Multi-Factor Authentication Fingerprinting Device Using Biometrics

An Independent Study
Submitted to the Faculty of
The Department of Electrical and Computer Engineering
Villanova University

By

Lauren Henderson

In Partial Fulfillment
Of the Requirements for the Degree of
Bachelor of Science in Computer Engineering

May 11, 2019

Acknowledgement

This research was funded by Villanova University’s Electrical and Computer Engineering Department and supervised by Dr. Richard Perry, Associate Professor.

Abstract

With the growth of ground-breaking technology exceeding new limits every day, it's important to be sure that the security of companies and individuals that utilize these advancements isn't threatened. In an age where some of the world's leading analytics are at our fingertips, literally, we always must keep in mind the threats that come along with it. Fingerprinting technology has widely been introduced and accepted as a safeguard to our most sensitive information. Fingerprinting sensors have been integrated into devices that range from everyday civilian use to military and government identification systems. However, currently these sensors lack the implementation of two-factor security; something that most every server, website, control system and access point currently uses as a counter to even the most advanced security threats. This paper will explore the benefits of a multi-factor security device that would combine a fingerprinting sensor and an LED pulse oximeter which would eliminate most if not all threats to fingerprinting authentication technology.

Contents

List of Figures

Chapter 1

Introduction

The chance of two fingerprints reading as the same is estimated at 1 in 50000 [1] making it an alluring form of identification and security. It has long been regarded as highly reliable and accurate, with uses expanding significantly in the past decades, ranging from inmate proof of identity in prisons to workforce management to the cell phones that millions of people carry in their pockets [13]. However, this extensive use of fingerprinting attracts major security risks. Methods to hack or break into systems that contain sensitive information are becoming increasingly easy with readily available advanced technologies that are growing at an immense rate. Criminals can recreate fingerprints using commonly found 2D or 3D printers [6] or hack into databases that store fingerprints to steal information. In a major security breach suffered by the Office of Personal Management, cyber criminals obtained the fingerprint information of 5.6 million people [3]. Because humans are not able to change their fingerprints, it is extremely difficult to reestablish confidence in the right person after a security breach. Furthermore, because fingerprints are physical (unlike passwords or key codes, which are mental), someone could be purposefully incapacitated or even killed to have their fingerprints used or removed. Current

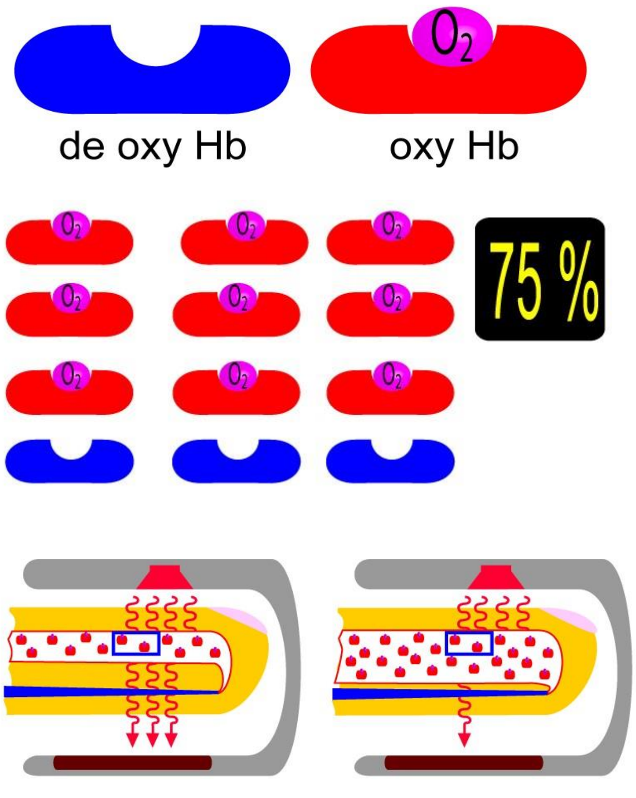

Fig. 1.1 Demonstration of how an LED pulse oximeter uses light to interpret oxygen levels in the blood [11]

fingerprinting devices are single-factor, meaning that the fingerprint is the only thing required as a proof of identity. If someone’s biometric information is stolen, there is no other way to verify that person’s identity using fingerprinting; a whole new method of identification will have to be enacted. In order to remedy this issue, a second or third factor of security could be implemented. Two-factor security is used widely: most social media now requires a password and a code sent to the user’s email or phone; card readers and ATMs often ask for a card and a zip code or a pin; account recovery requests the email associated with the account and the correct answers to security questions. Two factor authorization makes cyber-attacks less threatening because breaking passwords or codes are no longer sufficient for access, and it is unlikely an attacker would also be able to obtain the second factor of authorization [22].

