paper performed by Teufl, P., Zefferer, T. and Stromberger, C (2013) which analysed threats that could oppose encryption in mobile devices. The aim of this paper was to compare the data encryption systems within Android and iOS. As part of this, a platform agnostic encryption model was created and used common properties available within both mobile encryption systems. This model is then used as a platform to assess the current threats towards encryption with generic attack scenarios being created that would allow the evaluation of both mobile systems. These main threats, within the context of this research, were defined as theft and malware; malware being only considered as jailbreaking. The attacks included using malware, attacking backups stored on the hardware or within the cloud. The results found that iOS was more resistant in its key derivation function which is dependent on the complexity of the user's passcode. Android's file system-based encryption system seemed to be much simpler but more resilient to jailbreak attacks as on every boot-up it would require a passcode to unlock it. This can be circumvented however because of brute force attacks which can be run offline and depending on the complexity of the passcode can be broken by employing other processing capabilities. These findings suggest that no platform triumphs over the other, with both possessing their advantages and disadvantages. Although the method of this paper is clear, the method of data presentation in the comparison between encryption systems could have been more concise and better presented. Ever since FBE became mandatory with Android 10.0, it could be argued that this has made it an easier target for attacks. Cold boot attacks can be used to retrieve encryption keys from a device by performing a memory dump of RAM. Despite the usage of cold boot attacks to target a platform's encryption, it may not be enough due to the wide variety of different devices available. According to Groß, Busch and Müller (2021), the change from FDE to FBE allowed for the creation of a tool called 'fbekeyrecover' which can be used to recover the encryption key from FBE-enabled Android devices due to current tools becoming ineffective. They also created enhancements on The Sleuth Kit (TSK) and the Plaso framework to perform forensic analysis on the FBE enabled EXT4 images. The exact nature of the vulnerability was due to a flaw in its key derivation method which was able to be viewed due to the open-source nature of Android. To perform the analysis, a RAM image of the mobile device was required as well as the encrypted disk. The sample size of the mobile devices included thirteen mobile phones released. Out of the thirteen devices analysed, only three were vulnerable to the key derivation flaw. This included the Google Nexus 5X, Google Pixel XL and the Android Virtual Device. The paper does make note that the flaw that allowed for extraction of the encryption key was fixed for certain versions, so this affected the results of the experiments (Groß, Busch and Müller, 2021). The paper concludes that this method will help introduce research into breaking FBE enabled Android devices. The tool was limited because it was not able to circumvent newer device's encryption. Factors such as the metadata encryption which is used in conjunction with FBE made it resistant to attacks conducted in the paper. It also states that law enforcement may use other methods such as malicious bootloaders and other exploits that target the security of the phone with an example being the attack of its secure boot scheme. Despite reporting in the research that seven devices were found vulnerable to the flaw, it only reported three. This makes it important that data such as this is reported correctly. The sample size could be deemed reasonable for a study such as this but arguably could have included more. The results of this study show that despite breakthroughs in tackling encryption, the wide variety of devices and new additions to these devices severely affects the efficacy of forensic tools, or even causes them to be out of date, making it severely difficult for law enforcement to analyse these devices.

Built-in encryption within mobile devices has severely affected the progress of criminal investigations and caused public debate about access to such devices. In iOS's case, encryption is automatically enabled when the device is set up meaning it will be encountered by an investigator regardless. Furthermore, the result of encryption has prompted debate about law enforcement's ability to access such devices. Jacobsen (2016) argued the effects of encryption within mobile devices has a severe effect on law enforcement. It reiterates many cases where law enforcement, such as the

San Bernardino case, as well as another event in 2015 where a pregnant mother was killed on her doorstep. It was believed by investigators that the identity of the gunman was stored on her iPhone 5. The aim of this paper was to investigate the effects of Android and iOS encryption, in particular FDE, on law enforcement and use these findings to propose an amendment to the Communications Assistance for Law Enforcement Act (CALEA) in order to penalise the manufacturer and the mobile OS provider for each mobile device law enforcement does not have the ability to decrypt (Jacobsen, 2016). In essence, this act enhances the ability of US law enforcement on surveillance and requires telecommunications providers and manufacturers design their equipment to comply with law enforcement surveillance capabilities. Past efforts on remedying legislation were evaluated and an analysis was performed of how these efforts failed, which should inform their proposal to amend CALEA. Penalties to the manufacturer and provider included $127,500, but if they were to make their devices amenable for search warrants then they would be reimbursed. Although the paper provides a very detailed analysis on the effects of encryption, it would have been more effective to include a wider view of encryption within other countries and suggest amendments to their legislation. Despite the requirement of law enforcement to access these devices, it raises serious issues to user privacy and the technical requirements required to amend these technologies to incorporate a 'backdoor' of sorts that would allow them to circumvent phone security features. It would defeat the very nature of encryption and could allow an attacker access into a system if it is implemented incorrectly. According to Abelson et al. (2015), it argues that if such a system were to be implemented it would pose significant security risks that affect human rights and international relations. The technical difficulties faced in implementing these changes would be too difficult and the result would be a more vulnerable system. The aim of this paper was to set out the questions that the government will need to answer if they require access to computer devices. One scenario that was devised was if they assumed that law enforcement had exceptional access to encrypted devices, which demonstrated that it would be problematic due to technical differences and authentication issues (Abelson et al., 2015). Since the encryption key is combined with the passcode to encrypt the device, this would pose issues for access. The findings come together to create a plethora of questions that the government must answer including technical, operational, and legal questions if it is to challenge encryption.

