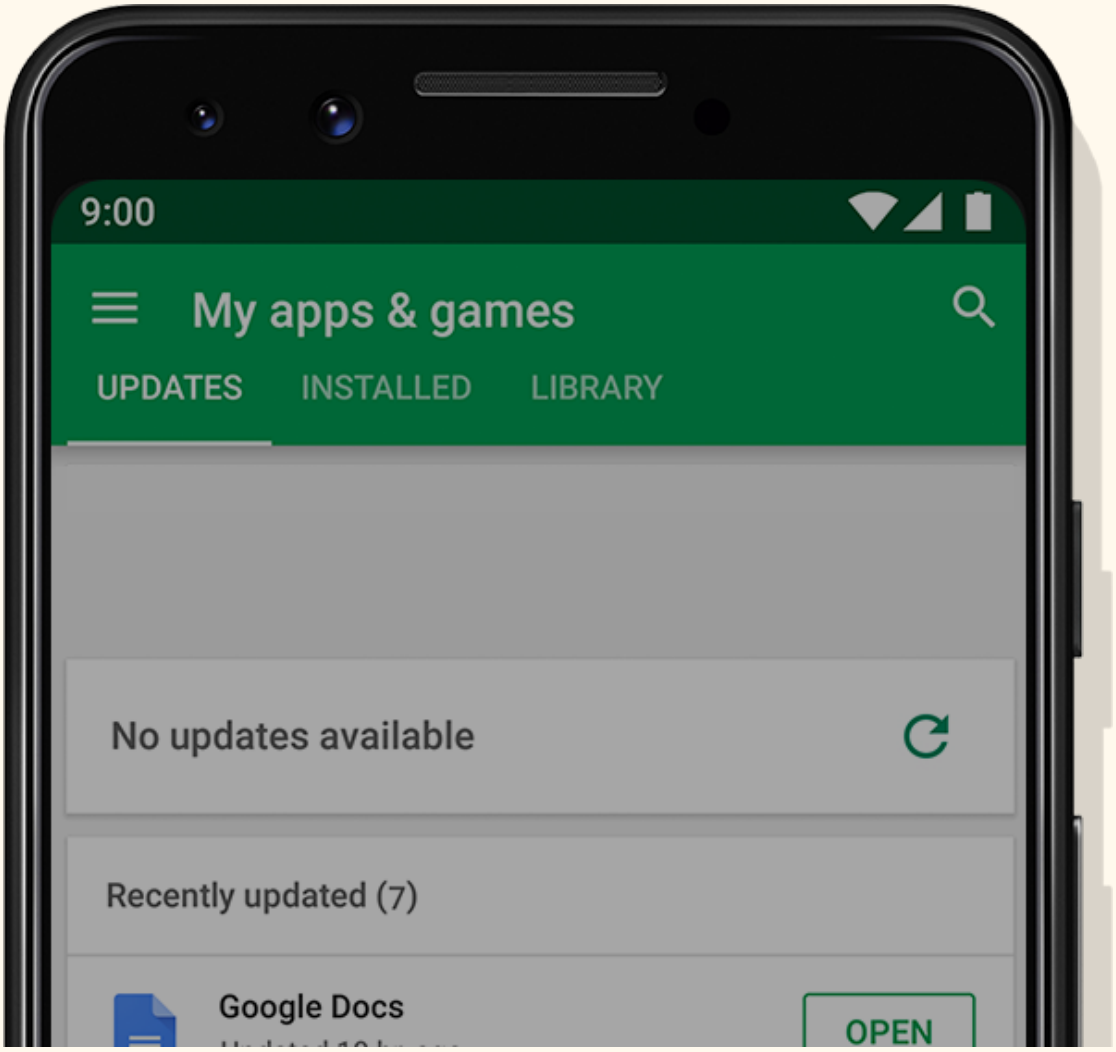
CMP416 DIGITAL FORENSICS

MOBILE FORENSICS
ANDROID SECURITY MECHANISMS

By Andrew R. Calder



Android Security Mechanisms

Mobile devices are evolving more quickly than ever, leading an increase in complexity in the context of forensics. Unlike traditional digital forensics (PC / Laptop) in which only a handful of vendors are commonly used, there are multitudinous mobile device manufacturers. With a market share approaching 85% worldwide - 84.8% as of 2018 (*IDC, 2018*), Android is by far the most widely used mobile operating system. However, manufacturers commonly offer their own flair on the Android operating system, using proprietary software and technologies which reduce inter-device accessibility; Samsung has *Samsung Experience*, Huawei has *EMUI*, Sony has *Xperia*. Only a few vendors such as Nokia and Google use what is referred to as *Stock* - the core release of Android. Additionally, each of these manufacturers release at least 2 new devices every year - investigators have to not just remain up to date with operating system changes but hardware changes too.

In the past, Android security was considered poor, it was buggy and the vulnerabilities found were crippling. Take stagefright for example; victims couldn't do anything to prevent infection - one simple MMS and it was all over- and it affected all versions of Android 2.2 to 5.1. These days Android security is a bit more robust and stock android includes many security mechanisms; File-based Encryption, Metadata encryption, Verified Boot (AVB), KeyStore, and DeviceManager -to name a few. Additionally, vendors may implement their own security mechanisms - for instance Samsung uses *Knox*. While these changes protect user data and privacy, for digital forensic investigator the changes lead to more headaches.

Starting with Android 7.0, Google began rolling out File-based Encryption; instead of encrypting the entire storage volume as a single unit, each individual file is encrypted. Additionally, as of Android 9.0 Pie with metadata encryption, a key present only at boot encrypts any content not otherwise encrypted with File-based. The key is protected by KeyMaster which is in turn protected by verified boot (*AOSP, 2018*). Forensic investigators might have to break the encryption to extract device data - which is difficult to do without intervention.

The case of the FBI versus Apple was a turning point; the security mechanisms on the iPhone 5c prevented FBI investigators from extracting data from a device that belonged to an individual tied to the San Bernardino Shooting (*Lichtblau and Benner, 2016*). When apple refused to provide any assistance in unlocking the device -taking a stance of absolute privacy and security regardless of the situation- investigators were forced to look into alternatives. For an

