2013 IEEE Security and Privacy Workshops

Preventing Cell Phone Intrusion and Theft using Biometrics

Fingerprint Biometric Security utilizing Dongle and Solid State Relay Technology

Donny Jacob Ohana
Sam Houston State University
Huntsville, TX, USA
djo007@shsu.edu

Liza Phillips
Law Enforcement
College Station, TX, USA
lphillips207@gmail.com

Lei Chen
Sam Houston State University
Huntsville, TX, USA
chen@shsu.edu

Abstract*—Most cell phones use a password, PIN, or visual pattern to secure the phone. With these types of security methods being used, there is much vulnerability. Another alternative is biometric authentication. Biometric security systems have been researched for many years. Some mobile manufacturers have implemented fingerprint scanners into their phones, such as the old Fujitsu F505i [7] and the current Motorola Atrix. Since theft of cell phones is becoming more common every day, there is a real need for a security system that not only protects the data, but the phone itself. It is proposed through this research that a biometric security system be the alternative to knowledge-based and password-based authentication. Furthermore, a device dongle must be implemented into this infrastructure to establish a reliable security system that deters theft for the majority; biometrics alone is not sufficient. Cell phones need power and must be charged almost daily. A biometric phone charger that acts as a dongle with a solid state relay, will be presented as a viable solution to theft in this research. Additionally, it will be shown through the results of this research that a system dependant only on biometrics is unreliable and unsecure. Essentially, a mobile security system that combines biometrics with dongle technology is believed to be the ideal solution for limiting the black market of stolen cell phones; without the biometric charger/dongle, the stolen cell phone would be rendered useless.

Keywords- mobile devices; mobile security; cell phone biometrics; biometric security; cell phone security dongle; cell phone relay

1. Introduction

Biometric security implementations are believed to prevent intrusions and theft against mobile cellular devices. Essentially, a biometric system is used for identification or verification based on physiological and biological factors. Generally speaking, criminal acts are motivated by various reasons. A victim can either be deprived of their cell phone by some form of theft, or be vulnerable to losing sensitive information through a breach in security. More cell phones are being stolen every day because there is a market which demands the supply; some refer to this as a black market which establishes an incentive for theft.

Cell phones have evolved tremendously and are progressively becoming more advanced. Instead of computers, people rather use their cell phones to check emails, surf the web, and more. Cell phones are also being used to pay with digital currency that links to a credit or debit card. This type of stored information is sensitive and appealing to different types of thieves. Once all cell phones will contain such information, the law may even change the criminal charge from theft of property to credit or debit card abuse. Biometric authentication has been studied as a security method to prevent these types of crimes. However, just like any other type of security system, there are penetrative vulnerabilities to biometric authentication systems as well; those vulnerabilities will be addressed later. We will also see how independent biometric systems are more vulnerable than combined protocols as the studies progress.

In contrast to those methods, this research proposes a framework that provides a more secure environment for mobile technology and products; a biometric recognition system that requires a synced biometric key. This can be accomplished by launching a cell phone that requires biometric authorization to access the phone and a biometric charger that must sync with the phone to enable a charge. Bottom line, the objective of this research is to establish a mobile security system that helps prevent theft of property and theft of sensitive information.

This paper is organized as follows: Section 2 and 3 describe the different types of biometric authentication systems and other authentication methods. Section 4 provides the proposed biometric architecture while section 5 discusses fingerprint uniqueness and application. Section 6 produces the implementations and experiments of this research. Section 7 and 8 conclude the paper with discussion and future work.

2. Biometric Techniques and Systems

2.1 Biometric Face Recognition

There are several different types of biometric authentication systems. Some of the more obvious ones are recognition of face, voice, and fingerprint. Other biometric authentication systems consist of gait recognition and artificial intelligence that adapts to the owner's uniqueness while combining other methods. According to one study [3] there are two types of face recognition protocols: face verification and face identification. Face identification is used for matching input identity with registered identity. Face verification is used to authorize proper access. With the system proposed in this research, the cell phone's camera was utilized to capture facial points. Once the data was captured, the system used that information to either activate or deactivate all functions. This system further used the OKAO Vision algorithm to assist with processing speed and memory usage.

DOI 10.1109/SPW.2013.19

Another study [9] used a different approach combining face recognition, location tracks, and RFID (Radio Frequency Identification Tags) technology. This adds a better sense of security since the mobile device detects whether or not the RFID badge and location is valid. The good thing about an RFID tag is that it is unique to the one that is carried by the owner. On a negative note, there are many privacy issues that would need to be addressed. For example, RFID tags can be read and tracked at a distance without the user's knowledge [12]. Besides the privacy issues held by RFID technology, there is definitely some vulnerability to a system dependent on face recognition alone [7].

