Swami Shreeji

Fingerprint Technology Security & Access on Smartphone Devices

Sapan Bodiwala, Rutgers University, USA

Digital Communication Information & Media

Anne Gilbert

December 9th, 2013

Abstract

Because smartphones are used more frequently and becoming supplementary to everyday life, they carry important user information and therefore raise concerns of privacy and security in the measures implemented to protect that information. My research focuses on the implementation of the fingerprint sensor on Apple's latest smartphone, the IPhone 5s. While Apple claims "Touch ID" provides, "a very high level of security" and the chances of a random match is "1 in 50,000" (Apple, 2013), fingerprint technologies are limited to providing a small level of security with an increased amount of convenience. In addition, there are disadvantages and concerns that fingerprint technology forces users to set unalterable authentication, involve leaving traces of verification that can be replicated, lose accuracy over time, and raise the possibility of losing one's finger to gain smartphone access. Therefore, fingerprint technology is not the solution to today's smartphone security issues. Instead, additional methods of smartphone authentication incorporating personal information and identity such as two-step authentication using encryption and eye identification can provide achievable solutions in order to resolve today's concerns of privacy and authentication.

Introduction

In today's society, the number of smartphone devices and users are rapidly increasing. According to Business Insider, the number of smartphones in use around the world will reach 1.4 billion by the end of 2013 (Leonard, 2013). This is heavily due to the amount of features smartphone devices provide for users today.

Smartphone owners are utilizing the most of many devices features by making phone calls, sending text messages, reading personal emails, managing personal finances, looking up directions, taking pictures, downloading private documents, and even logging into social network accounts (Ruggiero & Foote, 2012). With all of these capabilities, it's incredible how much personal information is being stored on smartphone devices in today's day and age. Hundreds of contacts, multiple text message threads, and gigabytes of media including pictures are just some of the types of personal data and information being saved to smartphone devices' memory. What's really amazing is the amount of personal data being stored on these devices is increasing each day (Ruggiero & Foote, 2012).

The enlarging amount of personal data and information stored on smartphone devices provides a large surge of concerns regarding privacy, security, and authentication. Users run the risk of having their personal information fall into the wrong hands when carrying a smartphone device. Due to the compressed size of these devices, smartphones can easily be stolen or found in the wrong hands for moments of a time. It's during those times when security and authentication play critical roles in user privacy.

To solve privacy concerns and issues, password protection was developed to protect from unwanted users to access the device's core features and data (Knott & Steube, 190). However very similarly, passcode protection on smartphone devices hasn't been a popular

choice of action. According to Apple, “more than 50 percent of smartphone users don’t use a passcode” (Apple, 2013).

In contrast, fingerprint technology has been around for many decades, also providing security against unwanted users and authentication for consumer’s access. Furthermore, Apple has taken the first step in integrating fingerprint authentication into its smartphone device by developing Touch ID. Touch ID uses a 500-ppi (pixel-per-inch) sensor to read a user’s fingerprint. The sensor takes a high-resolution image of the fingerprint, and categorizes it as an arch, loop, or whorl (Apple, 2013). Then, the sensor analyzes and determines authentication based on the image of both the scanned and saved images that are located on the A-7 processor.

Fingerprint technology seems like the obvious solution to security and authentication concerns; however, it only provides a layer of security, which does not protect personal information and data. In addition, there are disadvantages and concerns that fingerprint technology forces users to set unalterable authentication, involve leaving traces of verification that can be replicated, loss of accuracy over time, and the possibility of losing one’s finger to gain smartphone access. Therefore, fingerprint technology is not the solution to today’s smartphone security issues.

In order to explain why fingerprint technology is not the answer to smartphone security and why these devices need improved methods of authentication, I will first provide background information on fingerprints and fingerprint technology including biometric identification. Second, I will introduce the features and functions of Apple’s latest technology enhancement, the IPhone 5s’ Touch ID. Third, I’ll examine the advantages and disadvantages of using fingerprints as authentication. Next, I will discuss consumer

concerns regarding privacy and some of the concerns fingerprint technology brings to smartphone users. Then, I'll explain why fingerprint technology is not the solution to today's smartphone security concerns and how additional methods of smartphone authentication incorporating personal information and identity can provide solutions for privacy issues.