undisclosed sum, Israel-based firm Cellebrite offered to unlock the device and as of February 2018 they "currently have the ability to get around the security of devices running iOS 11" (*Brewster. T, 2018*). While this particular case doesn't relate to Android, the principles are the same - a solution exists, if you can afford it. What is the likelihood of local police departments having access to this level of tooling? For comparatively low profile cases - though involving serious crimes nonetheless - these sorts of resources are simply not available.

Device encryption is far from the only hurdle law enforcement faces. In 2014, Cambridgeshire, Derbyshire, Nottingham, and Durham police all reported devices seized as evidence had been remotely wiped - with 6 devices reported by Dorset police to have been wiped in one year (*Wakefield, 2014*). Both Android and iOS devices offer *remote wipe*/secure erase functionality; a great idea in principle -securely and remotely wipe all your data from your device in case it is stolen. In practice, such mechanisms are part of the reason Police have to use Faraday bags/cages on devices from the moment they are seized. Using a Faraday covering prevents the phone from connecting to any networks and thus prevents the wipe command from ever reaching them. A very recent case in New York reaffirmed the need for this sort of precaution; a woman believed to be the driver in a drive by shooting remotely wiped her phone after it was seized by Police. While she was charged with destroying evidence, there could have been incriminating data on the device involving other suspects (*Mathews, 2018*). In mobile forensics, such mechanisms are referred to as *Anti-Forensic* (*Tamma and Mahalik, n.d.*) as they make digital investigations significantly more difficult.

Resources available to local police forces are insufficient for dealing with crimes involving mobile devices. In PEEL: Police Effectiveness 2017 (Justiceinspectorates.gov.uk, 2017), it is reported that there is a backlog of 13,280 devices waiting to be examined. This could be due to the sheer variety of devices, lack of sufficient tooling, lack of training, or the unique challenges presented. For instance, consider data integrity - one of the fundamental rules of digital forensics - data that is considered evidence should not be modified. Thus, extracted device data should be a forensic match of the data present in the device. Unfortunately, this is practically impossible, without switching off a phone there is no way to guarantee that background processes which may make changes to files will not be running. Switching off a device comes with its own problems - it may activate a lockout feature or alter evidence on the device (Best Practices For Seizing Electronic Evidence, 2015).