Two different penetration attempts were made against a facial recognition biometric system: authentication by a photo and authentication by an image captured by another. The results of the experiment showed there was an illegal authentication success rate of 97% with a captured image and 87% with just a face photo. Based on the results, face recognition does not seem to be very secure, especially when someone could use a photo from an online social network such as Facebook or MySpace.

2.2 Biometric Fingerprint Recognition

Fingerprint recognition may seem to be a bit more secure because a fingerprint is extremely unique and difficult to mimic. One study [5] used fingerprint authentication for digital signing based on the X.509 certificate infrastructure. A unique feature to this research was the fact that users were able to download third party algorithms to customize protocols. Additionally, this research was conducted using an external USB optical fingerprint sensor and the US National Institute of Standards and Technology Biometric Image Software.

A different fingerprint authentication method was discussed in another article [6] involving an optical fingerprint reader as well. The belief in this research was that 2D code provides a more effective security protocol and QR codes are more reliable and secure. The information gathered is detailed to basic ridge patterns and specific characteristics. Both of these research articles presented a different method to the same type of biometric authentication system. According to a biometric evaluation study [7], penetration attempts were made against a fingerprint authentication system using an artificial fingerprint. The results showed an illegal authentication success rate of 81%. It seems that if an owner's fingerprint can be obtained and re-created with plastic and gelatin, a breach may take place and any sensitive information would be available to the attacker.

2.3 Biometric Voice Recognition

As a combined research method, one study [4] researched both fingerprint and voice recognition. Now that we have a better understanding of how fingerprint authentication works, let us take a look on how voice authentication differs. The idea behind this research was that three seconds was coded into the cell phone's database using a VOCODER. Once the voice was digitized, new input was compared to previous recordings for verification. A phoneme is the smallest unit of sound to form distinctions between utterances. A phoneme is also very unique and therefore only a small portion would have to be recorded for reference. One good thing about this research is that a proposed passphrase was recorded in addition to just voice. This adds extra protection against breaching this method.

Another study [10] used a biometric voice recognition system which exchanged a digital signature token encrypted and confirmed by voice. According to an evaluation study [7], penetration attempts were made against a voice authentication system using a recorded voice. The results showed an illegal authentication success rate of 89%. As we see here, voice authentication would be easier to breach than fingerprint authentication because any digital recorder could work. This includes but is not limited to the digital recorder installed on cell phones, which nowadays almost everyone carries. That being said, a session key exchanged during communication and verified by voice is a better solution than just a standard voice recognition method.

2.4 Biometric Gait Recognition and Artificial Intelligence

In contrast to independent authentication systems such as face, fingerprint, and voice recognition, other methods have been proposed to involve all three and more. One study on gait recognition [1] showed how cell phone authentication could be implemented by gathering gait data. Gait recognition essentially verifies authentication automatically by the way a person walks. In cases where a user is not walking, a PIN would be required instead. This method is unobtrusive because it is always recording and gathering data without the user having to make any physical inputs. For gait recognition to be successful, three approaches were used: Machine Vision Based, Floor Sensor Based, and Wearable Sensor Based Gait Recognition.

Another study [2] presented a method that combined all of the above with some basic form of Artificial Intelligence. The researchers believed there was too much vulnerability in biometric authentication if used independently. As a result, the researchers proposed a cell phone that would adapt to its owner like a digital pet. Artificial Intelligence is essentially a system where an intelligent agent extracts data in real time from the environment and makes decisions to increases the rate of success. In this research method, the "ePet" would not only authenticate a user based on physiological and biological factors, but the physical environment as well. The 'ePet' algorithm used both gait data and location tracks in conjunction with other biometrical authentication methods; face, voice, and fingerprint recognition.

3. Hardware Security Methods

3.1 Device Dongle and RFID Middleware

To better establish a security system that is universal, reliable, and un-obtrusive, there needs to be two pieces of hardware that requires pairing to be operable; without one the other will not work. This separates the key from the lock so to speak. Some software vendors utilize this type of security through the form of a USB device key, commonly known as a dongle. A device dongle is piece of hardware that plugs into a computer to allow authentication of certain programs to run. Furthermore, a dongle is a form of digital rights management in which security data is read from to authorize access.

Another reliable security method is a token-based authentication system such as an RFID tag. A Radio Frequency Identification-based Authentication Middleware (RFID) system uses an RFID tag as a token to authorize access via short wireless range such as bluetooth technology. Middleware, sometimes informally referred to as plumbing, is a layer of software above the operating system and below the application layer. RFID technology is widely used in retail companies such as Walmart to manage supply chains. Additionally, RFID technology is used in national identification cards in many countries [8]. The uniqueness of an RFID tag is that mere possession of this token allows access as long as the tag is within range. This protects the encrypted system and continuously authenticates the user for valid access.

