Vincent-Lübeck-Gymnasium
Glückstädter Str. 4,
21682 Stade

Vorfacharbeit im Seminarfach: Computing and Society (Bilingual)

Could and should the criminal justice system be able to bypass iOS security?

Verfasser/in: Jonas Wilms
Fachlehrer: Dominic Twyman
Abgabetermin: 18. Okt. 2017

Asselermoor, 16.Okt. 2017

1 Introduction 1
2 Overview of iOS security mechanisms 1
2.1 Encryption 1
2.2 Architectural security 2
3 Ways of bypassing 2
3.1 The human target 2
3.2 Brute force attacks 3
3.3 NAND mirroring 3
3.4 Extracting the UID 4
3.5 Implementing a backdoor 4
4 Conclusion 5
References 2

1 Introduction

iOS is one of the main mobile operating systems shipped with well-known products, including the iPhone and the iPad. As being very popular on the market, about every 10th smartphone sold currently (2nd Quarter, 2017) is an iPhone [1], thus possible attacking vectors and security holes in the iOS encryption system can endanger the privacy of millions of people. However as the data stored on them may be a possible evidence in crime cases, it is necessary to access the data stored on them without the users permission. This paper will discuss ways of bypassing a single devices security without weakening the privacy of the majority of users.

2 Overview of iOS security mechanisms

As iOS and its underlying technique are one of the main core values of the Apple Inc., detailed technical information about the underlying hardware and the iOS source code are not publicly available. Most of the available information are part of marketing campaigns by Apple or have been discovered by security researchers.

To prevent the access to the user's data, iOS devices can be locked with a PIN or a password. After 4 unsuccessful attempts to enter the passcode, there is a short delay before one can attempt it a 6^{th} time, after every following attempt the delay will be increased to up to 1 hour after 9 attempts. The user can enable the erasure of all data after 10 wrong attempts. Additionally fingerprint authentication can be used alternatively after one successful login and is available over a maximum time of 2 days before a password is required again [2] (pages 8,9,12). The device is locked again when it is either shut down or restarted, or after a user defined standby time, which can be immediately.

2.1 Encryption

While a lockscreen does not prevent the storage to be removed physically from the device, the extracted data is useless as iOS encrypts all data by default. Whenever files are stored on the flash storage, a random per file key is created and the file is encrypted with that key. The key is then stored in addition to the files metadata and encrypted again with the user's passcode and the so called UID, a unique random key that is built into the device at the factory. To access a file, the file is decrypted with the decrypted per file key and copied to RAM, where it can be used by the app that owns it [2] (page 10,11). Whenever an iOS device is locked, which happens after a certain inactive time when a password is set, iOS starts to erase certain per file keys, a reboot erases all of them [2] (page 12,13).

So until a first unlock all the device`s data which contains users data stays encrypted, after that decrypted data may be located in the RAM or per file keys may already have been decrypted using the users key and the UID. Which data is accessible mainly depends of the devices usage including background processes.

2.2 Architectural security

As stated above the data is inaccessible when it's on the flash storage, but it's unencrypted in the RAM, when the user uses its device. To prevent apps from spying the user, all the data is stored on a per app base, however apps can share their data with other apps. While the apps data is stored inside the RAM, all the keys used for decryption including the users passwords, which may be a 4-digit PIN, a password or a fingerprint, the UID and the per file keys are handled inside of a separate processor called Secure Enclave which also has its own private memory. The application processor only forwards passwords to it; the secure enclave then manages the physical encryption engine which is right between the RAM and the flash storage. The Secure Enclave checks passwords, stores them, and enforces the minimum delay between login attempts mentioned above. It has its own small Operating System which makes its integrity independent of the main processor [2] (page 7, 10). The physical encryption engine uses the AES algorithm which is considered safe until now by security experts such as Bruce Schneier [5]. This physical security was introduced with the A7 processor, so it is part of all devices newer than the iPhone 4 or iPad 1.

3 Ways of bypassing

3.1 The human target

Bypassing the encryption of a locked device requires a huge amount of technical knowledge. Therefore the easiest way is probably forcing the user to enter his passcode. However using force to get information out of suspects is forbidden in Germany [6], but it is partly allowed in the U.S [7] and in the U.K and Australia people can be imprisoned up to 2 years for not unveiling passwords [8][12], however that may still be better than being arrested for the crime.

If the suspect enabled touchID, it's possible to use his fingerprint to unlock the device, which would not require the suspect's allowance, but not everyone uses touchID and the device still requires a password after 2 days making this method unreliable.

