Basic access control mechanisms in Android devices – A high—level look

Ekku Jokinen

CMP416: Digital Forensics 2

BSc Ethical Hacking Year 3 (Accelerated)

2019/20

.

Abstract

Mobile forensics investigations present multiple unique challenges, many of which differ from regular digital forensics investigations regarding computers. Issues such as finding suitable tools, acquiring forensically sound data, anti-forensics methods meant to hide, encrypt or wipe data, and authentication mechanisms designed to prevent access to devices. This essay analyzes the most basic security features found in most Android smartphones, how they prevent unauthorized access to the devices and what it takes to bypass each of them. The main purpose of the essay is to provide a high-level view of these different security features and describe the skills and knowledge needed to circumvent them. The challenges arising from these security mechanisms are not necessarily related to how complicated they are to bypass, but rather the fact that each one involves a different set of knowledge regarding the bypass itself and the tools needed.

.

Modern Android smartphones have several different options to prevent unauthorized access to the applications and data stored on the device. By default, the different mechanisms are usually a swipe pattern, a PIN code, and a password. In addition, there can be several others, for example, hardware-level encryption, automatic and remote data wiping, fingerprint sensors and facial recognition. In addition to these phone dependent security protections, most users have a SIM card in their phone allowing them to send and receive calls and messages. This adds another security layer, a PIN and PUK code, that has to be bypassed in order to access the different kinds of data stored on the SIM card. Some of the more advanced security features are only present in high-end smartphones where the manufacturer has possibly implemented a custom version of the Android operating system (Bittium, no date). An investigator should not have to worry too much about facing such devices on a regular schedule as they are often hard for regular consumers to buy and often are very expensive.

All of these different security features present a potential problem to an investigator who needs to access the contents of a smartphone without the cooperation of the original device owner. For such cases, every mobile forensics investigator should understand how each of these mechanisms work and what is needed to bypass them manually or with specialized tools, while still preserving the forensic soundness of the data. If the data that is gathered from the device is accessed in such a manner that it can potentially change, it presents a very important legal problem and in a worst-case scenario, the whole case can be dismissed because of it. This essay attempts to describe on a higher level, how the different default authentication mechanisms work and what it takes to bypass them.

Many of the different security methods can also be used side by side, meaning that a user can open their lock screen with for example either their fingerprint, facial identification or swipe pattern, whichever they choose to use. The idea behind this is that the user has several fallback methods if for example due to bad lighting, facial recognition does not recognize their face and refuses to unlock the phone. For law enforcement and other investigators, this can be a positive and helpful thing as it gives them more ways to get access to the data. In the case of the three previously mentioned authentication methods, if the investigator fails to retrieve or deduce the swipe pattern, they still have the other two potential bypass vectors available to them. However, this does assume that the investigator has working knowledge of all of the authentication methods and has the necessary tools available to them.

Some of the more basic protection mechanisms are quite simple to bypass especially on older versions of Android phones. One of the three most basic screen lock mechanisms is the swipe pattern. Research by Van Bruggen (2014) observed that most of the participants in a study preferred the swipe pattern as a way to secure their device compared to other methods. This could be due to the fact that a user often chooses a pattern that is logical and intuitive and after a few repetitions, it is quickly implemented into the muscle memory of the user. The swipe pattern security mechanism consists of a three-by-three dot-grid where the user can choose any pattern allowed by a set of rules (Uellenbeck et al., 2013) by dragging their finger across the screen in the shape of the chosen pattern. After this, the screen can be unlocked by swiping the screen with the same pattern when prompted. There are several ways to bypass this security feature, one way is to simply crack the file responsible for holding the value of the pattern. The pattern is presented as a number sequence, for example, 3-2-1-4-7-8-9 and the sequence is then stored as an unsalted SHA-1 hashed value in an otherwise unencrypted file located in the Android file system (Rao and Chakravarthy, 2016).