Both of these security methods have been proven to be useful. As we shall see later in the proposed biometric security architecture, the cell phone charger will be incorporated as a type of dongle. Although there have been studies on protecting mobile devices with RFID tokens, the negative aspect to using this type of system is that it becomes intrusive to the user. It would not be practical for someone to possess a token on their person at all times to continuously have access to their cell phone. On another note, an RFID identification system does successfully support the theory of having two pieces of hardware to complete operability. Additionally, some Middleware advantages are portability and transparent authentication where access may occur without an overt interaction with the user.

4. Framework and Architecture

4.1 Biometric Cell Phone framework

The ultimate question that may arise is why a biometric system would be a better alternative to PIN or password based security methods. Only 18% of participants surveyed in one study used a PIN or password to secure their device [2]. Additionally, knowledge-based or password-based authentication methods have been proven to be weak solutions due to user input [8]. People tend to select short and easy passwords. In some cases where passwords are more complicated, people might write them down somewhere which that in itself is a security risk. For the more popular cell phone platforms such as the iPhone or Android OS, there are several easy ways to bypass the implemented security method. For example, if someone were to steal an Android based cell phone, they would only need to call that phone and while in duration of that phone call, press the back key. The attacker would then have full access to the phone bypassing the security PIN or pattern recognition requirement.

As shown in Fig. 1, a mobile security system, equipped with a biometric fingerprint scanner embedded into a charger/dongle, would be a remarkable solution to prevent theft. To accomplish this, both the cell phone and the charger should contain a biometric reader. The cell phone charger should also be equipped with a solid state relay. A relay is an electrically operated switch. A solid state relay acts the same but without any moving parts. To help better understand this, the framework to this research will be explained in more detail.

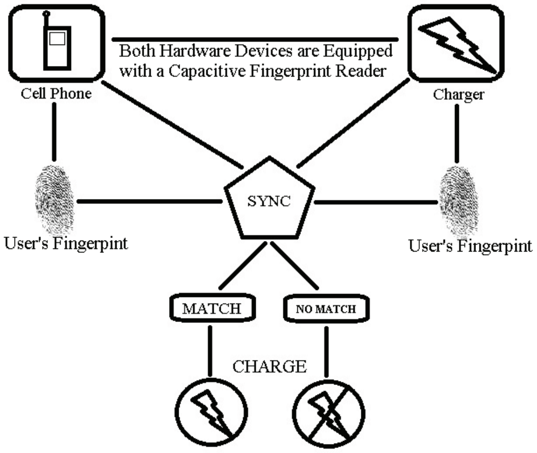

Fig. 1 Biometric Phone and Charger Architecture

As proposed, a cell phone and a cell phone charger would utilize a capacitive fingerprint reader which enables functionality. For example, when a cell phone is purchased, the cell phone would be programmed with the user's fingerprint. At that point in time, the cell phone charger would also be programmed with the user's fingerprint and can only be re-programmed by the manufacturer. The fingerprints then become an encrypted key which allows the two devices to be synced. This could also apply to a car charger, house charger, and USB cord. With the USB cord that connects to a PC, the phone's biometric reader could act as the authorization point.

Once the cell phone and charger contain the encrypted fingerprint key, the charger acts as a device dongle embedded with a solid state relay (on/off) that has to plug into the phone and be authorized to activate the charge. Additionally, the cell phone should be manufactured with a built-in lithium battery that cannot be removed. If the cell phone is ever to be separated from its synced charger indefinitely, the cell phone would be rendered useless. Reason being, the charger has to sync correctly with the phone (fingerprint match) for the phone to stay alive. In addition to this security method, the OS should provide user specificity. Meaning, the user profile and fingerprint is encrypted and specific to the encrypted fingerprint on file. If a new fingerprint key is programmed, a new profile would have to be created erasing the old one and preventing intrusion to sensitive information.

Another security feature that would be added is programming the power button to *only* lock and unlock the phone. This way if a cell phone were to be stolen, there would be no way to shutdown the phone without proper authorization. The user could then use a program such as Lookout (Android OS) to remotely destroy the data in a theft situation without having to worry about their phone being turned off. Ultimately, by the time someone steals a cell phone and attempts to hack the phone using artificial fingerprints, there should be enough time for the owner to remove their profile which is backed up onto a remote server. As we shall see later through the experimental methods in this research, biometric systems alone are too vulnerable and this proposed theory will be tested.

