Securing Sensitive Data Stored on Smartphones

Using Face Recognition to Unlock Mobile Devices

Mark Wilson
Department of Computer Science
Sam Houston State University
Huntsville, TX 77341
mrw004@shsu.edu

Lei Chen
Department of Computer Science
Sam Houston State University
Huntsville, TX 77341
lxc008@shsu.edu

Abstract – Smartphones and tablets have become the new staple of the business and commercial industries, allowing employees to complete necessary tasks without requiring them to be confined to an office. However, with this mobility it is required that employees using these devices remain cautious to secure the sensitive data that is stored on their smartphones. To better aid those employees that use smartphones to complete their daily tasks at work, it is imperative to develop the best security features possible in order to safeguard the data they carry. This paper presents security features that are already being employed to lock smartphones, and why they are weak in comparison to biometric security features. Biometric features will be outlined, specifically face recognition, and how it could be used to secure sensitive data stored on a smartphone.

Keywords: Smartphone, Biometric, Face Recognition, Security

1 Introduction

Due to the overwhelming increase in popularity of smartphones and other mobile devices being used in commercial business, industry, and the classroom alike, strong security measures must be in place to protect the sensitive data stored on those devices [3][10][12]. The smartphone, in particular, has boomed in the business world because it allows for employers and employees to complete more complex tasks in a more efficient manner. These devices empower each user with the ability to immediately contact their employer via a company website, email, or text message and increase productivity by improving communication by sending and receiving data in real-time. Both the options to retrieve available company data and communicate instantly with other employees allow for more informed decisions to be made and for productions to be streamlined [3].

Smartphones are imperative to business management and for employees to properly maintain their designated workloads while away from the office [1]. The primary method of securing all of the data stored on one's smartphone is employing a strong password. A password is a secret word or string of characters that is used as authentication to prove identity or to gain access to a particular resource [10]. Passwords are able to serve as an entry point to aspects of the user's everyday personal life, along with his professional life, including: logging into a computer, checking emails from a server, transferring funds, shopping online, accessing programs and databases, and even composing or reading work-related documents. Due to the potential negative impact of a compromised password, it is crucial that a new technique to unlock smartphones be developed in order to keep the contents of that smartphone protected from unauthorized users. As even more smartphones are introduced into both the workforce and personal lives of users, smartphones will need to be personalized through biometric methods in order to safeguard against physical intrusion.

This paper will be structured as follows. In Section 2, passwords, screen locks, and conventional methods to secure smartphones will be discussed along with a brief introduction of biometric security measures. Section 3 will outline face recognition and two of the most commonly cited issues that make face recognition unreliable. Section 4 discusses how face recognition could be used to best protect a smartphone using hardware that is already available in most modern mobile devices. Section 5 draws conclusions and Section 6 proposes future research in this field.

2 Background

2.1 Passwords and Screen Lock

The most popular method of securing data employed on modern smartphones is the screen lock. Locking the screen essentially blocks all access to the smartphone unless some type of word, code, or pattern is entered to unlock the smartphone's feature and data. The use of passwords and pass codes has remained the most popular among smartphones, but are likely the weakest form of security. Password strength can be measured by the complexity of the password itself, using such measures as: length of the word or string of characters, use of upper and lower case, inclusion of numbers and symbols, and use of dictionary words. Personal information is also often used as a security measure, using a spouse's name or birthday as a password, for example [10].

Employing a password or pass code to unlock a smartphone is a weak method of security for a number of reasons. When setting a password on many websites, the site will prompt the user for a password and gauge the strength of that password, often requiring a certain number of letters, numbers, special characters ($, %, &, #), etc. [10][13]. Unfortunately, this type of password strength gauge is not a common feature among smartphones; those smartphones with supported apps to measure the strength of a password are generally third party applications and cost an additional fee to download. This may leave a novice user with a weak password and unsecured device. Furthermore, the smartphones that use a password or pass code to unlock the screen lock generally only require a four-digit number, providing a scant ten thousand possibilities. Though many smartphone pass codes allow for sixteen-digit numbers, the majority of users do not employ that increased security due to lack of convenience. Convenience is one of the top reasons that an actual password is not used to unlock a smartphone. Having to input a word using either an onscreen keyboard or a QWERTY keyboard each time the user wishes to use their device may prove frustrating and unrealistic depending upon the length of the word. Finally, a strong method of unlocking a smartphone, introduced by Android, requires the user only to swipe a pattern across a three by three square of dots. This method provides strong security because it offers a multitude of different combinations, and remains simple and convenient all while looking aesthetically pleasing.