Literature Review

Fingerprints have been a well-known and established method of authentication for many decades. To go back to its initial uses, fingerprints were first used in 1858 by Sir William Herschel to sign contract documents (Watson, 2008). The initial purpose and intent of use was to decrease fraud and to ensure that the person who signed the document was authentic.

As time has moved forward and technology has advanced and developed, fingerprint authentication has become a popular method of verification. Fingerprint technology uses biometric identification (biometrics) in order to authenticate an individual based on personal human traits (Dass, 2013). In our case, the human trait is a fingerprint in which is un-identical to any other person, meaning each individual has his or her own unique fingerprint. Over time, a person's fingerprints do not change, as they remain the same throughout their life. This is an important concept when differentiating the advantages and disadvantages of fingerprint technology.

There are two levels of fingerprint features that are considered for recognition. Level one consists of valleys (white parts in between) and ridges (dark lines of fingerprint) in which are united into complex patterns (Dass, 2013). Level two features comprise of "minutiae", which contains the orientation, location, and angle of the ridges and valleys. Each fingerprint comprises of both level one and two features, which are then used for

recognition when scanning. In order to capture a fingerprint, a sensor is used to scan, measure, and generate the image containing both levels of features, which is then stored into a template database for matching (Dass, 2013).

Fingerprint matching is the procedure through which two fingerprint images are compared to determine the degree of similarity (Dass, 2013). Minutiae locations, angles, and orientations are compared between the scanned fingerprint and the stored image in the template database. Depending on the accuracy of the scanning device and the resemblance between the two fingerprints, access is either granted or denied to the user with the input finger.

IPhone 5s – Touch ID

Apple's latest smartphone, the IPhone 5s was developed and made available to the public on September 20th 2013 (Rosenblatt, 2013). This smartphone is Apple's 7th version of the IPhone with upgraded specs, added features, and even a new color (gold). The IPhone 5s comes in 16GB, 32GB, and 64GB versions to store large amounts of personal data and information (Rosenblatt, 2013). This data can include media files such as music and pictures, applications such as games and social networks, and personal data containing contacts, emails, text messages, and documents. Some information that is overlooked by consumers is also stored on the device including access to the calendar, geographic location history, and even saved passwords for applications containing access to email, mobile banking, and social networks (Ruggiero & Foote, 2012).

While the IPhone 5s introduced the latest mobile operating system from Apple, iOS7, which included many new added features that are intriguing for consumers, there was a particular area of focus in the development of the smartphone that often goes unnoticed by its consumers (Whittaker, 2013). That particular area of focus was *security*.

Because large amounts of data and information are stored on smartphones everyday, Apple wanted to ensure that personal data was protected (Apple, 2013). Previous IPhone versions integrated the standard 4-digit passcode for authentication. However, Apple researched and found that more than 50 percent of users didn't setup a passcode for their smartphone devices (Apple, 2013).

This led the company to approach the area of security and privacy concerns and take action. Apple purchased an identification software company in 2012 to focus on developing a new method of security (Rosenblatt, 2013). Apple calls it the Touch ID. The Touch ID is a fingerprint sensor embedded into the Home button on the IPhone 5s. It was designed and developed to enhance security on Apple's latest smartphone device by using biometric authentication to validate and confirm the correct owner of the device. This method of authentication prevents non-owners of the device from accessing data and information stored on the smartphone. Touch ID provides better security against thieves as "Find My IPhone" and "Remote Wipe" features are not accessible without the correct Apple ID, password, and fingerprint ("Apple unveils fingerprint", 2013). The IPhone goes one step further by also requiring the user to setup a 4-digit passcode, as previous versions of the IPhone did, for two-step authentication. This occurs only when the IPhone has been restarted, hasn't been unlocked for 48 hours, or when the settings are accessed (Apple, 2013).

