Security Vulnerabilities of Apple iPhone Fingerprint Authentication

Suruchi Devanahalli

Contents

1 Abstract

With the increased use of fingerprint authentication by large scale phone manufacturers like Apple and Google (Android), users can now use a password OR a fingerprint to unlock their mobile device. Apple phones that use fingerprint authentication now have to do 2 things: capture a user's fingerprint using an image based scanner and compare the computer representation of the fingerprint image with one that has been stored in the secure enclave on the Apple phone chipset. If the fingerprint representations match, the phone will unlock. This authentication method operates under the assumption that every person has a unique fingerprint. The question that must be asked : Is this authentication method impenetrable? This paper will discuss the fingerprint authentication methods used by Apple iPhones and the security vulnerabilities that are inevitably created in the process. The paper will also talk about anti spoofing technologies that can be used to protect the fingerprint authentication system against security attacks such as the use of a fake finger or a severed finger to unlock a phone.

2 Introduction

2.1 The Touch ID sensor and the Secure Enclave

The Touch ID sensor is the starting point of the fingerprint authentication process. When the capacitative steel ring that surrounds the home button detects a finger, the fingerprint sensor is activated and uses imaging array technologies to scan the fingerprint and sends the scan to the secure enclave ("IOS Security Guide." 8).

The Secure Enclave is a coprocessor built into the iPhone. It handles cryptographic operations relating to data protection key management. It is responsible for "processing fingerprint data from the Touch ID sensor, determining if there is a match against registered fingerprints, and then enabling access or purchases on behalf of the user" ("IOS Security Guide." 7). A processor forwards data from the Touch ID sensor to the Secure Enclave but cannot read it("IOS Security Guide." 7). Apple has released limited information about the Secure Enclave, given its important role in iPhone data security.

2.2 Fingerprint scan analysis

Once the secure enclave receives a raster scan of the fingerprint, it is vectorized for analysis where sub-dermal ridge flow angle mapping is used to create a map of nodes that represents the user's fingerprint ("IOS Security Guide." 8). The node map is encrypted and stored in a format that can only be read by the secure enclave (Apple 8). It is not backed up on any other platform such as iCloud. As the user continues to use the Touch ID, the node map stored in the secure enclave is expanded over time ("IOS Security Guide." 8).

2.3 Unlocking the iPhone

The data protection keys that are used to unlock the phone are wrapped with an additional key that is given to the Touch ID subsystem within the secure enclave (“IOS Security Guide.” 9). If the user’s fingerprint is recognized by the Touch ID subsystem, it provides the outer key that can be used to unlock the data protection keys, and the entire phone.

3 To The community

In April 2016, Apple revealed that 89% of its users that have Touch ID enabled iPhones and iPads, use the Touch ID to unlock their devices (Campbell) . Yet Apple has been very quiet about the security vulnerabilities that could be prevalent in their system. Most users are under the notion that fingerprints are totally unique and there is no chance that anybody would be able to get into their phone. It is important for users to know that this is not necessarily the case. This paper will serve to provide the community with information regarding how their phones are not totally secure with Touch ID and what can be done about it.

4 Security Vulnerabilities

4.1 Finger Print Spoofing

Finger print spoofing is the act of faking a phone owner’s fingerprint which is used on a Touch ID sensor to gain access to the resource that the Touch ID is protecting. For example, when the iPhone 5S was first released, Germany's Chaos Computer Club released a post and a video demonstrating how they were able to photograph a user’s fingerprint from a glass surface and print it onto a thin sticky film that can be stuck to anybody else's finger to gain access to the user's phone through the Touch ID (Arthur). The main point here, is that, the group did not have to hack into Apple's super secret Secure Enclave to gain access to the phone or the user's fingerprint. They were able to access the phone by external means. In July 2016, researchers at Michigan State University were asked by the University police to hack into a murder victim's phone using a similar technique that Germany's Chaos Computer Club used- a 2D spoof of a fingerprint (Cooper). In addition, the researchers were able to create a high resolution fingerprint that was detailed even more by adding wood glue ridges to the fingerprint's ridges (Cooper). They were able, to unlock the phone and continue the murder investigation. This goes to show that even after death, our fingerprints can still be used to unlock our phones. Our passwords on the other hand die with us.

4.2 Fingerprint credential spread and immutability

If fingerprint spoofing can be achieved by taking fingerprints from surfaces that a person has touched, then Touch ID users are more vulnerable than they were with a 4 number password. Finger print credential spread is a very real concern. We leave our fingerprint on anything that we touch. Granted, these may be partial fingerprints. But if a hacker really wanted to, they could piece together our fingerprints just as forensic experts do at crime scenes. The only difference is, the hacker has to be able to get access to things that you have touched. So they have to be near you. With passwords, this is not the case.