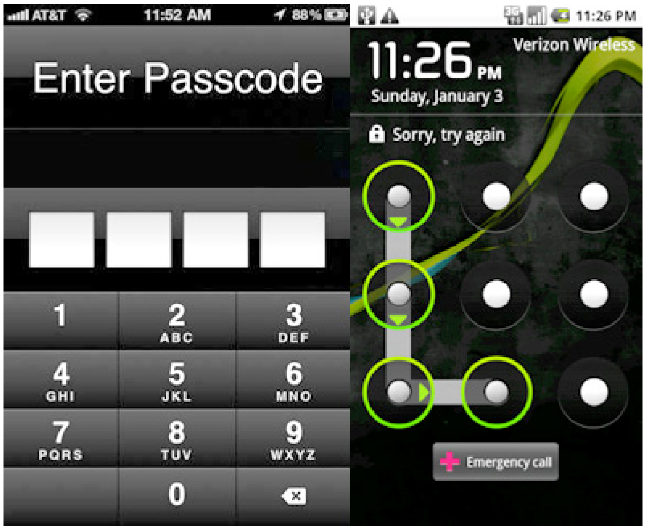

Figure 1. Examples of pass code and pattern security methods. Apple iPhone pass code (left) and Android security pattern (right)

Each of these methods protects a user's smartphone to varying degrees, but it is important to evaluate not only the technical merit of password combinations, but the physical security as well. Due to the majority of today's smartphones having touch screens that require user interaction to access data, regardless of the length of a pass code or the complexity of a pattern, the screen itself can give an intruder the solution to unlock the device. The residues and oils from a user's fingertips are naturally transferred to the smartphone's touch screen, especially those areas of the screen that are touched frequently (password, pass codes, and pattern swipes). It has been discovered that photographing a smartphone's touch screen and adjusting the contrast can reveal the user's pass code or pattern [7].

2.2 Different Types of Biometric Methods

Due to passwords being the weakest component of any important security system, it is necessary to attempt to fashion security in such a way that only authorized users are able to access restricted data [13]. Biometrics is the science and technology used to uniquely identify individuals based on their personal traits. Biometric security methods personalize access codes to ensure that only recognized users are able to view or modify sensitive data. This allows for a much stronger security scheme because access to information is based upon who a user is, rather than what that user has or remembers [9].

A particular biometric security scheme that would work well for securing smartphones is keystroke biometrics on an onscreen number pad. This method would not only require that the pass code be correct, but could also identify the user by typing rhythms that are compiled from the user's own style of typing [6]. Over time the smartphone itself would evaluate how the user inputs a pass code by compiling timestamps of touch and release of each digit on the screen. This method would be able to detect minor differences in habits such as using the index finger to enter a pass code versus the thumb. Upon detecting such a difference, this biometric method may determine that the person inputting the pass code is not the authorized user of the smartphone and additional security procedures could be deployed.

Voice recognition is another biometric security method that would readily apply to smartphones. This is a very plausible alternative to the standard pass code because the smartphone itself is able to offer all necessary hardware without having to attach external devices to properly capture the user's voice. Upon setting up the smartphone account the user could record a pass phrase that the smartphone would then compare and match to gain access to data in the future. This is a secure alternative to today's popular methods because a pass phrase could be known to others without risk of the smartphone being compromised because though the pass phrase could be duplicated, the voice could not [9].