Another possibility would be to gather the iOS device in an unlocked state, so that there is no need to unlock it.

While it's quite difficult to prevent the suspect from locking it, this technique was used by Scotland Yard to get access to a card frauder's iPhone [3]. However this technique can only be used before a suspect gets arrested and is heavily based on chance.

3.2 Brute force attacks

Against the recommendation of security experts, people still tend to use easy passphrases, for example 1234, "password", their own or a relatives birthday or their pets name. There is a slight chance to guess the password in 10 attempts, but this limit is software enforced so there are ways of bypassing it:

3.3 NAND mirroring

The device itself can be manipulated to weaken the security measures and therefore enable more password attempts. This method is called NAND mirroring, which refers to the NAND flash storage technique used in iPhones and iPads. The main idea of it is to enable unlimited passcode attempts through resetting the storage after 6 attempts to its original state. As the wrong attempts counter is stored in the regular devices storage, resetting the whole storage also resets this attempt counter. As the storage is glued into the devices motherboard, it needs some hardware modifications to work. After that, the devices storage can be reset after shutting down the device, then it can be restarted and another 6 attempts are possible. This cycle averages 90 seconds, making it possible to try all combinations of a 4-digit PIN in about 40 hours [4] (page 7). As the first attempt could be right as well as the last, a random passcode can be found in 20 hours average, so in less than one day. If the tried passcodes would be sorted after probability, this could be possibly improved. However there are some implications: a 4-digit PIN has only 10 000 possibly combinations. While using a PIN is common there is also a possibility to use a password of unlimited length. With every additional character, the time needed to brute force increases exponentially. For a 6 character password it would take:

$$\frac{(2 * 26 + 10)^6}{6} * 90s \approx 2\,232\,713\,years$$

So the device will probably be unlocked far beyond the lifetime of a potential suspect. While the average time can be improved using dictionaries and social engineering, this method is still unrealistic for longer passwords. And while NAND chips will probably survive the 1667 resets

needed to try all 4-digit pins, they probably won't survive the resets needed for longer passwords [4] (page 7). There is also a slight chance that the device is damaged during the modifications, making it risky as the evidence may get lost [4] (page 8).

3.4 Extracting the UID

As stated by Apple [2], it’s impossible to decrypt the data outside of the iPhones / iPads hardware, as the hardware crypto engine relies on a random UID glued into the device. As the internal crypto engine is physically slowed down, powerful brute force attacks aren't possible on the device itself. Running these attacks on a bunch of performant and heavily optimized clusters may enable an attacker to reduce the time needed to try out a few passwords drastically [13]. So extracting the UID is needed to break longer passwords. However, this is not that easy. Extracting the UID out of the processor has not yet been done. But as it is glued into the device inside the factory, the manufacturer, Apple or various intelligence services might be able to intercept and store the UID of every Apple device manufactured. However such a worst case scenario has not yet been proven or leaked, making it extremely unlikely to exist.

3.5 Implementing a backdoor

As shown above, the encryption that is used on current iOS devices makes it nearly impossible to unlock an encrypted device. Therefore a viable way to access unencrypted data would be "simply" disabling encryption. To do so, one would need to replace the iOS operating system with a frauded version, that does not encrypt the user’s data but stores the information in plaintext or directly redirects all the data to police servers.

To hook into iOS, one needs to bypass the security measures taken by the kernel, the core part of an operating system. This is only possible if there’s a bug inside the kernel that has not yet been fixed by Apple (called 0day in hackers slang), which occurs rarely [14]. Searching for 0days requires a huge personal effort and is a race against Apple fixing it.

Another possibility would be a backdoor, so a planned weakening of the kernel implemented by Apple. However as Security and Privacy are one of Apples commitments [9], the Apple Inc. would probably never risk their credibility and their customers trust. If a backdoor exists it has to be hidden deeply into the system, to make it undiscoverable by researchers. As revealed by the NSA scandal, intelligence agencies worldwide are forcing companies to implement such "features" [11]. There are also reports stating that the NSA is replacing devices with cracked versions [10]. While such

attacks seem to be the only way to successfully "unlock" all kind of passcodes, there is no known way to deliver such devices to "criminals only" as a backdoor needs to be implemented before the device is locked, so before the suspect was arrested. They may be used in rare cases to be delivered to known criminals, or they have to be shipped to all users, effectively disabling the privacy and security of every user.