In addition, passwords can be updated frequently and can be made more complex. With fingerprints, users only have the set of fingerprints that they were born with and can't change them without serious surgery. It is baffling that the immutability of fingerprints does not concern Apple enough for them to build their whole security system around credentials that will never change.

4.3 Partial fingerprints and the Master Print

When a user wants to enable fingerprint scanning on an apple device for the first time, they must place their finger on the sensor several times and at several different angles. This is so that the sensor can scan partial parts of the finger and create a more detailed node map of the finger in the phone's secure enclave. Because Apple has not released detailed information on how the phone matches the fingerprint Node Map to a user's fingerprint we can only guess. If Apple uses partial prints for authorization, in other words, if a part of the fingerprint matches the Node Map and the user is given access, then people who have similar partial fingerprints would be able to gain access to each others' phones.

NYU Tandon and Michigan State University Researchers have found that "there could be enough similarities among different people's partial prints that one could create a MasterPrint."(NYU Tandon School of Engineering) In essence, a MasterPrint would work like a common 4 number password like 1234. Even a simple password like 1234 has a high probability of success, especially if the hacker is just guessing, because of how common it is. A Master Print would contain the partial prints of common features in fingerprints.

5 Defenses

5.1 Liveness Detection

To protect against fingerprint spoofing, a fingerprint scanner should be able to detect a finger that is living - pulse, temperature, capacitance. It should also be able to detect if the finger is covered with some sort of thin film that is allowing it to have another person's fingerprint. One disadvantage of having these extra features is that they could take up more battery life and be more expensive. Researchers at M2SYS Technology have developed a finger scanner called M2-FuseID, which is "capable of distinguishing fingerprints made of artificial objects from a live fingerprint. " (Trader) It works by having an additional finger vein sensor that can detect the blood flow in the veins of the finger, thereby recognizing its liveness (Trader).

5.2 Fingerprint Scan Clarity

If fingerprint scan technologies were able to work with full finger prints instead of partial scans, there would be less of a chance that two people could access each other's phones. In addition, if sensors were able to retrieve high quality images of the fingerprints, an analysis could be done on the presence, size and frequency of pores as well as the sharpness of lines found on the fingerprint . If more characteristics of the fingerprint are analyzed, more differences can be found between any two fingerprints.

6 Conclusion

Fingerprint authentication on phones, in its current state, is not a secure way to protect data. One could argue that nobody can get into an Apple phone to steal a user's fingerprints, because Apple's Secure Enclave is highly secure. But people rarely seem to acknowledge the very real and rampant threat of fingerprint spoofing. When the means of authentication is a physical part of your body and not a password in your mind, it is so much easier for people to steal it by force. With the increase in money sharing apps (Venmo, Bank of America, Apple Pay, etc) that now allow you to authenticate transfers with your fingerprint, it is incredibly frustrating and scary to see that the risks of fingerprint authentication are not being taken seriously. Phone developers must look into new technologies that can strengthen this form of authentication AND they must disclose to the public how vulnerable users really are with this method of authentication.

7 References

Apple. “IOS Security Guide.” *IOS Security Guide*, Mar. 2017, <www.apple.com/business/docs/iOS_Security_Guide.pdf.>

Campbell, Mikey. “Average iPhone user unlocks device 80 times per day, 89% use Touch ID, Apple says.” *AppleInsider*, AppleInsider, 19 Apr. 2016, <appleinsider.com/articles/16/04/19/average-iphone-user-unlocks-device-80-times-per-day-89-use-touch-id-apple-says.>

Arthur, Charles. “iPhone 5S fingerprint sensor hacked by Germany's Chaos Computer Club.” *The Guardian*, Guardian News and Media, 23 Sept. 2013, <www.theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked.>

Cooper, Marta. “Police in Michigan are trying to 3D-Print a murder victim’s fingerprint to unlock his phone.” *Quartz*, Quartz, 26 July 2016, <qz.com/739538/how-police-in-michigan-are-trying-to-3d-print-a-murder-victims-fingerprint-to-unlock-his-phone/.>

NYU Tandon School of Engineering*,* “So You Think You Can Secure Your Mobile Phone With a Fingerprint?” *NYU Tandon School of Engineering*, 10 Apr. 2017, <engineering.nyu.edu/press-releases/2017/04/10/so-you-think-you-can-secure-your-mobile-phone-fingerprint.>

Trader, John. “Liveness Detection to Fight Biometric Spoofing.” *M2SYS Blog On Biometric Technology*, 13 July 2017, <www.m2sys.com/blog/scanning-and-efficiency/liveness-detection-fight-biometric-spoofing/.>