3 Security through Face Recognition

Obviously the most secure way to protect any important data is to employ a security measure with millions of possible combinations. Depending upon the length of the password being typed, or the complexity of the security pattern being swiped, those millions of possibilities may be achieved. However, in order to truly personalize the smartphone and secure it, the biometric method of face recognition should be employed. Face recognition security measures have improved exponentially over the past decade, but two particular factors are generally cited as a hardship: alignment and illumination [2][8][11]. Though these two factors present difficulty for many face recognition applications, both would be easily solved when applied to smartphone screen lock security.

3.1 Face Alignment

Face alignment is an extremely important factor when employing any face recognition security measure because human faces have so many variations and viewing angles. This issue is most notable in unmonitored video surveillance in which face recognition software must analyze a dynamic image and match that image to a known face. Due to constant motion of a person's body, poor resolution, side-views and profiles, and changes in appearance such as facial hair, sunglasses, etc., the recognition device may provide false negatives or false positives when matching an identity with a face.

Face recognition is dramatically improved when faces are analyzed with known parameters, including: fixed distance, centered in front of the camera or scanner, known expression, eyes open, and non-moving [5][11]. Naturally, images such as mug shots or passport photos in which these parameters are strictly controlled offer the highest accuracy of face recognition with the actual identity of a particular person.

Facial alignment is an easily solved problem on the modern smartphone. When entering the pass code or security pattern, the user generally looks at the screen and touches the appropriate places to unlock the smartphone. Many of today's smartphones are installed with forward-facing cameras to allow for video conferencing; this same camera could be used to capture an image of the user's face for recognition purposes. By using the forward-facing camera, the user would be able to see himself on the screen and guarantee the image was centered for proper recognition. The image would also be taken from a fixed distance (arm's length, or shorter) that would be approximately the same each time the user unlocked his smartphone.

3.2 Face Illumination

Similar to the alignment of the user's face to ensure proper recognition, illuminating the face is also necessary for an accurate result [11]. Depending upon the location and the model used, a sufficient amount of light may not be available to collect an image that can be used for face recognition. Often used in video, night vision or infrared settings may allow for a suitable image to be collected to accurately identify a person's face. However, due to the high contrast of both methods, they are not considered reliable.

Obtaining proper and consistent exposure ensures that details of the user's face are captured and can be analyzed accurately. Research shows that multiple lighting sources on a flat, lighted background, similar to the standard studio photography lighting format, produce the best results that can be most accurately analyzed [11]. This setup is unrealistic in reality when dealing with face recognition as a security measure, but would apply if attempting to identify a person from an archived digital image taken in a studio environment.

Few smartphones and mobile devices on the market today feature a forward-facing flash to accompany the forward-facing camera, but by either installing a low-level diffused flash or a swiveling flash to the smartphone, a consistent amount of illumination could be provided to accurately analyze the user's face. This provides the smartphone itself a means of illumination so users would not have to depend on ambient light sources that may not provide the amount of light necessary to confirm their face.

4 Face Recognition on Smartphones

Because business professionals and personal users alike store so many increasingly sensitive items on their mobile devices, it is important to secure those devices with the strongest method possible. By deploying a face recognition biometric security method to smartphones and other mobile devices users can be confident that data remain secure. The face recognition software would be used to unlock a screen-locked mobile device to prevent any unauthorized users from gaining access to that device.

4.1 Unlocking Smartphones With Only the User's Face

To employ the biometric face recognition software to secure smartphones and mobile devices, the opening screen that typically requests the user's password or security pattern would be replaced with a blank screen with a large crosshair. The user would activate the front-facing camera by touching an onscreen button titled, "push to unlock." Once the camera is activated, the user would hold his smartphone in front of his face at a distance to properly align his face within the oval of the crosshair. The face should be positioned in such a way that the vertical line of the crosshair runs down the bridge of the user's nose and the horizontal line of the crosshair would run through the user's eyes.

