Biometrics and Security in Smartphones

Steven Bullard
Efrain Gonzalez
Carter Jamison
Saint Leo University
Saint Leo, FL, USA

Steven:
Abstract:

In this paper we look at the significance of biometrics, specifically fingerprint readers which have been implemented into smartphones, primarily the iPhone 5S. The security of the technology is presented and analyzed while the security breaches and hacks are demonstrated in detail. We look at secure options in Android vs. iOS. And we also look at the future of biometrics and soon to be wearable technology. We then propose the idea of two factor authentication and a fingerprint database.

Keywords: iPhone, Security, Touch ID, iOS, Android

1 Intro

Technology is ever changing. In a world like ours we are constantly seeking the next big discovery, invention, what have you. One of the biggest influences of our daily lives right now is the internet. With that comes the idea of carrying the internet in our pocket, more specifically, the use of a smartphone. Advances in smartphones requires equal advances in security. In a perfect world, we would not need to worry about security authentication, back-ups, passwords, etc. But we do not live in that perfect world. Things we physically own or ideas we write down, including intellectual property, need protecting.
In all honesty, the point of the fingerprint reader is to save time, and to force people to implement some form of security on their devices, which often store very sensitive data. It is a cooler looking alternative to inputting long strings of complex passwords every time you want to unlock your device or authorize a transaction in the App Store. Humans are lazy and we want speed over most everything. Touch ID allows just that while also supporting just as much, if not more security than a passcode.

2 Apple History

Officially founded in 1976 [1], garage-started Apple Computer went from being the laughingstock of the neighborhood in Palo Alto, California to a multinational corporation with an incredible reputation for constantly revolutionizing different industries. While it was not taken seriously its first few years, Apple has been ahead of the game while laying cornerstones along the way of technological advancement within our world. Apple's public offering of $22 per share in 1980 jumped 32% in the first day, instantly making 40 employees millionaires [2].

3 iPhone Evolution

In 2007 a revolutionary device was unveiled at Macworld conference, the iPhone. Although smartphones had previously been around, none were quite like the iPhone. Combining three products into one: Internet browser, iPod (already a revolutionary device on its own), and Cellular Communication. In June of 2007, the device was released to the public, selling 700,000 units on the first weekend. Although many people could not afford the device with a contract due to its outrageous price, so a year later the second generation iPhone (3G) was released at half the price, selling over 1 million units the first weekend. This also launched the App Store, a 3rd party feature that allowed anyone to develop an application using XCode and upload to the store either for free or for a designated price.

Again a year later, as we start to see a pattern, the 3G is given an internal overhaul, selling another 1 million units opening weekend. In 2010, Apple decided to change things up a bit by reinventing the exterior of the phone, which had been roughly the same size and shape for three years. The iPhone 4, along with its new operating system which contained hundreds of fixes and updates also introduced a soon-to-be trademark feature that many Apple fans were waiting for, the Retina display.

In 2011, Siri, the artificially intelligent companion was introduced along with the iPhone 4S, selling a whopping 4 million units first weekend. In 2012 the introduction of iPhone 5 changed the physical dimensions of the glass screen that had been used for five years, making the resolution natively 16:9, which meant no more black bars when watching movies; a courteous renovation. Which leads us to today, 2013, and the first time in iPhone history of a dual device release. The iPhone 5S with its notable fingerprint reader, and the 5C which adds a splash of plastic color, undoubtedly geared towards a younger audience. Both these devices sold 9 million units their first weekend and are now available in 47 countries around the world [3].

4 5S vs. 5C

Fig 1 – iPhone 5S Touch ID Sensor http://icdn2.digitaltrends.com/image/iphone-5s-fingerprint-sensor-details-625x417.jpg

So why did Apple choose to release two devices at the same time? They probably wanted to create a more affordable device for those who previously had not been able to purchase Apple products due to their notorious overpricing. The biggest noticeable difference between the two models (5S and 5C) is their exterior. The 5C is made from a hard-coated polycarbonate [4], which is just a fancy way of saying cheap China plastic, and the 5S is made from aluminum like the previous model. Internally, they are vastly different. The 5S is sporting the new A7 processor, which is a 64-bit kernel architecture, the first ever smartphone to do this; while the 5C is still using the A6 processor. The 5S also has a new motion co-processor, which works the accelerometer and gyroscope to further pinpoint details of its user's current condition (if they are standing or sitting).