4 Conclusion

Most of the methods described above that require just a small effort and nearly no technical knowledge, such as gathering the device in an unlocked state or guessing the passcode, are heavily based on chance, so they often require a plan B. If the device is locked with a four digit PIN, NAND mirroring is probably the way to go and chances are high that the lockscreen can be bypassed in under one day. As it requires physical access to the device, it does not enable mass surveillance making it a morally acceptable method. However if a suspect fears to be under surveillance, he will probably take advanced measures concerning his security. Enabling a longer password as well as *direct locking on standby* just requires changing the devices settings in a few steps and is possible without technical knowledge. To then get access to the devices data requires either a 0day, a backdoor or a UID database. All these methods can easily be applied to multiple devices and therefore they're enabling mass surveillance. Even if the access is kept secure, there will be still no way to prevent abuse. That ranges from agents spying their family to criminal organizations, who are than able to gain millions of private photos, messages and even bank accounts. A few more arrests are not worth the insecurity of millions of people’s lives, and agencies that develop such tools or support companies in doing so, are overestimating the integrity of their employees or they don’t care of individuals’ privacy.

So while the investigative services can and should bypass iOS devices security in most cases, a bulletproof method that works in every case should not be developed as it enables the surveillance of innocents.

References

[1] Statista GmbH, “Marktanteil von Apples iPhone am weltweiten Absatz von Smartphones vom 3. Quartal 2007 bis zum 2. Quartal 2017,” 2017. [Online]. Available: https://de.statista.com/statistik/daten/studie/12864/umfrage/marktanteil-von-apple-smartphones-seit-2007/. [Accessed 15 10 2017].

[2] Apple Inc., “iOS Security,” 3 2017. [Online]. Available: https://www.apple.com/business/docs/iOS_Security_Guide.pdf. [Accessed 15 10 2017].

[3] BBC, “Phone encryption: Police 'mug' suspect to get data,” 2 12 2016. [Online]. Available: http://www.bbc.com/news/uk-38183819. [Accessed 15 10 2017].

[4] S. Skorobogatov, “The bumpy road towards iPhone 5c NAND mirroring,” 14 9 2016. [Online]. Available: https://arxiv.org/abs/1609.04327. [Accessed 15 10 2017].

[5] B. Schneier, “Schneier on Security : Can the NSA Break AES?,” 22 3 2012. [Online]. Available: https://www.schneier.com/blog/archives/2012/03/can_the_nsa_bre.html. [Accessed 15 10 2017].

[6] J. Wendt, “Darf die Polizei mich zwingen, mein Handy zu entsperren?,” ZEIT ONLINE GmbH, 4 11 2014. [Online]. Available: http://www.zeit.de/digital/datenschutz/2014-11/fingerabdruck-sensor-unsicher-passwort-nemo-tenetur. [Accessed 15 10 2017].

[7] C. Varma, “Encryption vs. Fifth Amendment,” 27 7 2015. [Online]. Available: http://www.coreyvarma.com/2015/07/encryption-vs-fifth-amendment/. [Accessed 15 10 2017].

[8] Federal Register of Legislation, “Crimes Act 2914,” 25 3 2015. [Online]. Available: https://www.legislation.gov.au/Details/C2015C00111/Html/Volume_1#_Toc415554770. [Accessed 15 10 2017].

[9] Apple Inc., “Apple products are designed to do amazing things. And designed to protect your privacy.,” [Online]. Available: https://www.apple.com/privacy/. [Accessed 15 10 2017].

[10] S. Gallagher, “Photos of an NSA “upgrade” factory show Cisco router getting implant,” WIRED Media Group, 14 5 2014. [Online]. Available: https://arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant/. [Accessed 15 10 2017].

[11] T. McCarthy, “NSA director defends plan to maintain 'backdoors' into technology companies,” Guardian News and Media Limited, 23 2 2015. [Online]. Available: https://www.theguardian.com/us-news/2015/feb/23/nsa-director-defends-backdoors-into-technology-companies. [Accessed 15 10 2017].

[12] J. Kirk, “Contested UK encryption disclosure law takes effect,” PC World Commmunications Inc., 1 10 2007. [Online]. Available: http://www.washingtonpost.com/wp-dyn/content/article/2007/10/01/AR2007100100511.html. [Accessed 15 10 2017].

[13] Better Buys, “Estimating Password-Cracking Times,” [Online]. Available: https://www.betterbuys.com/estimating-password-cracking-times/. [Accessed 15 10 2017].

[14] Finjan Mobile Inc., “Apple iOS Vulnerabilities – Zero Day Attacks,” 20 6 2017. [Online]. Available: https://www.finjanmobile.com/apple-ios-vulnerabilities-zero-day-attacks/. [Accessed 15 10 2017].