However, to access the root directory and the system files, the device needs to be rooted and a hidden feature called USB debugging mode needs to be enabled. However, enabling this special mode and rooting an Android device is not difficult when compared to, for example, iOS rooting, as guides are readily available online. The challenge comes from the fact that doing these procedures might affect the forensic soundness of the evidence more than previously thought (Barghouthy and Marrington, 2014). Because of this, the lead investigator should be consulted before rooting a device so that any data found can still be used as valid evidence in a court.

Once the stored hash is located, it can be cracked with for example the use of rainbow tables that list all possible variations. With modern hardware, this is not very hard to do as the number of patterns is very limited since each number can only be used once, and the previous number always dictates up to a point in which numbers can come next in the pattern. The investigator can write a simple script that produces all of the possible numerical combinations according to the set of rules and then calculates the one-way hash with the same cryptographic function. After generating the list, the original hash value found in the phone's file system can be compared against the values to find a match. The process of generating the hashes is a one-time thing as the same list can be used in future investigations and it is quite possible that such a list is already available from previous investigations. If there is an immediate need to access the data on the phone due to threats on life or other similar circumstances, the pattern can also be removed by accessing the phone's file system and simply deleting the file containing the hash value. However, this will effectively change the file system and whether it should be used needs to be verified from whoever oversees the investigation.

Some interesting research has been done to find another method for bypassing the pattern security feature, which doesn't rely on having root access to the phone (Aviv et al., 2010). This involves a more heuristic way to bypass the pattern and relies on the oil residue on a person's fingers. The residue leaves a smudge on the screen and by utilizing cameras and powerful lighting from different angles, it seems to be possible in many situations to recover partial or even full patterns from the smudges. However, a big part of successfully decoding the pattern from oil residue is how recently the device has been opened and how much random screen contact there has been afterward. If the user decides to wipe their screen clean or use a phone case that has a soft surface touching the screen, any possible smudges left behind could be greatly affected, rendering this technique useless for an investigator. The fact that this attack does not require changing the phone into different modes keeps the forensic soundness intact and in the case of a clear and recent smudge, it can be the fastest way to unlock the screen.

The other two basic authentication mechanisms present on almost every Android device are the PIN code and the password. The PIN (Personal Identification Number) and password security mechanisms are very similar to each other in how they work and bypassing them involves similar steps. As with the process of bypassing the pattern lock screen, to bypass these two security features, the device needs to be rooted and USB debugging mode needs to be enabled from the phone options which, as previously mentioned, can have an effect on the file system integrity.

The PIN security feature that Android offers consists of a numerical password that the user can choose. The minimum and maximum character count varies slightly phone-by-phone, but for example, the One Plus X requires the user to choose a PIN length that is between 4 and 16 characters. Unlike with the pattern method which imposes several rules to the user deciding the pattern, any number sequence can be used for the PIN. The user can also freely use any number repeatedly as many times as they want. The password

security mechanism consists of a password with a similar length of 4 to 16 characters. The user can use alphabetic characters, numeric characters and special characters in any order and combination. Since there are only 10 numbers available for the PIN option, the password is mathematically much more complex, but this only affects the time needed to crack it. With modern hardware and easily available cloud services, an investigator can effortlessly spin up multiple powerful GPUs with a cloud service and use them to do the necessary calculations in a very short amount of time and with minimal costs.

Like the file storing the hash value for the pattern, both the password and the PIN are stored in a specific file found in the phone's root file system. This file stores the user-generated password or PIN as a hash value which is a concatenation of an SHA-1 and MD5-checksum. Unlike the pattern file which utilized no salting, the file containing the hash for the PIN and password has been salted using a random string. The salt value is stored in its own file, which can once again be found in the root file system. The specific location for this second file depends on the Android version (Digital Forensics Corp, no date). Once located, the salt can be viewed using any hex viewer or SQL file browser, and after combining it with the password or PIN hash, the plaintext value can be brute-forced with a script similar to the one used for calculating the hash values for the pattern.