The 5S has a slow-motion video ability which enables the user to record up to 120 frames per second in 720p. Of course the most intriguing of these differences is the 5S fingerprint reader (dubbed Touch ID) that is built right into the Home button. The iPhone lets you add up to five unique fingerprints which can be selected to unlock the phone and even authorize purchases from the App Store. This feature is a hot debate right now in regards to the actual security it claims.

5 iPad Air – No Touch ID?

The iPad Air and iPad Mini with Retina, both released after the 5S, do not have the Touch ID feature. There are a few speculations as to why, but primarily Apple's way of doing things is keeping new technology product-exclusive for as long as possible before branching out and implementing it to other devices. The most plausible guess is that it was simply a productivity error. There were known problems with 5S production [5] with the Touch ID feature, and seeing as these devices were announced right around the same time, it could just be that there simply was not enough resolve to meet deadlines – so perhaps Touch ID will be implemented on the next generation tablets, most likely to release Quarter 4 of 2014. Or perhaps this feature is already on its way out from the problems users have been running across with the 5S?

6 Touch ID Issues and Complaints

The fingerprint reader, like all new technology, came with bugs. Many of the consumers who purchased the latest flagship smartphone have been having more trouble than they should in regards to their Touch ID. A Wall Street Journal business editor tweeted regarding his own device that the Touch ID was buggy and worked, "a very frustrating 70% of the time." [7] This 70% is generous compared to what some users are claiming however.

The way the Touch ID actually works is like this: you set up your fingerprint (1 of 5) by repeatedly lifting and holding your desired print on and off the home button. This act does not actually store an image of your fingerprint (like those in the database of the cool crime scene TV shows) but instead translates your input as a mathematical representation, to which Apple claims cannot be reverse engineered [6].

This mathematical representation can be thought of exactly like a hash function. The iPhone then stores this encrypted information in a secret compartment within the A7 chip, known as the Secure Enclave, which was specifically developed to protect Touch ID and passcode data. The encrypted data is protected with a key that only the Secure Enclave has access to. This data is only ever used and seen by the Secure Enclave, meaning no other 3rd party app or even the Operating System has access to your print (or rather, hash), which also means it is not stored anywhere on Apple Servers, backed up to iCloud or anywhere else you can imagine – it is totally locked down to that unique device. Apple took this even a step further by pairing each and every Touch ID Sensor to only the device or CPU that it is associated with.

This theory was tested and proved by employees at iMore blog and forum. They took two brand new devices, ensured the Touch IDs worked, swapped the Touch IDs within devices, and tested the feature, finding that it did in fact not work. When setting up a new print the screen fails immediately. They swapped the sensors again to find the Touch IDs working again

with their original respectively paired devices.

This adds an extra layer of protection unique to each device. An attacker would have to modify the sensor cable itself in order to tamper with the Touch ID feature under the hood, so to speak. However, this makes DIY repairs a little bit more challenging, especially since removing the Touch ID is required for replacing cracked screens, probably the most common repair due to the full-glass front and back of the device mixed with the carelessness of those who do not invest in a warranty or protective case.

7 Ways to Improve the Feature

With biometrics implemented into pocket devices, there are a lot of areas where physical problems can arise. Moisture, oils, sweat, and debris can affect the overall performance of the Touch ID [8]. Keeping your device (and hands!) clean by using microfiber cloths can certainly help decrease the print fail rate. Since people are cell phone dominant, meaning they use a designated pocket to hold it and a designated hand to grab it, usually linked with which hand they write with, there is a way to increase recognition. The iPhone allows for up to five fingerprints. But what the iPhone does not know, is if you are using the same print for each one registered. Most people usually use their dominant thumb to unlock, so by adding five prints of that same thumb, there is a greater chance the device will recognize it and accept it.

