Mobile Forensics
Device Authentication

Jordan Gribben

CMP416: Digital Forensics 2

BSc Ethical Hacking Year 4

2021/22

Smartphones have become an essential part of modern society and communication, with around 1.38 billion devices being sold in the year 2020 alone. (O'Dea, 2021) Each device can contain extremely personal data unique to each user, for example, location data, health information and access to user's various accounts. Due to this, devices must have a way to protect user data to ensure it cannot be accessed by anyone who picks up the mobile device. This is done via device authentication, the most common forms of device authentication are passcodes and biometric authentication. However, with this many devices worldwide continually gathering data it is inevitable that some devices will hold essential information that can be used as evidence in a criminal investigation. This poses as a problem for criminal investigations, as while the devices may hold key information that is vital to an investigation the various authentication method found on mobile devices can prevent law enforcement agencies from gaining access. While this is extremely useful for users as it shows their data is secure it can have a serious impact on criminal investigations.

This allows for the question, what are some of the key challenges facing law enforcement in the field of mobile forensics, to be asked. Devices authentication will be investigated further to see what problems it poses for law enforcement and how they get around various authentication methods.

Adding any form of authentication to a device is a keyway to keep the data it contains secure, the use of a good passphrase, passcode or even biometric authentication will greatly increase the security of a device. With smart devices using passphrases and passcodes since their inception, they are the most used form of authentication for a mobile device, these are also required to set up biometric authentication. When using a passcode for authentication on iPhones Apple requires a minimum four digit passcode with six digits being the default, a custom alphanumeric code is also available. If an incorrect passcode is entered multiple times it locks the user out for a set period, with this time expanding if an incorrect password continues to be entered. iPhones also have the option to erase the devices data after ten failed passcode attempts, this will wipe the phone completely to a state where it can only be restored by a backup (Apple, 2021). While the passcode options are extremely useful for its users it can create issues for law enforcement, one such issue is the erase data option found on iPhones. Due to this law enforcement would not be able to try various passcodes in case they lose the data they need for an investigation, this forces them to use other methods to get the devices data.

Another method of device authentication can be found with the use of biometric authentication. This is done by taking users biometric data such as fingerprint or face data and using this to authenticate the user. Due to this data not being 'guessable' unlike a passcode, biometric data can be a far more secure method of device authentication, when used properly. Fingerprint biometrics can be found on most modern day smartphones, with around 60% of smartphones that shipped in the year 2018 having a form of fingerprint sensor. (O'Dea, 2020) iPhone's started using fingerprint authentication with the release of 'TouchID' in 2013 alongside the release of the iPhone 5s, this technology was then used in all following iPhones until the iPhone X. Fingerprint authentication is extremely popular both to users and to developers, for developers it is a cheap and simple way to add a strong form of security onto a device. For users it provides a simple and coinvent way to keep their data secure without having to constantly input their devices passcode. A lot of mobile devices also come with a button on the front of the device, this button usually acts as a method to get to the home screen on the device however, developers have use it to implement their fingerprint sensors. This adds even more convenience to users as this button is likely to be pressed to turn the phone on, instantly unlocking it before seeing the lock screen. However, some sensors are placed in other locations such as the back or side of the phone.

When using fingerprints for biometric authentication there are various ways to collect the biometric data. One way this is done is with capacitive fingerprint technology, these sensors work by using fingers as conductors to complete the circuit and 'scan' the finger. The fingerprint is taken by using a

capacitive surface to detect where the skin comes into contact, due to a fingers various ridges each area will have a different level of resistance. Using the varying levels of resistance, the sensor can form the various characteristics of a user's fingerprint such as ridges, scars, and patterns. Due to the capacitive sensor using fingers as conductors to complete the circuit this makes them harder to spoof. (Dongdong, 2017)

Apple's TouchID is based around capacitive sensor technology, with the data from TouchID being stored directly onto the smart device and not saved on the cloud, this method is called Secure Enclave. Apples Secure Enclave biometric data is stored as a mathematical representation of the data for added security, to ensure that if a data leak were to happen the 'raw' data would not get out. Apple are purposefully vague on this mathematical data and the way it is stored to ensure it stays as secure as possible. TouchID uses various safeguards, this safeguard is in place to ensure that devices can only be accessed by an authorized user. The safeguard in place will require the user to enter their passcode if any of the following conditions are met; If the device has been restarted, security settings have been changed, if a user has exceeded the amount of TouchID attempts, if 48 hours has passed since the device was previously unlocked. (Apple, 2017)