The IPhone 5s comes with Apple's 64-bit A7 processor (CPU), which uses what the company calls, "Secure Enclave" (Apple, 2013). This new security feature was included on the A7 chip to protect fingerprint data from the rest of the phone's hardware and operating system. Apple also adds that the fingerprint image is encrypted and is only accessible using

a key that only Secure Enclave has (Apple, 2013). This means that no other application, service, or part of the operating system has access to the fingerprint data.

Advantages vs. Disadvantages

Fingerprint technology that uses biometrics provides a few advantages towards authentication over standard password methods. One of the main benefits is that fingerprints cannot be forgotten or lost. A user who is trying to authenticate into a system or device that requires his or her fingerprint will not ever forget their password because it is stored on their finger. So as long as the user has all of their fingers, they will not have lost their verification to access the system. Most systems and devices require passwords or passcode to authenticate a user to gain access. These benefits are important when considering the amount of complex passwords users are forced to remember in order to gain access to systems or devices (Sanzziri, Nandugudi, Upadhyaya, Qiao, 2013). Another important advantage of fingerprint technology is the time convenience it provides for users when authenticating. Depending on the sensor, a fingerprint can be scanned and authenticated automatically within a few seconds, without having the user enter in a memorized password ("Apple unveils fingerprint", 2013). A non-forgettable or losable password and the time convenience that fingerprint technologies provide are great advantages over standard password and passcode methods. These advantages are important to consider when applying security technologies to smartphone devices. With the assumption that large amounts of complex passwords are already remembered by smartphone owners, fingerprint authentication makes gaining access much more convenient by saving time and effort.

On the other hand, fingerprint authentication that makes use of biometrics also produces disadvantages for user verification. One important disadvantage to consider is

that fingerprints cannot be altered or changed (Dass, 2013). This means that each user's verification method is limited to the amount of fingerprints an individual has for authentication. Another significant disadvantage to think about is that fingerprints can be replicated. According to CNet, Apple's Touch ID on the IPhone 5s was hacked by a German based group named the Chaos Computer Club. The hack was completed only 48 hours after the phone was released to the public (CNet, 2013). A hacker known by the name, "Starbug" replicated a user's fingerprint within 30 hours, however he stated that with better preparation he would have been able to accomplish the task in 30 minutes (Whitney, 2013a). Additionally while fingerprints can be replicated, they also exist on any objects that users touch. Traces of fingerprints can be found on everyday objects people interact with including glass, paper, furniture, and metal meaning they are no secret to the public (Griggs, 2013). When these disadvantages are considered in the implementation of smartphone devices, consumers bring up many concerns with personal data and information privacy.

Concerns of Privacy and Security

With increasing amounts of personal information being stored on smartphone devices, users want their personal information to be safe and secure. According to research conducted by Pew Internet, more and more users are concerned with personal information being revealed online (Whitney, 2013b). The study found that 50% of Internet users are concerned about the amount of personal information found about them online as compared to 30% in 2009 (Whitney, 2013b). A total of 792 participants were surveyed on how they feel about personal information being exposed on the Internet. Of the participants, 66% of Internet users have photos, 50% have birth dates, and 46% have email addresses available online to the public (Whitney, 2013b). Personal information available online also includes

30% of home addresses and 24% of cell phone numbers. The biggest concern users have is that they feel it is impossible to be completely unknown on the Internet (Whitney, 2013). Considering the types of information found online from the study with the amount of personal information on smartphones, these statistics suggest that personal data privacy is an ongoing concern and will continue to grow in the future with the increased amount of smartphone devices. Smartphones that fall into the wrong hands can lead to even greater concerns, exposing even more private data that isn't available online.