These days, lockout features don't only activate if the device has been switched off entirely. In fact, even something as simple as being in an unfamiliar place can trigger a soft-lockout, requiring the users passcode to proceed. With *Smart lock* - a toolset for Android that primarily focuses on making it easier to access your devices, features were added that engage a

soft-lockout when in an unfamiliar location or your device is handled abnormally (*Google Account Help, 2018*). A soft-lockout is not much of an issue if a suspect cooperates and provides access to the device. However, if police were forced to look into other means of accessing the device, such as attempting to bypass or trick biometric security mechanisms, a soft lockout would prevent them from doing so - as it requires the password or pin to be entered.

In the USA, citizens are protected from having to unlock their phone by the 5th Amendment, but due to laws not being updated, biometric unlocks are exempt from the protections. In the UK under RIPA (Regulation of Investigatory Powers Act 2000), everyone must give up their passwords or otherwise provide access to their devices upon request. Failing to disclose a password or otherwise provide access to a device is punishable by upto 5 years in jail. What if the owner of the device literally cannot cooperate; what if the owner is dead? Biometric security is not just a legal issue but also an ethical one.

While there are no publicly known examples of such a situation in the UK, there are several in USA. In the case of Abdul Razak Ali Artan - an ISIS associated terrorist who had gone on a killing spree before being shot dead by police, an FBI agent applied Abdul's index finger to the home button of the phone found on him. Unfortunately for the FBI, the phone was already locked and required a password. Meanwhile, at local police level, reports have surfaced stating it is now relatively common for fingerprints of deceased to be used to provide device access. For example, in overdose cases, the information on the victims phone can lead Police to their dealer (*Brewster, 2018*). Assuming police don't have access to the non argumentative, conforming dead body of a individual, can they reasonably use biometrics to unlock the device?

At the 2014 Chaos Computer Club, a security researcher who goes by the handle *Starbug,* used a high resolution photo to construct a working model of the German Defense Minister's fingerprint which was able to unlock their personal phone ('*Starbug*' *Krissler, 2018*). Another recent example exhibits police actually using this technique; investigators approached Michigan State University professor ,Anil Jain, requesting help breaking into a victim's phone. Police had scans of the victim's fingerprints from when he had been arrested previously, which were provided to Anil who was tasked with 3D-printing the dead man's fingerprints to get into his smartphone.

Aside from the ethical issues, these cases present questionable legal issues. The 5th Amendment protects individuals from being held for committing a crime unless charged by police, it also protects against self-incrimination. In the case discussed above, the reasoning is fairly simple "the fingerprints are of the deceased victim, not the murder suspect. Obviously,

the victim is not at risk of incrimination" - Bryan Choi (*Engadget, 2018*). However, for living suspects -and the UK- there have been no cases to set the precedent and as such no legal standards have been agreed upon.

As phone manufacturers race to maximise screen space, the fingerprint sensor has been moved to inside the screen. The location isn't really the point of interest, but rather the technology that enables it. In 2018, Qualcomm released their *3D Sonic Sensor* - essentially an ultrasonic fingerprint sensor which uses soundwaves to 'read' your fingerprint. Not only is the sensor more accurate than its optical counterparts (can read depth differences), but it can also detect a pulse (*Dolcourt, 2018*). The depth read would reduce the effectiveness of image scan based fingerprint copies, and checking for a pulse would prevent dead bodies and high quality 3D printed copies from unlocking the device all together. Even if the police did have the resources to buy or develop a fingerprint cloning system, it would likely be useless on devices released after 2018.

Although fingerprint sensors are the most common biometric sensor on mobile devices, facial recognition is on the rise. Unlike the iOS implementation (Face ID), Face Unlock on Android does not explicitly require any special sensors - it just uses the front facing camera. 'Face Unlock' first appeared in Android 4.0 Ice Cream Sandwich, in 5.0 it was renamed 'Trusted Face' - and still it did not require any special sensors. While Apple's implementation is not tricked by simple exploits such as holding up a picture of the person, the same cannot be said about Trusted Face. Due to the insecurity of trusted face, google appears to have taken a security through obscurity approach -the option to enable face unlock is very well hidden in Android 9.0 Pie and comes with many warnings about the security implications.