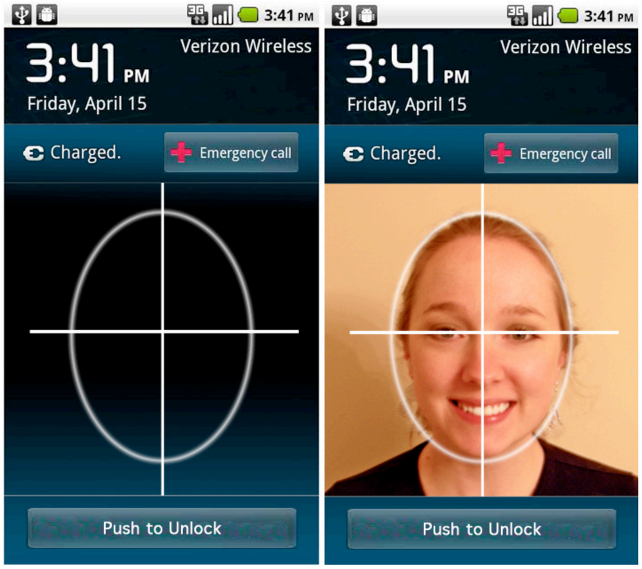

Figure 2. Example of the face capture crosshair (left) and proper face positioning in the crosshair (right)

By properly positioning the user's face in the crosshair, the common problem of face alignment would be corrected because a consistent image of the face would be taken each time. In order to center the user's face within the oval and the eyes along the horizontal line, the smartphone would capture an image that had extremely similar proportions each time. This would solve the obvious problems of side-views and profiles, and the distance from where the image was taken in relation to the camera.

For the business professional, who uses his smartphone most during daylight hours and inside of office buildings, etc., ambient light would not likely create an illumination problem. However, for the common user that does use his smartphone at various times of the day and direct ambient light was not available, a flash from the smartphone itself would be extremely helpful in order to capture an image that was bright enough to analyze. It is recommended that any flash used for this security technique either be diffused or set to a lesser power than the usual flash for a camera phone. This would both conserve the smartphone's battery life and allow for the image to capture facial detail and not overexpose the image.

After capturing the user's image, the smartphone would analyze it and compare it to a previous image taken to verify that it is the same authorized user. The comparison method could be performed using two different methods; the captured image could be compared to an image of the designated user upon initially setting up the security measure on his smartphone, or images of successful attempts to unlock his smartphone would be saved and used for comparison. The latter option would compare each subsequent captured image to a previously authorized image allowing the user's images to somewhat evolve and change slightly over time. This option would allow for minor facial changes, such as: five o'clock shadow, healing injuries, and possibly conservative haircuts. This would also allow for the smartphone to only save one captured image at a time, reducing the amount of hard drive space necessary to run the software.

In the event a dramatic facial change, such as: plastic surgery, new injury, shaving facial hair, etc., along with possible error in the software, it is important that a secondary security measure be available until a new image of the authorized user be captured for comparison. However, it is stressed that the secondary security measure be as strong as possible and not to simply rely on the biometric technology. Users often create a weaker password to secure their data when they believe they are being protected by two or more security methods [13].

Touching the "push to unlock" button a second time would capture an image. Upon comparing and verifying the captured image to the saved image of the authorized user, the smartphone would be unlocked and access would be granted as usual. This level of security is neither needed nor intended for the common user, but would benefit business professionals, college professors, government employees, and tech enthusiasts alike. With the proper speed and resources, taking a picture of one's self to unlock a smartphone may prove no more time consuming than entering a password or swiping a pattern.

5 Conclusion

This paper proposed a new method of safeguarding sensitive data stored on a smartphone or mobile device using face recognition software. The popularity of smartphone and other mobile devices have increased tremendously over the past decade, and society is finding a growing number of people using those devices. Depending upon the occupation of the user, be it corporate businessman, government employee, or even student, each store their own types and amounts of sensitive data on their devices. The screen lock is the first line of defense against unauthorized users accessing other's devices, but unfortunately, the average user has a weak or predictable password or pass code that would fail to safeguard one's smartphone. Presented in this paper is not a new method of face recognition or biometrics, but a new way to employ face recognition to secure technology that is becoming exponentially more prevalent in modern society. By using a biometric technology to secure smartphones, the smartphone itself is trained to react strictly to the user and may be considered impervious to break-in.