8 Cost to Build an iPhone

Apple spends exactly $199 (with the majority of that cost going to the glass screens) on a 16GB 5S model, which retails for $649 [9], however the majority of those who purchase iPhones wait long enough to be eligible for a discount (with the renewal of a 2-year contract from a service provider like AT&T) which then costs the customer exactly $199. Apple profits from each device when the service providers pay to add that device to their array of smartphones; and from the few crazy and wealthy percent who pay full price.

9 Security Breaches

Less than two days after the iPhone 5S was sold to the public there were multiple accounts of those who claimed they had bypassed the fingerprint reader, as if it was their only mission. A notable group of German hackers, known as the Chaos Computer Club [11], uploaded a video to YouTube showing they could indeed bypass the Touch ID sensor. They photographed an original fingerprint at a high resolution, then cleaned the image in post-production, inverted the image and laser printed it to a transparent sheet with thick black toner ink, then they used pink latex milk to transfer the 'negative' print to the flesh like material. This fake print was then heated up by human breath to give it moisture which then successfully unlocked the iPhone on the first attempt. YouTube Video Here: https://www.youtube.com/watch?feature=player_embedded&v=HM8b8d8kSNQ

Apple claims its fingerprint sensor is better than those existing currently due to its higher resolution scans, but all the hacker group had to do was increase the resolution of the photographed print respectively. The CCC comments that, "It is plain stupid to use something that you can't change and that you leave everywhere every day as a security token." [10] This hack was the 3rd security flaw reported since the devices

release. Previously someone discovered how to bypass the lock screen to access photos and email. Also another person discovered how to make a phone call to any number from a locked device by exploiting the emergency call function. Apple's head of software, Craig Federighi, comments on the idea of extracting a fingerprint digitally from the actual device, "No matter if you took ownership of the whole device and ran whatever code you wanted on the main processor, you could not get that fingerprint out of there. Literally, the physical lines of communication in and out of the chip would not permit that ever to escape." [10]

10 Other Companies Adopting This Technology

Apple is not the founder of fingerprint technology. In fact fingerprint readers have been implemented to security features long before the iPhone was even invented. Even Motorola had integrated a print reader in one of their smartphones in 2011, a model called the Atrix. Ironically, right after the release of iPhone 5S Motorola sent a tweet intending to put down the idea of fingerprint readers in cell phones [12]. HTC proclaimed shortly after the 5S was announced that they too would have a device with this technology.

The HTC One Max's fingerprint sensor is more difficult to use and is not as well integrated to the device as the iPhone's. The sensor itself is located on the back of the device, making it hard to see when you hold it properly (screen facing you). It is located right underneath the protruding glass that covers the camera lens, and since it requires a swiping motion to activate, more than likely your finger will smudge the glass and blur your next photo. It is not easily felt as the iPhone's which is built into the indented home button, so often users have to physically turn the phone over to see where to put their fingerprint [13].

11 Firmware

iOS 7 is all the rage right now. Whether you love it or hate it, iOS 7 is advanced and completely diverse from the previous iPhone Operating Systems throughout the years. But something that unique is bound to come with issues that need patching. Currently on iOS 7.0.4, the previous firmware updates were primarily geared towards bugs in the Touch ID [14]. 7.0.1 fixed an issue regarding Touch IDs authentication in the iTunes Store. 7.0.2 fixed bugs that allowed a hacker to bypass the lock screen passcode (as stated in the security breach section). Along with 7.0.2 they introduced a Greek keyboard for passwords, improve security. 7.0.3 was a huge update, including a feature called iCloud Keychain, which keeps track of all your usernames and passwords along with associated credit card numbers [15]. A password generator was also implemented into the web browser to suggest unique and hard to guess passwords. And another lock screen bypass hack was fixed. Future patches should allow for two-factor authentication when unlocking the device. Meaning a user can choose to unlock the phone with a required fingerprint and then passcode or password as well.