5. Fingerprint Uniqueness and Common Biometric Readers

5.1 Fingerprints

As we saw from earlier studies, vulnerabilities do exist in biometric security systems as well as the standard PIN or password-based security methods. That said, fingerprint recognition seems to be a better alternative compared to other biometric methods for security. Reason being, voice and face recognition can easily be spoofed using a photo or voice recording [7]. Additionally, other methods proposed such as location tracking and user recognition can be too intrusive on human privacy. In order to have a better understanding of just how unique fingerprints are, let us go over some basic facts and information.

Fingerprints serve as friction ridges to assist in the ability to grasp and hold objects. The ridge arrangements on every finger of every person are unique, different, and permanent from birth until death, unless altered by injury, disease, scaring, or decomposition. Fingerprints develop during the formation of the fetus and are in their ultimate form before birth. At about 5-6 weeks, the hand of the fetus is flat with a thick structure of tissue. About one week later, the fingers begin to separate and volar pads begin to grow as shown in Fig. 2. As the volar pads begin to regress, ridges begin to form at around 10-11 weeks. Due to the individual pressure and stresses during fetal growth, fingerprints become very different from one another. Essentially, when a baby touches the inside of the womb, the fingerprints are formed randomly. This is why no two sets of fingerprints are the same.

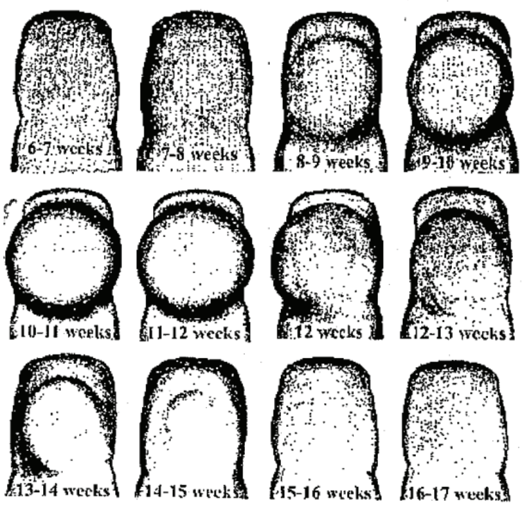

Fig. 2 Volar pad formations

Since fingerprints allow for unique human identification, it is important to learn and understand how they are analyzed. There are ultimately three levels of detail: level 1 detail such as ridge flow classification (Fig. 3), level 2 detail such as dots and Bifurcation (junctions), and level 3 detail such as ridge features (shapes, widths, and pores). It is important to note that individualization cannot occur at the level 1 detail. Fingerprints contain approximately 90% of moisture from the sweat that seeps out from the pores in the skin. Within that sweat, oils and fats are secreted. Sometimes when a person touches an object, a latent fingerprint is left behind from the oils and fats. Latent meaning it cannot be seen by the naked eye unless developed under forensic equipment. Once the fingerprint is developed, it is known as a patent print because it is visible.

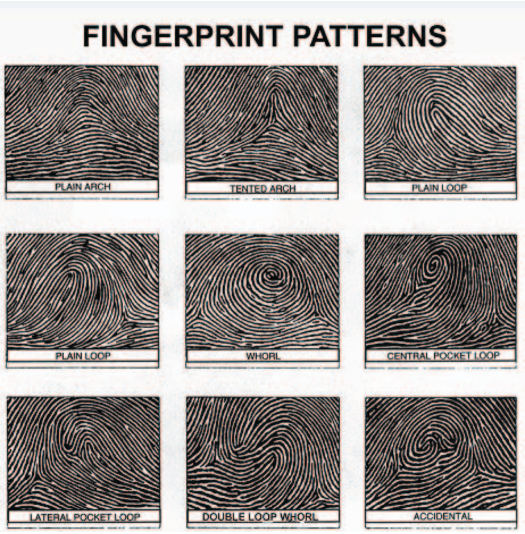

Fig. 3 Basic level 1 detail fingerprint patterns

5.2 Biometric Fingerprint Readers

There are mainly two types of fingerprint readers commonly used to access digital devices: optical and capacitive. In some of the other proposed methods established in this paper, a camera or optical fingerprint sensor was elected for fingerprint scanning [2,4,5,6]. The problem is that a camera that works as an optical scanner uses light and can easily be fooled using a detailed photo. Capacitive fingerprint readers are more difficult to spoof since the object must be able to hold an electric current and on some, the ridges must be 3D. The reliability of such a scanner will be tested in the experiments to come.

6. Biometric Implementations and Experiments for Cell Phone Security Architecture

6.1 Research Implementations

Through law enforcement experience and research, it has been seen that cell phones are commonly stolen in public places where property was left unattended. In most cases, cell phones are stolen to make quick cash at pawn shops or amongst locals. One thing to keep in mind is that a victim's fingerprint could still be on their phone or other items stolen with their cell phone. That said, it may be possible to lift the victim's fingerprint and create a mold. The artificial fingerprint based on that mold could then be used to try and authorize access on a device that has a biometric reader. If that is true, biometric security alone would not be sufficient enough to protect cell phones from theft or intrusion.