Optical sensors are another way to obtain fingerprint data, these sensors work by shining light from a screen onto the finger to get an image of the fingerprint, this technology is commonly used with in-display fingerprint scanners. (Qiu, 2014) This method of gaining the fingerprint data is less secure than a capacitive sensor due to optical sensors taking pictures of the finger. If a user's fingerprint was captured and put on a plastic sheet, the captured fingerprint could be placed on top of the biometric sensor to unlock the phone.

Fingerprint biometric authentication is an extremely useful feature of mobile devices as it provides users with a strong and simple way to secure a device. However, it does create some issues for law enforcement. For example, if an iPhone were to be seized law enforcement would only have 48 hours to get the suspect to unlock the phone via biometric authentication. This leaves law enforcement with very small time frame to get a suspect to unlock a device in this way.

Another form of biometric authentication that is used in mobile devices is facial recognition, this technology uses mobile devices font facing cameras too look at the users face to determine if they are an authorised user. Facial recognition technology makes use of various algorithms to identify and map faces, some algorithms look to identify specific facial features such as size/shape of nose. (Park, et al., 2014) Facial recognition on certain devices can be unreliable, this is due to some facial recognition technology being easily confused when facial features are changed such as, shaving a beard and wearing glasses. Due to this unreliability a passcode/word is required alongside facial recognition technology to ensure users always have access to their device.

With the introduction of the iPhone X Apple introduced facial recognition to their devices in the form of 'FaceID'. FaceID uses the iPhone cameras 'TrueDepth' system, this system uses an infra-red camera that takes 30,000 reference points on a user's face, this allows the iPhone to take the geometry of the users face and use it to create a depth map. This mainly focuses on specific facial features such as the mouth, eyes and nose. Unlike android devices FaceID does not struggle to correctly identify users after a facial change such as putting on glasses or shaving. According to apple the odds of FaceID falsely identifying a user for someone else is around 1 in 100,000, compared to TouchID where Apple say the odds are 1 in 50,000. To avoid the device from being unlocked by accident or forcefully unlocked FaceID requires that users look directly into the device. (Apple, 2021) A liveness check is also performed, one way this is done is by checking to see if the users eyes are open in case someone try's to unlock a device while the authentic user is sleeping. The Secure Enclave storage method is also used

with FaceID once again storing it as mathematical data to ensure that the raw facial data is stored on the device.

While fingerprints and facial recognition are the most used method of biometric authentication, there has been other method that have appeared in mobile devices throughout the years, one of these methods is voice recognition. The google assistant that can be found on various android devices was previously able to unlock android devices before the feature was removed around version 9.0 of the google app. (Fisher, 2019) This feature was removed due to the google assistant's ability to tell the difference between different user's voices, this allowed this form of authentication to be easily bypassed by someone mimicking an authenticated user's voice or playing back an audio recording of an authentic user's device. Another form of biometric authentication that has been used in mobile devices was an iris-scanning system. This system developed by Samsung uses a specialised camera within the mobile device that uses an infrared LED to capture a user's iris pattern. However, it was then discovered that this system could easily be bypassed by having a high resolution image of an authentic user's iris and overlaying this onto a contact lens.