Efrain:

12 Android vs. iOS

Since the beginning of time, or should we say since smartphones have been around, they have completely changed our way of life. The question that remains, which is still one of most heated and contended debates in regards to mobile

smartphones security is "Which is more secure, iOS or Android." To answer this question I will not review iOS 1.0 till 7.0 or Android Cupcake (1.5) till its most recent version released Jelly Bean (4.3). This question will be answered on the two most recent operating systems (OS) available and most wildly used today, Apple's iOS 7 and Android's 4.3 Jelly Bean. Although like anything else in life, aesthetics and ease of use cloud our judgment and we are more likely to use the newest and greatest thing around instead of taking security into consideration. In fact "only 12% of buyers take security into account when they're buying a phone." [16] To compare these two OS we will use a three layer approach and I will use my personal phones for comparison, starting from the lock screen, to application security, and finally on to advance security protection. The iPhone is loaded with iOS 7.0 and the Galaxy S 4 is currently running Android 4.3 Cyanogen mod.

13 Security Options

In the first layer, we are at the lock screen of both phones. With Android I am presented with five options to secure my device:

1. Slide unlock which has no security features, it just needs to be utilized in order to gain access into the phone.
2. Face Unlock, which is by no means secure, in fact it was proven to be faulty by using a picture to gain access to the phone.
3. Pattern, which is fairly secure, but less secure if the owner does not clean their screen.
4. A pin, which is the second most secure, which increases with the amount of digits.
5. A password which like any other password can be a simple password such as "12345pass" to whdzsa#7%2*&%Fs"

In iOS 7 with an iPhone 5S you only have three options.

1. Slide unlock which has no security features, it just needed to be utilized to gain access into the phone.
2. A pin which is the second most secure, which increases with the amount of digits.
3. Or you are able to choose to not have a simple pin and you can use a password as in Jelly Bean. This feature is there newest and will be thoroughly discussed through this paper. Their fingerprint reader, which is used to gain access to the phone.

If these options are taken into consideration, overall they all provided amply options, but a user would be more inclined to choose Android in this case.

14 Google Play vs. App Store

The second layer to consider is the Google Play Store vs. Apple's app store. As we all know, and the more technologic inclined are to assume that because Google does not require there app's go to rigorous testing before being released to the public they are more likely to harbor malware. Which yes, they can be correct, but just because Apple takes this precaution does not make it more secure that Android. In fact recently Apple allowed an app called Jekyll into its app store. This app "could send e-mails and text messages, tweet, take photos, steal personal information and device ID numbers, and attack other apps, all without the user ever knowing. It even had a way to direct Apple’s Safari browser to a webpage

filled with additional malware." [17] So both are able to be taken advantage of.

Android, being an open source platform allows their users to have full control of their phone and install applications from approved sources to unapproved sources. This gives the user empowerment and less headaches trying to perform work around as in the iPhone. In addition unlike iOS which prompt's a user upon installing a new application 'If the user allows the application to access data and statistical information'.

Android actually displays all the information that the app will access and asks for approval before being installed. More so, in the current rom I am using it goes even further and contains an option called Privacy Guard. Privacy Guard manages which apps have access to your personal information, regardless of what agreement you might have made upon installation. This is a huge feature only available on Android. However, even though Android has all these available features, iPhone still comes out on top since it takes such preventative measures to combat malware from being introduced in its app store.

15 Advanced Security

The third and final layer, which will be discussed, is advance security options. In Android, once the phone is rooted a program called super user is installed. This app denies all access to apps which are not approved for use. This app also has the ability to set certain time lengths of approval. The times range from "This time only", "The next 10 minutes", or "Permanently". For those who are familiar with Linux, it is essentially root permission from an application which can be very useful, but also dangerous to the inexperienced. Android also has a feature, which is not enabled by default. This feature is encryption, and Android uses AES-CBC 128bit on its phones. Unfortunately, it is not enable by default and takes extra time to setup. The setup time is worth the added layer of security. iOS one up's Android again by implement its encryption by default, and it uses a whopping AES 256-bit encryption. [18] iPhone wins in this area as well by implementing the features by default, it ensures its users are protected from the moment they begin to use their phones. As one can see, both are very powerful and have their own advantages and disadvantages, however in the case of security iOS 7 comes out on top.