Most research studies that have successfully hacked into a system equipped with an optical biometric fingerprint reader, did so by using a live finger to create a mold. A real life scenario where someone would force another to press their finger into a mold would be highly unlikely, unless the victim was of high profile. For research purposes, the experiments will demonstrate both scenarios where there is a compliant and non-compliant victim. A non-compliant victim could also be substituted as a victim who is not present. It is important to show through this research that a biometric system would at least buy enough time for the victim to erase their data in a theft situation. Reason being, if there is a will there is a way. As of now, no mobile security system is 100% hack proof but by separating the key from the lock (phone and charger), stealing cell phones would be discouraged.

With the proposed theory of a biometric phone combined with a biometric charger that acts as a device dongle, a suspect would have several different obstacles to overcome. For example, a suspect would have to accomplish stealing both devices (cell phone and charger) for proper pairing, have the materials and knowledge to lift and re-create an artificial fingerprint, and have the equipment and programming knowledge to reset any of these devices. In most common theft situations, this would be unlikely although not impossible. Due to the lack of hardware and software accessibility, an experiment using a biometric charger with a solid state relay (on/off) was not conducted; this will optimistically be implemented in future work. However, experiments attempting to hack a capacitive biometric reader were conducted using different methods. Since most research studies focused on optical scanners, or stationary capacitive scanners, the experiments were based on a swipe style capacitive fingerprint reader with anti-spoofing technology; this obviously increases the difficulty level of hacking.

6.2 EXPERIMENTAL METHOD

It has been shown in previous research studies that biometric readers, both capacitive and optical, have been hacked using various methods. To reiterate the purpose of this experiment, the following will be tested:

- Can some of these methods be easily reproduced
- Can law enforcement forensic material be used to bypass a swipe style capacitive fingerprint reader
- Is biometrics alone reliable enough to prevent intrusion and theft without additional security
- Would the combination of preparation time and hacking, be enough for a victim to discover their --- property to be missing, log online, and erase their user profile or data

To conduct these experiments, the following materials were used:

1. Computer running Windows 7 OS
2. UPEK Eikon To Go capacitive fingerprint reader with anti-spoofing technology
3. Law Enforcement forensic equipment such as Mikrosil, black powder, magnetic powder, dusting brush and ink pad
4. Latex gloves
5. Double sided copper-clad PC circuit board (PCB)
6. Etchant solution containing ferric chloride and hydrochloric acid
7. Electric iron
8. Transparency paper
9. gelatin
10. HP Scanjet 4850 scanner
11. HP Deskjet 6988 printer

Before running any experiments, all necessary device drivers were installed for the Eikon USB fingerprint reader (Fig. 4). Additionally, the biometric reader was hardware and software tested repeatedly with positive results.

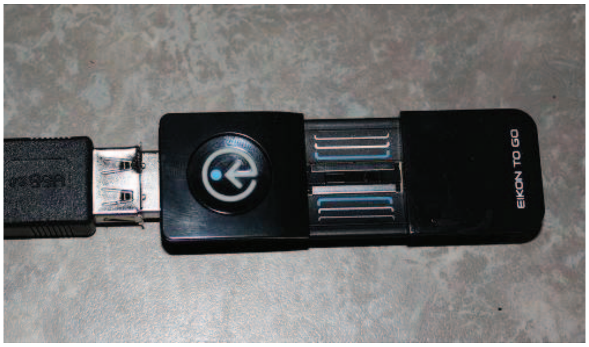

Fig. 4 Eikon To Go USB Biometric Fingerprint Reader

The first breaching attempt was made with an ink pad and a latex glove. By rolling ink on one of the fingertips before putting on the latex glove, a patent (visible) fingerprint was transferred inside the glove after pressing down firmly. The latex glove was then flipped around and placed back on the hand to swipe the finger for authorization; experiment lead to negative results (5 minutes).

The next experiment involved lifting a print from a glass cup. After touching a glass cup for a brief moment, magnetic fingerprint powder was used to develop the latent fingerprint (Fig. 5). Once the fingerprint was visible to the naked eye, Mikrosil, a forensic casting material, was used to lift the print (Fig. 6). A small amount of Mikrosil was placed onto the glass cup, over the developed print (Fig. 7). After several minutes, the Mikrosil dried and set to a rubbery substance (Fig. 8). The dried Mikrosil was lifted off the glass revealing a patent print. After the print was successfully lifted, attempts were made to breach the computer using the biometric reader; experiment lead to negative results (10 minutes).