Another study was done on undergraduate students at a small private college on the thoughts about securing information and the use of passwords (Knott & Steube, 2012). A list of survey questions was provided to 49 students exploring the importance of passwords, the difficulty in creating passwords, and the interest in using machine generated passwords. The results found that 94% of those students said password protection is important (Knott & Steube, 2012). The importance of passwords was calculated based on the interest of password protection for each student. The more interested a student was in personal data protection, the more important and difficult it was to manage a secure password (Knott & Steube, 2012). Due to the feeling of difficultly in managing a secure password, smartphone users may feel fingerprint technology provides increased security and convenience without the hassle of creating and managing a password. This is an important point that may have influenced Apple to develop Touch ID in the first place as many users did not setup passcodes for their smartphones (Apple, 2013). Both studies provide statistics on how users feel about the importance of information privacy and password protection as well as suggest why Apple implemented Touch ID.

Concerns of Fingerprint Technology

With the implementation of Touch ID (fingerprint technology) on Apple's latest smartphone device, many concerns have been raised from the public and media about information privacy and personal safety. One concern smartphone users are having is that their fingerprint data may lead criminals to go as far as cutting off users' fingers to gain access (Strange, 2013). Since your fingerprint is permanent, simply cutting off your finger could provide authentication for a lifetime. However, Validity Sensors chief technology officer Sebastien Taveau states that the Touch ID contains, a "RF capacitive sensor" which requires the finger to be alive (Strange, 2013). While a cut off finger may not be able to authenticate through IPhone's Touch ID, there is future potential that a hack can be developed in order to get the sensor to validate the cutoff finger. As "Starbug" hacked Touch ID into authenticating a replicated finger within 48 hours of public release, fingerprint technology has the potential to be cracked by other procedures (Whitney, 2013a).

Another concern a few IPhone 5s users are having with fingerprint technology is that Touch ID isn't always accurate. Complaints have been made over the past few weeks as Touch ID is having trouble authenticating the real user (Epstein, 2013). A consulting engineer Dr. Drang stated, "I rescanned my fingers this weekend, and Touch ID has been amazingly fast and accurate since then [a few weeks later]. Just before each rescan, though, I was so frustrated with Touch ID I felt like throwing the phone across the room" (Epstein, 2013). Seems like he isn't the only one complaining as many other users have contacted him about the issue as well (Epstein, 2013). Accuracy is a crucial feature for fingerprint technology, and while there haven't been many reports of issues, concerns that Touch ID does not retain its accuracy over time remain prominent. These concerns may lead to

future issues of not being able to authenticate into the smartphone device at all, which defeats the purpose of setting up security in the first place. Smartphone security is meant to protect your personal information against others, not from yourself.

Because the IPhone 5s uses Touch ID to authenticate purchases made from the App Store, there is a concern as to how that verification process is completed. Apple states that fingerprint data is not accessible by other applications or parts of the operating system, yet the App store requires correct authentication using fingerprint data (Griggs, 2013). While that doesn't necessarily mean the fingerprint data is being transferred to Apple's servers, it suggests there must be some type of token confirmation being sent over to Apple (Griggs, 2013). This leaves a small crack for hackers to imitate user accounts. User accounts contain personal information including billing address and credit card numbers, which can lead to further fraud issues and privacy concerns.

Privacy worries continue in the United Kingdom, relating to the potential use of fingerprints to track employees. The London chapter of the National Union of Rail, Maritime and Transport has told its associates to not use fingerprint technology to log in and out of work (Osborne, 2013). The union feels that the implementation of biometrics would be used to keep track of staff activity. Personal data such as the biometrics of ones' fingerprints does not belong in the hands of a company. Fingerprints are permanently tied to each individual, meaning any fingerprint data that lands in the wrong hands can lead to severe privacy and fraud issues. Because fingerprints are permanent, the potential of someone obtaining that data could lead to lifetime worries of fraud (Ruggiero & Foote, 2012). When incorporating biometrics within technology, there is always a large privacy

risk of personal information falling into the wrong hands that can be harmful for individuals who adopt fingerprint technology.