Biometric security mechanisms on Android might be exploitable by forensic investigators for now, but with the direction manufacturers are taking -promises of better security and higher accuracy- it is unlikely that biometric security will continue to be a viable lockscreen bypass. Additionally, since a soft-lockout effectively disables all use of biometric authentication, the benefits to investigators in real world scenarios are questionable.

In another case of security through obscurity - albeit unintended- Chinese phones present a growing challenge for forensic investigators. Chinese Android manufacturers such as OnePlus, Huawei and Xiaomi have become well known globally in recent years. However, Chinese phone manufacturers are relatively young compared to their western counterparts and don't always conform to standards, leading to confusion and caution when analysing them; it can be uncertain how a device will behave in otherwise certain scenarios.

The severe lack of a manufacturing standards authority makes Chinese phones particularly difficult to analyse for various reasons. Firstly, is the way they are produced - the devices are made for a single production run; the manufacturer has little concern for post-sale support and just wants to churn out devices. Unstable and inconsistent OS experiences are not uncommon, nor is difficulty finding (due to these OS quirks) compatible forensics tools. Furthermore, connectivity on the devices may not follow the standards associated with those parts - for instance the power and data lines may be switched to force sales of a manufacturers proprietary accessories, with little regard for availability of these accessories outside of China (*North, 2012*).

The seeming carelessness of these Chinese companies isn't all bad for forensic investigators, in fact sometimes they make gaining access to the device easier. In 2017, it was revealed that OnePlus had mistakenly been shipping a Qualcomm engineering test application in their devices for years (*OnePlus Community, 2018*). The application -'EngineerMode'- is accessible through a dialer shortcut "*#808#*", which is accessible whether the devices are locked or not. The application contains various production tests, one of which "escalatedUp" -if selected- would allow root access over Android Debug Bridge (ADB). While 'EngineerMode' was limited to OnePlus devices, there are other similar stories of debugging and engineering tools present in the final product.

As touched on earlier, there are a wide variety of mobile devices. These devices may or may not conform to supposed industry standards. It is becoming increasingly difficult for forensic tools to support all devices, or at very least perform basic functions on all devices. Of the three largest Logical Acquisition tools; 'XRY Logical', 'Oxygen Forensic Suite', and 'Katana Lantern 4', only one publicly lists their supported devices - 'Oxygen Forensic Suite' claims to support more than 200 devices. According to *GSMArena,* over 400 new devices launched last year - more than double the total supported devices of the forensics tool (*GSMarena, 2018*).

The unsustainable level of support required isn't the only issue with mobile forensic tools, there is also the financial cost. GrayShift's *GrayKey* is a bruteforce unlock tool for pin secured lockscreens, it can crack a four digit pin in anywhere from a few minutes to a few hours, and a six digit pin in around three days. Which may seem like a long time but its significantly faster than any other similar systems. The catch? It costs $15,000 - and that's just for a one year license. Despite the seemingly steep cost, *GrayKey* is actually one of the cheaper options. In comparison, Cellebrite - the company famously involved in the San Bernardino shooter case- charges a reported $1500-$2500 per device. It is extremely unlikely that in the current climate of police spending cuts that such devices/tools would be made available to forensic investigators with the exception of high priority cases such as acts of terror (*BBC News, 2018*).

Security Mechanisms protect users data on mobile devices. On Android, a variety of security mechanisms are available to users -from passwords and pins, to biometric authentication and device encryption. Devices that require password or pin authentication may be unlockable using costly software or hardware tools, or cooperation from the device owner. However, biometrics, encryption, and even country of origin can add additional challenges and costs both in terms of forensic tool development, and digital forensic investigation. With the current climate of police funding cuts, forensic investigators simply do not have the resources required to complete their work, evidenced by the backlog of 13,280 devices waiting to be examined. Further development of Android security mechanisms is only going to improve users privacy and security in the future, will investigators be able to keep up?