This day of age, the technology we have at our fingers are fascinating, welcomed and are also becoming the norm. It is not uncommon to see a family household where each member has at least two electronic devices. Those devices range from iPhones, Android phones, iPad's, or Android tablets. We can only imagine what will be available 10 years from now. With all this technology it makes us lazy as human beings, why go research in a library when it is so much more easier and convenient to use a search engine such as Google and after a few clicks you are looking at exactly what you were looking for. The disadvantage that we are facing with this technology is from a security stand point. Security is constantly evolving at the same rate as new features and devices are coming out to help use with our daily lives that we are unable to keep up from new attacks and breaches.

The Apple iPhone 5s is a prime example, aesthetically the iPhone is superb, as well as it’s graphically user interface is very forgiving for beginners. So a question that might be asked is, "Why is this such a bad thing?" The reason is that we as consumers are looking for devices that are simple yet secure from all things good or

bad. We are looking for simplicity, since we are too lazy to punch in a password/ pin code but we want the security like that of a Top Secret government facility. It is impossible to have both. The iPhone 5S new feature is one of those that cannot be both. As previously discussed it has implemented a fingerprint reader, which not only allows access to navigate the iPhone, but also enables the users to purchase items directly from the iTunes store. This is wonderful, but from a security point of view it can introduce many issues. What issues might that be?

A brief and very likely situation can occur, suppose someone nefarious gains access to your phone, and let's also suppose a person has their Gmail account in their iPhone, which is not uncommon these days. With any person's email address, the account can contain very sensitive information. That sensitive information can range from personal images to banking information. A person's email essentially keeps a digital footprint of a person's life. When you purchase an item from Amazon, you are sent an email receipt, when you make payments in other accounts you are sent an email. When you create other accounts such as a Facebook or an online banking account you must register it with a legitimate email account. However more importantly when you forget your password where is the new temporary one sent, or where is the "change your password" link sent to, your email of course. All it takes is for one person to access your phone and your life can be drastically damaged.

16 Two Factor Authentication

Yes you can have enabled Two-factor authentication on your accounts via the Google Authenticator app, which provides users with a randomly generated token that expires after 30 seconds. However where exactly is that app located, on the phone of course. Another question that might be asked is how can this happen my fingerprint biometrics cannot be hacked. On the contrary as human beings we leave our finger prints everywhere, anything we touch, the fingerprint can be lifted and copied to create a fingerprint a sensor would not know was real or not. In addition "As Deloitte & Touché researchers noted way back in 2006, spoofing a person's biometrics, particularly fingerprints (using lifted prints on gummy bears), and is a legitimate threat. However, it's the second problem with biometrics that is the really big one: once a person's biometrics have been compromised, they will always be compromised." [19]

So the question that remains is how can we use this unique trait, and is it even worth our time and investment? Although like anything having to do with technology, it will continue to get better, and now that it has been integrated with one, if not the most popular brandings other manufactures will follow suit and implement those in their phones. So essentially it comes down to us computer scientists. We need to create solutions to resolve this issue, and others to come in the future.

The main advantage that comes to mind is since it is not secure enough to be used alone, it will enhance security since it can be used as a layered defense strategy, which is also used in Network Security. Like with anything, two things are better than one, and the same is true here. I suggest a fix to this problem is to implement a two-factor option which can be enabled by the user via it settings. Not only should a user be able to authenticate themselves via the fingerprint readers, but they should also have to enter a pin passcode. These two together will greatly increase its security.