Why Fingerprint Technology is Not the Solution

While the Touch ID significantly improves security for user's who previously did not set passcodes for their IPhone devices, fingerprint technology is limited to an increased amount of convenience, only providing a small level of security. Apple claims, "Touch ID" provides, "a very high level of security", however fingerprint technology is not a form of encryption, meaning it does not protect users' data and information on the device (Rivera, 2013). Any password or passcode can eventually be cracked through using tools like XRY and MRE (Rivera, 2013). While Touch ID uses another form of authentication (fingerprint images), it is still possible to be replicated. As mentioned before, the Chaos Computer Club was able to accomplish the hack within 48 hours after the IPhone 5s was released to the public (CNet, 2013). Once the authentication method is bypassed, personal data and information is fully accessible to the non-authenticated user. Important information can now be acquired, copied, or erased from the smartphone device. These first level security methods have limitations and are not the solution for secure personal information and data storage on smartphone devices.

The only real way to protect personal information and data on smartphone devices is by method of encryption (Rivera, 2013). Encryption methods using AES (Advanced Encryption Standard) have been implemented on Apple's smartphone devices since the IPhone 3GS (Garfinkel, 2012). However, once the user enters in the correct information to authenticate access to the smartphone, the encrypted data is restored to human readable information. This encryption method is limited to the cracking of the Touch ID as mentioned before. One feasible solution for smartphone security would be to require a ten-

character passcode after the scanning of a user's finger (Garfinkel, 2012). This method provides an improved version of two-step authentication, requiring a user to scan their finger and provide a ten-character passcode. Yet, this would create hassle and inconvenience for everyday smartphone users, forcing them to authenticate two times, while also running the possibility of the encryption password becoming hacked.

In addition, palm recognition and eye recognition systems have also been considered for implementation in smartphone devices. A Japanese company *Softbank Mobile Corp* developed an application that scans users' palm patterns using the front facing camera on smartphone devices (Yirka, 2012). Palm recognition systems have been compared to other methods of biometrics including fingerprint matching. Research has found that palm recognition using genetic based algorithms is reliable 96% of the time versus one fingerprint, which is reliable 92% of the time (Cenys, Gibavicius, Goranin, & Marozas, 2013). However, one issue that Softbank Mobile Corp's application has is that it needs proper lighting, meaning users would not be able to authenticate in the dark (Yirka, 2012). Furthermore, EyeVerify developed an application that authenticates smartphone users by reading the patterns of veins in the users' eyes (Metz, 2012). While the application can identify the difference between an image and a real person, the technology is limited to the resolution of the camera on the phone (Metz, 2012).

Both palm recognition and eye authentication seem like probable solution to smartphone security. However, because palm prints provide more information, detail and have increased accuracy over fingerprints, the technology is still limited to non-alterable biometric information that is subject to objects that users interact with each day. On the other hand, eye authentication suggests a stronger solution to smartphone security

because the biometric data for eyes is not permanent nor does it leave traces on objects. The orientation of veins inside eyes changes over time, meaning the biometric data is alterable rather than permanent like for fingerprints (Metz, 2012). However, humans are not in control of eye vein orientation, meaning authentication cannot be changed when the user desires. This concern is something smartphone users may want to reflect upon when considering eye authentication for personal data security purposes.

Conclusion

With the increasing adoption of smartphones, security concerns will continue to grow until there is a probable solution for protecting personal information and data on these devices. While fingerprint technology provides advantages over passwords, there are three main limitations that restrict the technology from making smartphones more secure, which include the inability to alter authentication, the possibility of fingerprint replication, and the loss of accuracy from the technology. Debates of whether the importance of smartphone security lies in protection of personal information or convenience for users remain prominent. When viewing security significance for personal information and data, it is important to consider valid authentication over convenience. The palm recognition method provides only a solution to the accuracy concern of fingerprint technology, however eye verification and encryption deliver solutions that are significant, offering biometric data that is alterable, two-step authentication, and non-accessible data to the public. Eye authentication and encryption provide solutions for secure personal information, rather than user convenience. Worst-case scenarios should always be considered in regards to an individual's personal data and information, especially for smartphone devices.

Bibliography

Apple. (2013, October 22). IPhone 5s: About Touch ID security. Retrieved from http://support.apple.com/kb/HT5949

Apple unveils fingerprint tech for iPhone 5s access and iTunes payments. (2013). *Biometric Technology Today*, 2013(8), 1.