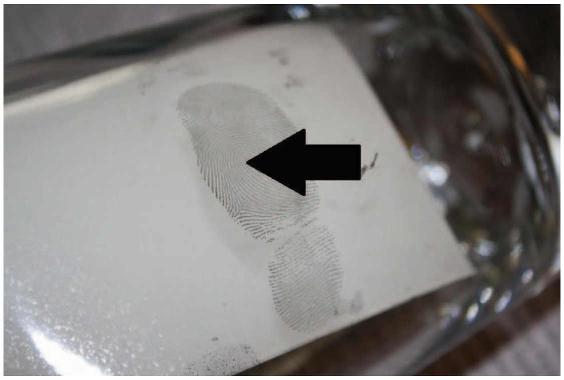

Fig. 5 Fingerprint Lifted from Glass Cup using Forensic Powders

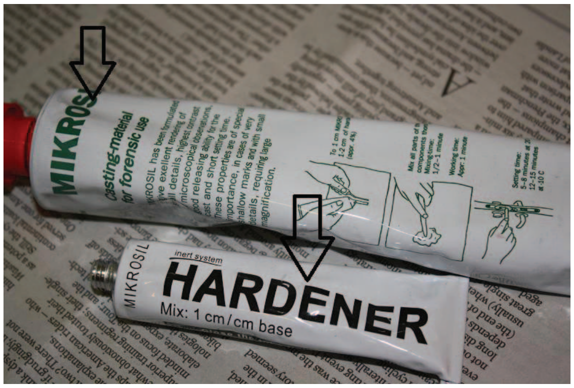

Fig. 6 Mikrosil

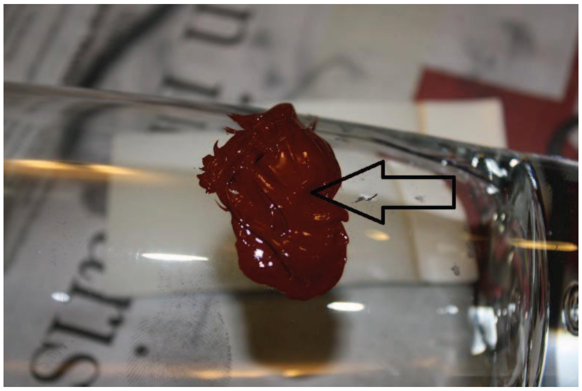

Fig. 7 Mikrosil Placed onto Fingerprint Area

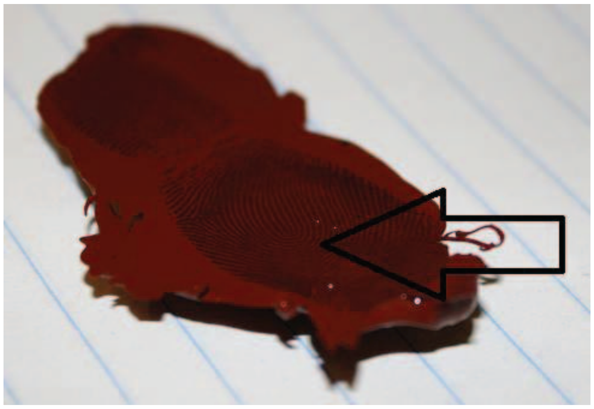

Fig. 8 Identified Lifted Fingerprint on the Mikrosil

As to try and partially mimic one of the previous studies' experimental methods [7], a 1:1 ratio of gelatin was mixed with hot water. The gelatin was then poured into a cup as the time elapsed for cool down. Once the gelatin hardened, it was removed from the cup and an attempt was made for the biometric reader to identify a finger. This biometric reader was supposed to contain anti-spoofing technology as well as the ability to detect the live layer of a finger. That being said, the gelatin was read as a live finger without recording any ridge patterns. After trying to figure out what made the capacitive reader scan one thing but not the other, it appeared moisture was the key. Since fingerprints contain 90% of moisture as mentioned earlier, it would only make sense that the capacitive reader measures moisture with electric conductivity (20 minutes).

To further experiment with the Mikrosil, a small amount was placed on one of the fingers of a compliant subject. Once the Mikrosil dried and set, it was pulled off for a further look. It could be seen that the Mikrosil molded to the fingerprint ridges in a 3D format. After attempting to swipe the mold across the scanner, nothing happened. Another attempt was made after touching the Mikrosil to some water for moisture. When swiping the Mikrosil this time around, the fingerprint reader scanned a partial image of the fingerprint.