Carter:

17 Biometrics

Biometric Authentication, also known as Biometrics, is a form of technology that makes use of biological traits for identification purposes. Using biometrics as a form of security has really expanded over the last few years quite rapidly. This has happened mostly for two reasons, the first of which is security and the second is convenience. Biometric identifiers are basically split up into two groups; the first is physiological. This includes fingerprints, palm prints, facial recognition, retina scanning, DNA, and iris recognition. The second form is behavioral which includes voice and typing rhythm. In computer science, most biometric authentication is used for access control. The most common example of this is using biometrics as a password, although it is not uncommon for biometrics to also be used as an identifier. [20]

18 Uniqueness

Since biometrics are unique to the individual that they are describing, they tend to be more secure than previous methods of identification and access control. Previous methods for these include photo identification and written passwords. It is much more difficult to fake a retina scanner or palm print than to guess a password or create fake photo identification.

Typing a password or constantly carrying photo identification is also much more of a hassle than placing your palm or eye up to a scanner. Granted the first two methods are not an enormous inconvenience or incredibly difficult, the latter two methods are much easier. Also, a password or photo identification card can be lost or forgotten, whereas a hand or eye cannot be. This contributes to the security of biometrics because not only is it more difficult to fake a palm scanner or retina scanner, but also the authorized individual cannot give or loose these to an unauthorized user

When biometric data is taken, it verifies certain parts of the scan as match points. These match points are then converted to numeric data via an algorithm. Then, this numeric data is compared to verified match points of how the scan is supposed to be. If the new numeric data is compared and accepted, the new scan is approved. If the data is rejected, then the new scan is denied. Also, all of this information is immediately encrypted to help decrease the chances of identity theft. [21]

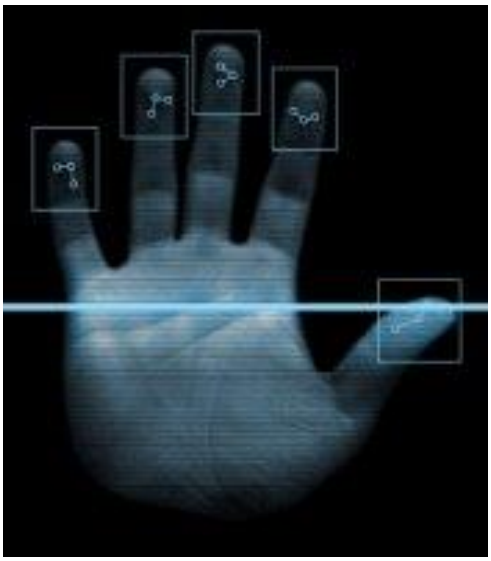

Fig 2 - http://findbiometrics.com/solutions/hand-readers-finger-scanners/

19 Principles of Biometrics

Biometric technology needs to contain a few principles in order for it to be used. The first is that every person needs to

contain whatever biological part is being analyzed (ex. If implementing a palm scanner in a business, every employee needs to have a hand). Next, the biological trait needs to be unique and permanent to every individual (ex. All humans have different palm and fingerprints and these prints do not become unrecognizable over time). Measurability and performance are the next principles; they also overlap a little. Measurability means that this trait needs to be able to measured (ex. Fingerprints) and performance means that this measurement needs to happen fast and it needs to be accurate and reliable. The final two principles are acceptability and circumvention.

This technology needs to be so secure so that the individual providing the scan needs to feel secure and not worried, and also the one protecting the information (ex. The employer) needs to feel safe that their private information is guarded by this biometric security. Circumvention refers to how easy these biometric traits can be faked or bypassed. Circumvention can be decreased by multimodal systems. These systems have multiple copies of the same verified match points, therefore increasing the verifications that new match points are compared to. This allows for things like cuts on fingers during a finger scanning to go unnoticed. [22]

20 The Future

As the future progresses, biometrics will become more entwined with it. Currently, the largest biometrics database system is in India, it's called the "Aadhaar." It's India's National ID program. It is a biometric identity which will follow an individual their entire lifetime. Also, it's accessible and verifiable instantly, anytime, and anyplace. Currently, there is about 550 million people currently a part of the database, however India aims to enroll the entire population in it. [23] At the moment, it looks like the next biometrics technology to emerge will be brain and heart signals. Currently, researchers at the University of Wolverhampton are leading the way regarding the research and development of this technology, although it appears that this form of biometrics will not be as fast to procure and it looks like it may be quite difficult to read accurately.