This essay has discussed the reasons for how encryption poses a key challenge in law enforcement capabilities. This has found that generally the threat of encryption poses a significant challenge for law enforcement. Advancements in each platform's encryption methods and the large variety of devices available on the mobile market make it difficult for law enforcement to rely on specific tools. Both Android and iOS pose significant challenges, particularly iOS because its source code cannot be viewed compared to Android being open source. By default, hardware encryption cannot be turned off on iOS devices once a passcode is set which can introduce challenges if mobile devices that need to be accessed. Although iOS may be harder to access, Android encryption is still very difficult to defeat. From the perspective of law enforcement, their capabilities and resources make it difficult to overcome the complex encryption within mobile devices and it is clear action needs to be taken to oppose encryption methods before it becomes too overwhelming to deal with. Despite the need for action on circumventing encryption methods, it would severely undermine the safety of compromised devices and affect the privacy of individuals. In addition, it could be very vulnerable if attackers were to obtain the method of decrypting a device, making the consequences very severe. Therefore, there needs to be careful consideration for challenging encryption as this could affect concerns of privacy and cause significant vulnerabilities within mobile devices.

References:

Abelson, H., Anderson, R., Bellovin, S.M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P.G., Rivest, R.L., Schiller, J.I., Schneier, B., Specter, M.A. and Weitzner, D.J. (2015). Keys under doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications. *Journal of Cybersecurity*, [online] 1(1), pp.69–79. Available at: https://academic.oup.com/cybersecurity/article/1/1/69/2367066 [Accessed 17 Nov. 2021].

Android (2019). *Encryption | Android Open Source Project*. [online] Android Open Source Project. Available at: https://source.android.com/security/encryption [Accessed 18 Nov. 2021].

Apple (2021). *Encryption and Data Protection Overview*. [online] Apple Support. Available at: https://support.apple.com/en-gb/guide/security/welcome/web [Accessed 18 Nov. 2021].

Beckett, P., Buller, G. and Hughes, K. (2017). Your Mobile Device – The Best Piece of Evidence in an Investigation. [online] Alvarez & Marsal | Management Consulting | Professional Services. Available at: https://www.alvarezandmarsal.com/insights/your-mobile-device-best-piece-evidence-investigation [Accessed 11 Nov. 2021].

D3 (2017). *Challenges in Mobile Forensics*. [online] d3pakblog.wordpress.com. Available at: https://d3pakblog.wordpress.com/2017/01/07/challenges-in-mobile-forensics/ [Accessed 15 Nov. 2021].

Encryption Working Group (2019). *Moving the Encryption Policy Conversation Forward*. [online] Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/2019/09/10/moving-encryption-policy-conversation-forward-pub-79573 [Accessed 15 Nov. 2021].

Garg, S. and Baliyan, N. (2021). Comparative analysis of Android and iOS from security viewpoint. *Computer Science Review*, [online] 40, p.100372. Available at: https://www.sciencedirect.com/science/article/pii/S1574013721000125 [Accessed 9 Nov. 2021].

Groß, T., Busch, M. and Müller, T. (2021). One key to rule them all: Recovering the master key from RAM to break Android's file-based encryption. *Forensic Science International: Digital Investigation*, [online] 36, p.301113. Available at: https://www.sciencedirect.com/science/article/pii/S266628172100007X [Accessed 16 Nov. 2021].

Jacobsen, K. (2016). Game of Phones, Data Isn't Coming: Modern Mobile Operating System Technology and Its Chilling Effect on Law Enforcement. *George Washington Law Review*, [online] 85(2), pp.566–611. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2856603 [Accessed 10 Nov. 2021].

Mohamed, I. and Patel, D. (2015). Android vs iOS Security: A Comparative Study. In: *2015 12th International Conference on Information Technology - New Generations*. [online] International Conference on Information

Technology: New Generations (ITNG). Manhattan, New York: IEEE, pp.725–730. Available at: https://ieeexplore.ieee.org/abstract/document/7113562 [Accessed 9 Nov. 2021].

Stevanovic, I. (2020). The One OS to Rule Them All - 33 Android vs iOS Market Share Stats. [online] KommandoTech. Available at: https://kommandotech.com/statistics/android-vs-ios-market-share/ [Accessed 11 Nov. 2021].

Teufl, P., Zefferer, T. and Stromberger, C. (2013). Mobile Device Encryption Systems. In: *Proceedings of SEC 2013: Security and Privacy Protection in Information Processing Systems*. [online] 28th IFIP TC 11 International Conference. SpringerLink, pp.203–216. Available at: https://link.springer.com/chapter/10.1007/978-3-642-39218-4_16 [Accessed 9 Nov. 2021].

Turner, A. (2019). 1 Billion More Phones Than People In The World! BankMyCell. [online] BankMyCell. Available at: https://www.bankmycell.com/blog/how-many-phones-are-in-the-world [Accessed 11 Nov. 2021].