At that point, it was clear that a combination of both moisture and 3D ridge detail would create a substantial artificial fingerprint worth scanning. To test this, the Mikrosil mold was taped onto a finger. Next, the finger was dipped into a cup of water for a short period of time. After soaking the Mikrosil fingertip in water, the fingerprint was swiped and the biometric reader successfully scanned the print almost completely. As shown in Fig. 9, the scanned image can easily be compared with the other fingerprint. However, the ridge areas that were not scanned were due to the loss of moisture in those areas (8 minutes).

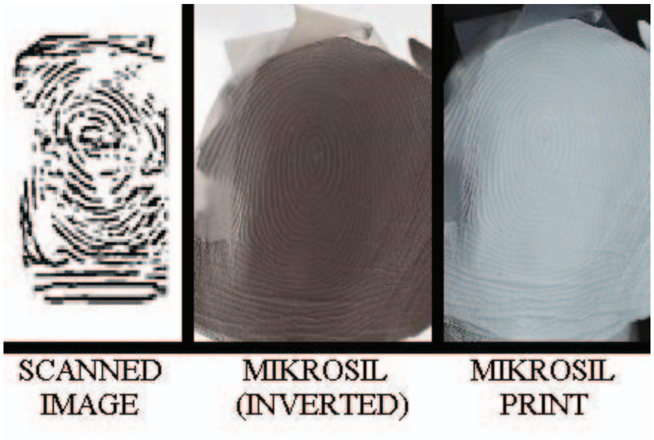

Fig. 9 A comparison chart between the Mikrosil print and the scanned image after creating a layer of water for moisture; the second photo is inverted to show the ridges better

Since the previous experiment worked, it was essential to try and make an artificial print from a patent print because the Mikrosil mold from a live finger would be considered a reverse print. Meaning, the artificial fingerprint scanned would not match the one on file. After experimenting with the Mikrosil and a compliant subject, the next experiment consisted of scanning a fingerprint lifted from an object.

A patent fingerprint was scanned onto a computer and the image resolution was converted to 600 dpi. The fingerprint image was then printed onto a sheet of transparency paper. Next, the printed fingerprint was placed faced down onto a copper clad board (PCB) and the image was transferred using an electric iron. After several minutes, the PCB board was placed into a plastic tray containing the etching solution (ferric chloride), with the image faced down for approximately 20 minutes. As shown in Fig. 10, the fingerprint remained etched as the solution removed most of the copper surrounding the print. Several attempts using Mikrosil and gelatin were made to create a 3D fingerprint from the copper mold; experiment lead to inconclusive results due to poor copper mold structure (30 minutes).

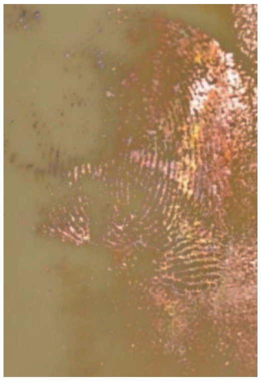

Fig. 10 Etched fingerprint remaining on PCB

6.2 Result Analysis

As shown in Fig. 11, there was relatively some positive success in hacking a capacitive biometric fingerprint reader. As we can see from the results, the latex glove had no affect on the biometric reader. Even if moisture were to be applied, the capacitive reader scans the image from reading the hills and the valleys of the fingerprint ridges; without 3D detail there is no way for it to scan. When attempting to swipe the Mikrosil, there was no biometric input without moisture. Once this theory was understood and applied, the biometric reader scanned the Mikrosil fingerprint every single time it was swiped, as long as there was moisture or water present. In reference to the PCB experiment, additional support to this research would have been founded if the copper mold had turned out more pronounced. Since the mold needed to be refined, only partial scans were able to be made by the biometric reader. That said, this experiment was still able to show that a biometric reader alone can still be hacked without victim compliance.

	Ink	**Mikrosil**	**Gelatin**	**Mikrosil w/Moisture**
Latex	NO	N/A	N/A	N/A
PCB	N/A	NO	INCONCLUSIVE	INCONCLUSIVE
Live Finger	NO	NO	N/A	YES

Fig. 11 Comparison chart for materials tested and results

Based on the research experiments conducted, the results provided sufficient data to support the proposed framework. In regards to previous biometric hacking methods, they were not simple to replicate. However, with enough practice, it can be done quite efficiently. Law enforcement material was shown to efficiently work as long as moisture was present. This is also dependent on the type of biometric scanner tested. In reference to reliability, it is apparent that biometric security alone is not as dependable as most people would think. Additionally, even though a fingerprint on file would be encrypted, if suspects were to practice fingerprint lifting it could compromise an array of security risks. On a positive note, the time it takes to prepare and execute such a hack would in fact provide sufficient time for a victim to erase their profile remotely as long as discovery is within a timely manner.