6 Future Work

Future work for this security model will include the development of the interface to both iOS and Android platforms. An extensive amount of time will be budgeted to integrate a face recognition software into the smartphone OS that will provide both speed and user-friendliness while performing accurately and securely. Smartphone hardware will be evaluated to determine the maximum efficiency to power a camera flash, store captured facial images, analyze and compare images, and how quickly these operations can be completed. Most importantly, once properly developed, surveys must be conducted to determine if the general public would use this security model. As quickly as smartphones are improving, if the technology is not able to perform at a rate similar to entering a pass code or pattern users may opt to employ a less secure method. Finally, research must be conducted to determine any major faults or holes in the security of a smartphone face recognition system, and how to repair those faults.

7 References

[1] F. Douglis, "As I Emerge From the Mobile Phone Dark Ages, I Look Around in Fear and Wonder," *IEEE Internet Computing*, vol. 14, pp. 4-6, Jul./Aug. 2010.

[2] M. Hanmandlu, et al., "An Experimental Study of Different Features for Face Recognition," in International Conference on Communication Systems and Network Technologies, 2011 IEEE. doi: 10.1109/CSNT.2011.121

[3] I. Henri and L. Aurelie, "Give Me a Mobile Phone, and I Will Work Harder! - Assessing the Value of Mobile Technologies in Organizations: An Exploratory Research," in International Conference on Mobile Business (ICMB), 2006 IEEE.

[4] G. Hua et al., "Introduction to the Special Section on Real-World Face Recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, no. 10, pp. 1921-1924, Oct. 2011.

[5] P. Li, et al., "Automatic Recognition of Smiling and Neutral Facial Expressions," in Digital Image Computing: Techniques and Applications, 2010 IEEE. doi: 10.1109/DICTA.2010.103

[6] R.A. Maxion and K.S. Killourhy, "Keystroke Biometrics with Number-Pad Input," in IEEE/IFIP International Conference on Dependable Systems & Networks (DSN), 2010 IEEE.

[7] C. Moor, "Your Finger Smudge Could Be Your Downfall" available at: http://www.talkandroid.com/10653-your-finger-smudge-could-be-your-downfall/#TtaFGkZ3yHI

[8] P.J. Phillips, "Improving Face Recognition Technology," in Computer, 2011 IEEE. available at: http://gala.cs.iastate.edu/coms510/references/IEEEComputer_FaceRecognition_March2011.pdf

[9] A. Pocovnicu, "Biometric Security for Cell Phones," *Informatica Economica*, vol. 13, no. 1, pp. 57-63, 2009.

[10] M.S. Vijaya et al., "Password Strength Prediction Using Supervised Machine Learning Techniques," in International Conference on Advances in Computing, Control, and Telecommunication Technologies, 2009 IEEE. doi: 10.1109/ACT.2009.105

[11] A. Wagner, et al., "Towards a Practical Face Recognition System: Robust Alignment and Illumination by Sparse Representation," *Trans. Pattern Anal. Mach. Intell.,* unpublished. doi: 10.1109/TPAMI.2011.112

[12] J. White and H. Turner, "Smartphone Computing in the Classroom," in Pervasive Computing, 2011 IEEE. available at: http://www.computer.org/pervasive

[13] H. Wimberly and L.M. Liebrock, "Using Fingerprint Authentication to Reduce System Security: An Empirical Study," in IEEE Symposium on Security and Privacy, 2011 IEEE. doi: 10.1109/SP.2011.35

[14] R. Xia et al., "Business Models in the Mobile Ecosystem," in Ninth International Conference on Mobile Business / Ninth Global Mobility Roundtable, 2010 IEEE. doi: 10.1109/ICMB-GMR.2010.30