While biometrics obviously display an immediate side of safety, there are still quite a few concerns regarding it. While things like a face cannot be replicated (at least for the most part), it can still be compromised. If the facial image of person is compromised or stolen, nothing can be done regarding the matter. That person's information and image is now available to the public or toward a malicious person. On the other hand, if a password is stolen, it can be cancelled and a new one can be reissued. This gives a password an advantage for sure. Also, some items require a form of biometric security (example, a safe containing a lot of money). If some thief wants to steal this safe, they will likely need the person whose biometrics unlock it, which could lead to kidnapping or even worse. Another issue regarding biometrics is privacy. By giving someone (or by having this information stolen) a finger print or DNA sample, you are relinquishing some serious personal security and allowing yourself to be put in certain unwanted situations. DNA can be used in many different ways in today's world. It could be analyzed (in an unwanted way), given or sold to another organization or person, or it can even be used to frame a person. A fingerprint can also be used in similar unwanted fashions. This added sense of unique security is essentially a double-edged sword. [24]

21 Wearable Technology

Although it is not really a form of biometrics, there are many technological devices that are constantly being developed for use with the human body. A wonderful example of this is Google Glass. Glass is essentially a pair of glasses that can be connected to a smartphone powered device and can display information on the inside of the glasses and can be controlled via the human eye. A person can open applications and perform many of the same functions simply with the movement and blinking of their eyes. Other similar devices are constantly be developed as well. Recently the watch market has included devices like this. Currently, Samsung offers a watch, which can be connected to the Samsung Note 3 via Bluetooth and can function similar to the smartphone itself.

While biometrics seem be helping to pave the way of the world's future, there are certainly some issues and kinks which need to be worked out. As the field increases, there will definitely be new and better forms of biometric security introduced as well.

Works Cited

[1] Stanford, Glen. "Company History: 1976-1981." *Apple History*. N.p., n.d. Web. 25 Nov 2013. <http://apple-history.com/h1>.

[2] Mesa, Andy. "Apple History Timeline." *Apple Museum*. N.p., n.d. Web. 25 Nov 2013. <http://applemuseum.bott.org/sections/history.html>.

[3] iClarified, . "The Evolution of the iPhone." *iClarified*. iClarified, 10 Nov 2013. Web. 25 Nov 2013. <http://www.iclarified.com/35644/the-evolution-of-the-iphone-infographic>.

[4] Costello, Sam. "7 Key Differences Between iPhone 5S and iPhone 5C." *About*. About, n.d. Web. 25 Nov 2013. <http://ipod.about.com/od/iPhone5SandiPhone5C/tp/Differences-Between-Iphone-5s-Iphone-5c.htm>.

[5] H, Michael. "No TouchID fingerprint scanners on new iPads." *Phone Arena*. N.p., 22 Oct 2013. Web. 25 Nov 2013. <http://www.phonearena.com/news/No-TouchID-fingerprint-scanners-on-new-iPads_id48583>.

[6] Kazmucha, Allyson. "Touch ID takes hardware security to new levels." *iMore*. N.p., 31 Oct 2013. Web. 25 Nov 2013. <http://www.imore.com/apple-took-touch-id-security-one-step-further-secure-enclave-heres-how-and-what-it-means>.

[7] Wolverton, Troy. "Apple iphone's new fingerprint sensor draws complaints." *silicon beat*. N.p., 18 Nov 2013. Web. 25 Nov 2013. <http://www.siliconbeat.com/2013/11/18/apple-iphones-new-fingerprint-sensor-draws-complaints/>.