7. Future Work

As for future work, there are several things on the agenda. For starters, it would be ideal to refine circuit board etching techniques to examine how fast and accurate one could be made for a good solid mold. In the future, other biometric fingerprint readers should be tested as well. After establishing a solid foundation in creating artificial fingerprints that work well on different scanners, it would be essential to experiment with the second part of the proposed research; a biometric cell phone charger/dongle with a solid state relay. This would of course require additional hardware and some software programming on both ends. If successful, it could be the ideal solution to deter theft of mobile devices.

8. Conclusion

Biometric authentication standards should be implemented to prevent intrusions and theft against mobile cellular devices. To protect these important assets, a system other than PIN or password verification must be used because cell phones are lost or stolen on a daily basis. As we can see from the research above, biometric authentication is a better alternative although must be combined with other technology to create better security. Overall, the majority of faces, voices, and fingerprints are not duplicated unless replicated. The only negative aspect to biological and physiological identification is that biometric patterns cannot be revoked. Meaning, a biological key cannot be changed or altered. If a security system containing biometric keys was breached, identity theft and other identity crimes could occur.

As we saw throughout different independent processes, replications of faces, voices, and fingerprints can be used to obtain authorization illegally. To establish a fail-safe, there must be a system that combines biometrics with hardware keys. In other words, if a cell phone is only protected by biometrics, it can still be resold and used once it is wiped clean. Some independent business owners even like to take cell phones and flash them under another provider to access a market that is not typically available. This research concludes that by incorporating biometrics into a device while establishing a key/lock system (cell phone and charger), theft and intrusion of cell phones would be discouraged. Furthermore, it is important to note that this application can be utilized for any device that requires power. So essentially, if the equipment is separated from its power source and another power source cannot be duplicated without a key or hardware security device, the equipment will be useless.

9. Acknowledgments

The Author thanks Liza Phillips, an expert in fingerprint development and identification, for her assistance with the experiments conducted in this research study. Additionally, L. Phillips was able to provide the author with very useful resources regarding fingerprint information. The author would also like to thank Dr. Lei Chen for his guidance and support.

References

[1] M.O. Derawi, C. Nickel, P. Bours, and C. Busch, “Unobtrusive User-Authentication on Mobile Phones Using Biometric Gait Recognition,” *Electronics & Communication Engineering Journal,* pp. 306-311, Oct. 2010.

[2] M. Tanviruzzaman, S.I. Ahamed, C.S. Hasan, and C. O’brien, “ePet: When Cellular Phone Learns to Recognize Its Owner,” *Communications of ACM,* pp. 13-17, Nov. 2009.

[3] Y. Ijiri, M. Sakuragi, and S. Lao, “Security Management for Mobile Devices by Face Recognition,” *Electronics & Communication Engineering Journal*, pp. 49-55, May 2006.

[4] H.A. Shabeer and P. Suganthi, “Mobile Phones Security Using Biometrics,” *Electronics & Communication Engineering Journal*, pp. 270-272, Dec. 2007.

[5] G.G. Rivera, J. Garrido, R. Ribalda, and A. Castro, “A Mobile Biometric System-on-Token System for Signing Digital Transactions,” *Electronics & Communication Engineering Journal,* pp. 13-19, Mar. 2010.

[6] S. Liu, “Anti-counterfeit system based on mobile phone QR code and fingerprint,” *Electronics & Communication Engineering Journal*, pp. 236-240, Aug. 2010.

[7] H. Manabe, R. Sasaki, Y. Yamakawa, and T. Sasamoto, “Security Evaluation of Biometrics Authentication,” *Electronics & Communication Engineering Journal*, pp. 34-39, Sep. 2009.

[8] E. Syta, S. Kurkovsky, and B. Casano, “RFID-based Authentication Middleware for Mobile Devices,” *Electronics & Communication Engineering Journal,* pp. 1-10, Jan. 2010.

[9] R.J. Hulsebosch, and P.W.G. Ebben, “Enhancing Face Recognition with Location Information,” *Electronics & Communication Engineering Journal,* pp. 397-403, Mar. 2008.

[10] S. Kopsidas, D. Zisiadis, and L. Tassiulas, “Voice Interactive Personalized Security (VoIPSEC) protocol: Fortify Internet telephony by providing end-to-end security through inbound key exchange and biometric verification, *Electronics & Communication Engineering Journal,* pp. 1-10, Nov. 2006.

[11] I.J. Jozwiak, and K. Marczak, “A Hardware-Based Software Protection Systems – Analysis of Security Dongles with Time Meters,” *Electronics & Communication Engineering Journal,* pp. 254-261, Jun. 2007.

[12] R. Pappu, S.L. Garfinkel, and A. Juels, “RFID Privacy: An Overview of Problems and Proposed Solutions,” *Electronics & Communication Engineering Journal,* pp. 34-43, May 2005.