Cenys, A., Gibavicius, D., Goranin, N., & Marozas, L. (2013). Genetic algorithm based palm recognition method for biometric authentication systems. *Electronics & Electrical Engineering*, 19(2), 69-74.

Dass, S. C. (2013). Fingerprint-based recognition. *International Statistical Review, 81*(2), 175-187.

Epstein, Z. (2013, December 5). Touch ID on Apple's iPhone 5s is losing accuracy over time for some users. *Yahoo! News*. Retrieved from http://news.yahoo.com/touch-id-apple-iphone-5s-losing-accuracy-over-173542063.html

Garfinkel, S. (2012, August 13). The iPhone has passed a key security threshold. *MIT Technology Review.* Retrieved from http://www.technologyreview.com/news/428477/the-iphone-has-passed-a-key-security-threshold/

Griggs, B. (2013, September 15). How secure is your iPhone 5S fingerprint? *CNN*. Retrieved from http://www.cnn.com/2013/09/12/tech/mobile/iphone-fingerprint-privacy/

Knott, C., & Steube, G. (2012). Student perceptions of password security and maintenance. *International Journal Of Management & Information Systems*, 16(3), 189-202.

Leonard, H. (2013, February 7). There will soon be one smartphone for every five people in the world. *Business Insider.* Retrieved from http://www.businessinsider.com/15-billion-smartphones-in-the-world-22013-2

Metz, R. (2012, December 4). Instead of passwords, security software checks your eyes. *Mashable*. Retrieved from http://mashable.com/2012/12/04/password-security-eyes/

Osborne, C. (2013, September 17). IPhone fingerprint scanner sparks privacy worries. *CNET News*. Retrieved from http://news.cnet.com/8301-1009_3-57603298-83/iphone-fingerprint-scanner-sparks-privacy-worries/

Rivera, J. (2013, March 28). How secure is the passcode on my phone? *Lifehacker*. Retrieved from http://lifehacker.com/5992740/how-secure-is-the-passcode-on-my-phone

Rosenblatt, S. (2013, September 10). IPhone 5S comes with Touch ID fingerprint scanner. *CNET News*. Retrieved from http://news.cnet.com/8301-1009_3-57602245-83/iphone-5s-comes-with-touch-id-fingerprint-scanner/

Ruggiero, P., & Foote, J. (2012). Cyber threats to mobile phones. *United States Computer Emergency Readiness Team*. Retrieved from https://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf

Sanzziri, A., Nandugudi, A., Upadhyaya, S., Qiao, C. (2013). SESAME: Smartphone enabled secure access to multiple entities. *Computing, Networking and Communications (ICNC), 2013 International Conference on Computing*. (879-883).

Strange, A. (2013, September 15). No, a severed finger will not be able to access a stolen iPhone 5S. *Mashable*. Retrieved from http://mashable.com/2013/09/15/severed-finger-iphone-5s/

Watson, S. (2008, March 24). How fingerprinting works. *HowStuffWorks.* Retrieved from http://science.howstuffworks.com/fingerprinting3.htm

Whitney, L. (2013a, September 25). Hacker video shows how to thwart Apple's Touch ID. *CNET News.* Retrieved from http://news.cnet.com/8301-13579_3-57604554-37/hacker-video-shows-how-to-thwart-apples-touch-id/

Whitney, L. (2013b, September 5). Half of Internet users worry over personal info exposed online. *CNET News*. Retrieved from http://news.cnet.com/8301-1009_3-57601478-83/half-of-internet-users-worry-over-personal-info-exposed-online/

Whittaker, Z. (2013, September 10). IPhone 5S fingerprint sensor: The end of passwords? *CNET News.* Retrieved October 22, 2013, from http://news.cnet.com/8301-1009_3-57602126-83/iphone-5s-fingerprint-sensor-the-end-of-passwords/

Yirka, B. (2012, September 5). Japanese partnership results in palm recognition security for smartphones. *Phys.org.* Retrieved from http://phys.org/news/2012-09-japanese-partnership-results-palm-recognition.html