As with the pattern security mechanism, the password and pin lock screens can easily be bypassed just by deleting the two files storing the values. However, by deleting them, the forensic soundness of the data will again suffer, so this way of bypassing the lock screen should not be used unless there are mitigating and urgent circumstances and there is no better way to unlock the phone in the needed time frame.

In addition to the three basic screen unlock methods, when turning a mobile phone on, a second PIN code is needed by default to access features utilizing the SIM card and the information stored on it. Some of the forensically interesting data available on a SIM card include calls made and received, SMS messages and contacts saved onto the memory available on the SIM card (Srivastava and Vatsal, 2016). A PIN code is a four-digit code that can be set by the owner of the device, or it can also be turned off. Different carriers have different default PIN codes, but they are often freely available either on the carrier's website or on websites that list such information (Control-F, no date). Often these default PIN codes are very insecure and consist of repeating a single number (0000) or incrementing a number (1234), so changing it is encouraged. Pre-paid SIM cards are also readily and cheaply available in almost all stores that sell everyday items and because they can be bought with cash and the buyer does not have to provide any personal information, burner SIM cards are quite often used by people involved with criminal activities. Bypassing a SIM card's PIN protection becomes an issue if the seized phone is off or has to be restarted at some point during the investigation.

A SIM card utilizes a two-level security mechanism which means if the PIN code is entered incorrectly three times, the SIM card will be disabled (Kuhn, 1997). To enable it again, a special 8-digit PUK (Personal Unlock Key) code needs to be entered. If this code is entered incorrectly ten times, the SIM card will be permanently blocked and cannot be reactivated. Because PUK codes are fixed and cannot be changed by the user, if the PIN code or the PUK code are not recovered during an investigation, and the device owner declines to provide them, the PUK-code can be requested from the carrier as they usually have it on record. Because of this, as long as the investigator has the correct legal permissions, bypassing a locked SIM card is one of the easier tasks an investigator has to do but it is still one of several possible (and probable) challenges they have to solve.

Smartphones do not explicitly need a SIM card for text messages, phone calls and internet use as there are countless applications available that can act as substitutes for them and these substitutes work over public Wi-Fi. Devices without SIM cards can also be used as music players or tablets if the owner has, for example, bought a new phone and transferred their original SIM card into that. However, having a SIM card in a mobile phone should be expected and even if the owner is carrying multiple smart devices, at least one of them will most likely contain one and because of this, an investigator should be prepared to bypass a SIM card PIN code. However as explained earlier, this process should not present many problems.

If manually bypassing any of the previously mentioned security features is deemed to be inappropriate due to legal reasons, there are several tools available that can achieve the same outcome. Some of the most feature-rich tools include Cellebrite's different tools, Oxygen Forensic and Paraben's tools. These all support the Android operating system as well as several others but are quite expensive and smaller law enforcement agencies might not be able to afford such tools. However, at least Cellebrite claims to be able to bypass Android locking mechanisms while still preserving the forensic soundness (Cellebrite, 2019). Some open-source tools exist like Autopsy, but they often lack the more advanced features that paid tools have.

The challenge in implementing any kind of tool into an investigator's toolkit is that they have to spend a significant amount of time to get to know each and every feature. By thoroughly learning their tools, any accidental file modification is prevented and if the tool is able to bypass security features automatically, this frees up time that can be spent on other areas of an investigation.

Even though most people who carry a smartphone are not experts in security, it is realistic to expect that they have at least one of the several available security features enabled on their devices. Because of this, law enforcement and mobile forensics investigators need to possess at least a high-level understanding of how each of these features work and what is needed to bypass them. This allows them to choose the correct methods and tools they need to get the necessary data and simultaneously preserve the integrity of it so it can potentially be used as evidence. By knowing at least the basics of the different authentication methods also allows the investigator to more easily figure out where they can find more in-depth information if they end up needing it.