References

Justiceinspectorates.gov.uk. (2017). PEEL: Police effectiveness 2017 - A national overview. [online] Available at: https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/peel-police-effectiveness-2017-1.pdf [Accessed 11 Nov. 2018].

IDC. (2018). IDC - Smartphone Market Share - OS. [online] Available at: https://www.idc.com/promo/smartphone-market-share/os [Accessed 2 Dec. 2018].

AOSP. (2018). Metadata Encryption | Android Open Source Project. [online] Available at: https://source.android.com/security/encryption/metadata [Accessed 2 Dec. 2018].

Lichtblau, E. and Benner, K. (2016). U.S. Says It Has Unlocked iPhone Without Apple. [online] New York Times. Available at: https://www.nytimes.com/news-event/apple-fbi-casehttps://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html [Accessed 5 Dec. 2018].

Brewster, T. (2018). The Feds Can Now (Probably) Unlock Every iPhone Model In Existence. [online] Forbes.com. Available at: https://www.forbes.com/sites/thomasbrewster/2018/02/26/government-can-access-any-apple-iphone-cellebrite/#2054fed8667a [Accessed 8 Dec. 2018].

Wakefield, J. (2014). Phones held by police remotely wiped. [online] BBC News. Available at: https://www.bbc.co.uk/news/technology-29464889 [Accessed 10 Dec. 2018].

Mathews, L. (2018). Suspect Remotely Wipes iPhone X While It Sits in Police Evidence - Geek.com. [online] Geek. Available at: https://www.geek.com/tech/suspect-remotely-wipes-iphone-x-while-it-sits-in-police-evidence-1760393/ [Accessed 12 Dec. 2018].

Tamma, R. and Mahalik, H. (n.d.). Practical mobile forensics. 3rd ed. Packt Publishing.

Best Practices For Seizing Electronic Evidence. (2015). 4th ed. U.S. Department of Homeland Security: United States Secret Service, pp.11-13.

Google Account Help. (2018). Google Smart Lock. [online] Available at: https://support.google.com/accounts/answer/6160273?hl=en [Accessed 11 Dec. 2018].

Brewster, T. (2018). Yes, Cops Are Now Opening iPhones With Dead People's Fingerprints. [online] Forbes.com. Available at: https://www.forbes.com/sites/thomasbrewster/2018/03/22/yes-cops-are-now-opening-iphones-with-dead-peoples-fingerprints/#3414f5e2393e [Accessed 11 Dec. 2018].

Dolcourt, J. (2018). Qualcomm announces first ultrasonic fingerprint reader: Headed to the Galaxy S10?. [online] CNET. Available at: https://www.cnet.com/news/qualcomm-announces-first-ultrasonic-fingerprint-reader-headed-to-the-galaxy-s10/ [Accessed 11 Dec. 2018].

Engadget. (2018). Police get dead man's finger 3D-printed to unlock his phone. [online] Available at: https://www.engadget.com/2016/07/21/police-get-dead-man-s-finger-3d-printed-to-unlock-his-phone/ [Accessed 12 Dec. 2018].

'Starbug' Krissler, J. (2018). I see, so I am... You. [image] Available at: https://www.youtube.com/watch?v=VVxL9ymiyAU&feature=youtu.be [Accessed 9 Nov. 2018].

North, K. (2012). The Chinese Cell Phone Menace. [online] Forensic Magazine. Available at: https://www.forensicmag.com/article/2012/05/chinese-cell-phone-menace [Accessed 12 Dec. 2018].

OnePlus Community. (2018). What is EngineerMode?. [online] Available at: https://forums.oneplus.com/threads/what-is-engineermode.680377/ [Accessed 12 Dec. 2018].

Gsmarena.com. (2018). Phone Finder results - 2018-2018 GSMArena.com. [online] Available at: https://www.gsmarena.com/results.php3?nYearMin=2018&nYearMax=2018 [Accessed 13 Dec. 2018].

BBC News. (2018). Ministers 'unaware of police cuts impact'. [online] Available at: https://www.bbc.co.uk/news/uk-45477960 [Accessed 13 Dec. 2018].