[8] Kahn, Saqib. "Quick Tip How to improve iphone 5s's fingerprint recognition." *Value Walk*. N.p., 25 Nov 2013. Web. 25 Nov 2013. <http://www.valuewalk.com/2013/11/improve-iphone-5ss-fingerprint-recognition/>.

[9] Zeman, Eric. "$649 iPhone 5s costs Apple $199."*information week*. N.p., 24 Sep 2013. Web. 25 Nov 2013. <http://www.informationweek.com/mobile/mobile-devices/$649-iphone-5s-costs-apple-$199/d/d-id/1111661?>.

[10] Curis, Sophie. "iPhone 5s fingerprint sensor hacked within days of launch." *Telegraph*. N.p., 23 Sep 2013. Web. 25 Nov 2013. <http://www.telegraph.co.uk/technology/apple/iphone/10327635/iPhone-5s-fingerprint-sensor-hacked-within-days-of-launch.html>.

[11] Arthur, Charles. "iphone 5s fingerprint sensor hacked by German'ys chaos computer club." *the guardian*. N.p., 23 Sep 2013. Web. 25 Nov 2013. <http://www.theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked>.

[12] Greenberg, Andy. "Motorola bashes apple's iphone fingerprint reader; forgets it sold one first." *Forbes*. N.p., 11 Sep 2013. Web. 25 Nov 2013. <http://www.forbes.com/sites/andygreenberg/20

13/09/11/motorola-bashes-apples-iphone-fingerprint-reader-forgets-it-sold-one-first/>.
[13] S, Ray. "HTC's implementation of the fingerprint sensor shows why others have failed in this before." *Phone Arena*. N.p., 28 Oct 2013. Web. 25 Nov 2013. <http://www.phonearena.com/news/HTCs-implementation-of-the-fingerprint-sensor-shows-why-others-have-failed-in-this-before_id48720>.
[14] iPhoneHacks, . "Download iOS 7.0.1 for iPhone 5s and iPhone 5c, fixes Touch ID bug." *iPhoneHacks*. N.p., 21 Sep 2013. Web. 25 Nov 2013. <http://www.iphonehacks.com/2013/09/download-ios-7-0-1-iphone-5s-iphone-5c-fix-touch-id-bug.html>.
[15] Anonymous, . "iOS Support." *Apple*. Apple, n.d. Web. 25 Nov 2013. <http://www.apple.com/support/>.
[16] softonic. "Security Showdown: iOS 7 vs. Android 4.3". Web. http://features.en.softonic.com/security-showdown-ios-7-vs-android-4-3
[17] Gigamon "Researches show how to slip malware into Apple's App Store" Web. http://gigaom.com/2013/08/17/researchers-show-how-to-slip-malware-into-apples-app-store/>
[18] Apple " iPhone in Business" Web. http://www.apple.com/iphone/business/it/security.html
[19] Aitel, Dave. USAToday. "Why fingerprints, other biometrics don't work". Web. http://www.usatoday.com/story/cybertruth/2013/09/12/why-biometrics- dont-work/2802095
[20]"Biometrics Security." RSS 20. N.p., n.d. Web. 25 Nov. 2013. <http://findbiometrics.com/applications/biometrics-security/>.
[21]Sutherland, Lennard-Peter. "biometrics." Search Security. N.p., n.d. Web. 25 Nov. 2013. <http://searchsecurity.techtarget.com/definition/biometrics>.
[22]"Biometrics Security Considerations." Systems and Network Analysis Center Information Assurance Directorate. NSA, n.d. Web. 22 Nov. 2013. <http://www.nsa.gov/ia/_files/factsheets/i73-009r-007.pdf>.
[23]“What is Aadhaar?” AAPKA AADHAAR. Web. 22 Nov. 2013. <http://uidai.gov.in/what-is-aadhaar.html>
[24]“Advantages and Disadvantages of Biometrics Systems” SNG Security Web. 21 Nov. 2013 <http://www.sngsecurity.co.za/biometrics_systems_advantages_disadvantages.html>