Most of the default security features are often very possible to bypass and because the device owners can have multiple different authentication mechanisms enabled simultaneously, it provides multiple bypass vectors to an investigator. Therefore, the technical side of bypassing a simple lock screen should not present a serious problem to a forensics investigation. However, even if there are several different methods and tools available to bypass each of these features, the challenge comes from needing an investigator who has the working knowledge of actually operating said tools. A possible option would be to have multiple investigators, who each know how to bypass certain types of authentication mechanisms and how to use certain forensics tools. However, this will quickly add to the overall investigation cost and certain specialized investigators might not be available at every moment. Another challenge related to the different methods and tools is that an investigator will also have to take into account how certain methods might alter the validity of the evidence.

Any investigator whose work might involve them bypassing smartphone authentication, or even just working with smartphones in general, will have to continuously keep researching and practicing their skills, as new devices with different implementations and features are released periodically. Even small Android updates might drastically change how a security feature works and how securely it stores the

password values that the investigator or forensics tool needs to manipulate. Such updates might also break the tools themselves that the investigators use, and new tools or updates need to be acquired and learned in such cases.

REFERENCES

Aviv A. J., Gibson K., Mossop E., Blaze M., and Smith J. M. (2010) `Smudge Attacks on Smartphone Touch Screens`, WOOT'10 Proceedings of the 4th USENIX conference on Offensive technologies Article No. 1-7. doi: 10.1.1.176.4678.

Barghouthy, N., & Marrington, A. (2014) `A Comparison of Forensic Acquisition Techniques for Android Devices: A Case Study Investigation of Orweb Browsing Sessions`, 6th International Conference on New Technologies, Mobility and Security (NTMS). doi:10.1109/ntms.2014.6813993.

Bittium (no date) *Bittium Tough Mobile™ - Secure and Strong LTE Smartphone*. Available at: https://www.bittium.com/secure-communications-connectivity/bittium-tough-mobile (Accessed: 1 November 2019).

Cellebrite (2019) *Overcoming Locked Android-Powered Devices with the Latest Innovations*. Available at: https://www.cellebrite.com/en/blog/overcoming-locked-android-powered-devices/ (Accessed: 4 November 2019).

Control-F (no date) *Default SIM PINs*. Available at: https://www.controlf.net/simpin/ (Accessed: 21 October 2019).

Digital Forensics Corp (no date) *Extracting data from a locked Android device*. Available at: https://www.digitalforensics.com/blog/extracting-data-from-a-locked-android-device/ (Accessed: 2 November 2019).

Kuhn, M.G. (1997) *Probability Theory for Pickpockets— ec-PIN Guessing*. Available at: https://www.cl.cam.ac.uk/~mgk25/ec-pin-prob.pdf (Accessed 21 October 2019).

O2 (no date) *Support*. Available at: http://service.o2.co.uk/IQ/SRVS/CGI-BIN/WEBCGI.EXE?New,Kb=Companion,question=ref(User):str(Mobile),CASE=14742 (Accessed: 21 October 2019).

Rao, V. V., & Chakravarthy, A. S. N. (2016) `Analysis and bypassing of pattern lock in android smartphone`, 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC). doi:10.1109/iccic.2016.7919555

Srivastava A, Vatsal P (2016) `Forensic Importance of SIM Cards as a Digital Evidence`, Journal of Forensic Research 7:322. doi: 10.4172/2157-7145.1000322.

Uellenbeck, S., Dürmuth, M., Wolf, C., & Holz, T. (2013) `Quantifying the security of graphical passwords`, Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security - CCS '13. doi:10.1145/2508859.2516700

Van Bruggen, D. C. (2014) *Studying the impact of security awareness efforts on user behavior*. Ph.D. dissertation. University of Notre Dame. Available at: https://curate.nd.edu/downloads/und:sx61dj5598x (Accessed: 1 November 2019)