Due to biometric data being nearly impossible to change if a data breach were to occur and the user's biometric data were to get leaked, it would significantly weaken that user's security on all devices and applications that contained that data. This would also weaken any future devices/application that the user decided to apply biometric data to. Therefore, it is essential all biometric data is kept as secure as possible such as making sure the data is encrypted to a good standard, Apples Secure Enclave is a good example of how biometric data should be stored. Due to the highly sensitive nature of biometric data, there is a high level of security around both the data itself and the methods used to authenticate this data. When a forensic analysis takes place on a mobile device trying to bypass the biometric authentication will prove to be challenging due to the high level of security, instead it would be easier for other authentication systems such as passcodes to be targeted during forensic analysis. Mobile devices will tend to have a weaker 'entry point' in their security than the biometric data, these areas are where forensic analysts will target. This is especially true if the device is running an out-of-date OS as these tend to have known vulnerabilities, that may allow for data from the device to be pulled without having to authenticate the device. Finding a way to bypass authentication essential, if a forensic investigation where to rely on brute forcing a passcode authentication system it could take days to crack manually, wasting precious investigation time. Additionally, if an incorrect passcode is entered too many times it is possible that all data on that device, this could lead to law enforcement losing key evidence. To keep their devices secure and their unbiased position companies such as Apple refuse to help law enforcement during forensic analysis of their devices. One such case was in 2016 with the FBI investigating and iPhone 5c belonging to Syed Rizwan Farook, where Apple famously refused to unlock the iPhone for the FBI when they request for a new version of Apples operating system to be created. Apple refused as it would undermine their devices security, this then let to a legal dispute between Apple and the FBI which was dropped when the FBI announced they managed to unlock the device without Apple. (Cook, 2016)

Due to the time, it would take to brute force devices, and that companies will not cooperate with law enforcement forensic investigators turn to third party tools and software to analyse devices. One such tool is GrayKey, (Lorenzo, et al., 2019) this tool is used by federal law enforcement in the united states of America like the FBI. While the length of time to crack a devices passcode various based on the passcode itself, GrayKey claims that for a six digit passcode it could take up to three days if not longer to be cracked. (Reed, 2018) According to Greyshift, even if a device is disabled a GrayKey device will be able to work with it. Due to this GrayKey also seems to bypass the rule of erasing the data after 10 failed passcodes. GrayKey will unlock a device then download all the contents onto the GrayKey device, this data can then be forensically analysed. This is a fantastic tool for law enforcement to get around device authentication with it coming in two different models, one that requires an internet

connection, can only be used on a singular network, and has a limited number of unlocks before having to pay for more. The second model can be used without an internet connection and has an unlimited amount of uses. However, while this is a great tool for forensic analysis it does have some down sides, the first major downside comes with the second model and the public. If the second model was stolen from law enforcement by a malicious actor, they would be able to use it to access data from other devices. Additionally, the GrayKey device is no doubt exploiting a vulnerability found within iPhones, once Apple have patched this vulnerability any iPhone on a iOS version after this patch will potentially no longer be compatible with the GrayKey device rendering it useless in some cases. Since technology is constantly updated it poses challenges for forensic analysts. Since various forensic tools rely on specific vulnerabilities if these are patched out in an update it could potentially make these tools unusable. Therefore, forensics tools do not always disclose the vulnerability they rely on and why the security of these devices is kept secretive, to ensure no major vulnerability is found. As technology advances, forensic analysts must also, to ensure they can still find the data they need.

United States law differs greatly from that of the UK, one of the greatest differences between the two is the US constitution. The constitution contains various amendments that grant US citizens various rights, one major amendment that has been a topic of conversation regarding mobile devices is the fifth amendment. The fifth amendment grants the US citizens the right against self incrimination, allowing them to refuse to answer any police questions that lead to them incriminating themselves. This has caused a massive debate relating to biometric authentication, discussing whether attributes such as fingerprints or facial features come under this amendment. Due to the fifth amendment preventing against self incrimination, law enforcement are not allowed to coerce a suspect into giving away any information that may unlock their device such as a passcode. However, biometric data is not fully covered under the amendment with it varying on a court by court basis. For example, in Minnesota a State v Diamond case was held, this case concluded that using fingerprint biometrics was not a violation of the fifth amendment, this was appealed but ultimately failed as the court ruled that the production of a fingerprint is not testimonial and therefore does not violate the constitution. (Lemus, 2017) Additionally, some courts have deemed that it is not a violation the constitution as providing a fingerprint does not require any mental process compared to providing a passcode. (Langston, et al., 2019) However, other courts have deemed it against the fifth amendment to get biometric data from suspects. In one case a court argued that since the biometric data can be used to unlock a device it confirms ownership of the device. Since devices contain persona data such as banking information, which would normally be blocked behind a passcode or password, using a biometric lock was found to be no different than securing a device with a passcode. Due to this the court found that getting a suspect to unlock their device with biometric data would be unconstitutional and protected under the fifth amendment. (Chase, 2020)

However, unlike the US if a suspect in the UK were to refuse to unlock a device the suspect can be prosecuted under section 49 of the Regulation of Investigatory Powers Act was 2000. If the police have obtained permission from the courts to request the information from a suspect and the suspect refuses, they can then be charged under the act. If someone were to be sentenced under this act, they would get a maximum of 2 years, unless it is a matter of child endangerment or national security in which case it is extended to 5 years. This law is great for law enforcement as a suspect's device can still be forensically analysed even if not unlocked by the authorised user, if this were to happen and condemning evidence were to be found the suspect would then face a longer jail sentence due to breaking this law as well as another.

Overall while device authentication does cause issues for law enforcement in the field of mobile forensics, there are many ways law enforcement can get round these issues. One way to get round this is third party tools, these tools allow for forensic analysis not just to unlock a device but to extract the data from that device as well, allowing them to analysis the data and find the evidence they need.

Additionally, court orders may be obtained to get around these issues. These court orders will require suspects to hand over the information needed to unlock a device, this can then be given forensic analysts full access to the device to find the data they need.

References

Apple, 2017. *About Touch ID advanced security technology.* [Online]
Available at: https://support.apple.com/en-us/HT204587
[Accessed 28 October 2021].

Apple, 2021. *About Face ID advanced technology.* [Online]
Available at: https://support.apple.com/en-gb/HT208108
[Accessed 2 November 2021].

Apple, 2021. *Use a passcode with your iPhone, iPad or iPod touch.* [Online]
Available at: https://support.apple.com/en-gb/HT204060
[Accessed 29 October 2021].

Chase, A., 2020. *Secure the Smartphone, Secure the Future: Biometrics, Boyd, Warrant Denial and the Fourth and Fifth Amendments,* San Francisco: UC Hastings College of the Law.

Cook, T., 2016. *A Message to Our Customers.* [Online]
Available at: https://www.apple.com/customer-letter/
[Accessed 8 November 2021].

Dongdong, W., 2017. *Introduction of capacitive fingerprint sensor,* Beijing: Institute of microelectronics, Tsinghua University.

Fisher, C., 2019. *'OK Google' will no longer fully unlock your phone.* [Online]
Available at: https://www.engadget.com/2019-03-01-ok-google-voice-match-unlock-update.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAANFNCNP6MsXhhh4mENRy4tuXSINILe5_-39yjcIRJSVGZmI8hXlJp2cohHSkVEyCeej8q3-n4f91tMJvPbcQGUkRLOCHcDGvy
[Accessed 8 November 2021].

Langston, J., Callahan, D. W. & Popinski, J., 2019. *Mobile Devices and the Fifth Amendment,* Birmingham, alabama: ISSA.

Lemus, E., 2017. *When Fingerprints Are Key: Reinstating Privacy to the Privilege Against Self-Incrimination in Light of Fingerprint Encryption in Smartphones,* Dallas: SMU Dedman School of Law.

Lorenzo, F. et al., 2019. *Evaluating Side Channel Resilience in iPhone 5c Unlock Scenarios,* Mobile: IEEE.

O'Dea, S., 2020. *Share of smartphone shipments with a fingerprint sensor worldwide from 2014 to 2018.* [Online]
Available at: https://www.statista.com/statistics/804269/global-smartphone-fingerprint-sensor-penetration-rate/
[Accessed 28 October 2021].

O'Dea, S., 2021. *Number of smartphones sold to end users worldwide from 2007 to 2021.* [Online]
Available at: https://www.statista.com/statistics/263437/global-smartphone-sales-to-end-users-since-2007/
[Accessed 1 November 2021].

Park, Y. Y., Choi, Y. & Lee, K., 2014. *A Study on the Design and Implementation of Facial Recognition,* Asan: Department of Computer Engineering, Sunmoon University, Korea.

Qiu, L., 2014. *FINGERPRINT SENSOR TECHNOLOGY,* Shanghai: Next Biometrics.

Reed, T., 2018. *GrayKey iPhone unlocker poses serious security concerns.* [Online]
Available at: https://blog.malwarebytes.com/security-world/2018/03/graykey-iphone-unlocker-poses-serious-security-concerns/
[Accessed 5 November 2021].