LED pulse oximeters detect heart rate and oxygen saturation level in the blood. Using a light emitter with alternating red and infrared LEDs that shine through a reasonably translucent site with good blood flow allow the sensor to read characteristics of oxygenated and deoxygenated hemoglobin. Deoxygenated hemoglobin absorbs more red light and allows more infrared light to pass through, hence offering insight to the levels on oxygen in the blood [21]. Figure 1 illustrates how these LED pulse oximeters work.

This paper will demonstrate how an LED pulse oximeter can optimize the defense of fingerprinting scanners. Specifically, it will exhibit the advantages of an LED pulse oximeter over other secondary forms of security and how this approach addresses very specific, fundamental flaws in the current fingerprinting security systems. This method aims to address the following threats:

1) Fabrication of fingerprints using printers or other means.

2) Fingerprint extraction through manipulation or coercion.

3) Incapacitation of a user to gain access to scanners, including drugging, removing of digits and even killing.

4) Breaking or hacking into databases that maintain user access information.

Chapter 2

Literature Review

Fingerprinting biometrics are applied in airport security, government buildings, cars, blood banks, and even schools [29]. Considering the speed at which two-factor security is being implemented in today's devices and the range of applications for fingerprinting scanners, it is not unreasonable to assume that this is the first attempt at integrating a second form of security into a fingerprinting device. Some work in this field has been conducted with the purpose of patient identification and health analysis [8] [5] [15] [14]. The fingerprinting scanner works to identify the patient while the LED pulse oximeter aims to provide health information. These two devices do not work in conjunction as a security measure—they work for identification purposes.

Other modes of security have also been used to create multimodal biometric authentication devices, including the successful integration of iris scanners [19], user possession of an RFID [2] and even a digital signature [20]. None of these, however, aim to eliminate the risk of a person who is being coerced into relinquishing their biometric data; if a person can be convinced or forced to provide their fingerprint, it is reasonable to assume they can also be force to scan their eyes, produce an RFID badge or sign a keypad.

Some other proposals suggest integrating an LED oximeter and fingerprinting sensor for the same purposes suggested here. US patent US9349035B1 [9] describes a multi-factor system that integrates a fingerprinting sensor, a touchscreen and an LED pulse oximeter together to offer staged levels of authorization. The resource or application that is being requested is evaluated on a scale of importance as deemed by the algorithms in the controller. The level of importance determines the number of factors needed to authenticate the user. Importance in this system is usually determined by the amount of personal identifiable information (PII) the resource would yield if access is granted. For example, access to a social media account or a game might require a single factor of authentication, while access to a phone or a bank account will require multi-level, utilizing up to all three sensors. That proposal, however, does not use an LED pulse oximeter specifically for the purpose of authentication. In fact, the paper explored the use of many different biometric sensors in conjunction with a finger-printer. What the paper is really proposing is simply the idea of escalating security based on the resources being requested.

Other factors of multifactor authentication used in conjunction with a fingerprinting sensor include spoof detection module using pixel gray level average and the variance of pixels corresponding to a fingerprint ridge and valley, density of sweat pores, density streaks and other metrics [23]. That method simply analyzes two different parts of the fingerprint itself, which is not helpful if the fingerprint is being spoofed.

Chapter 3

Methodology

A fingerprinting-LED pulse oximeter multi-factor security device plays on the idea that a user must have a valid fingerprint pulse, and blood oxygen level in order to gain access to a system. Fabricated fingerprints using printers or other means and severed digits would fail to meet these requirements due to lack of pulse and hemoglobin in actual flowing blood. In order to address the other aforementioned security threats, algorithms have been developed and implemented through the software that is run on a controller to prevent unauthorized access. According the ALERRT Center at Texas State University, there are certain conditions that a human meets when experiencing extreme stress [28]. Researchers refer to these conditions in terms of stress level with the following effects on heartrate:

- Condition white: normal resting condition where daily activities have little to no adverse effects on the body. Heartrate around 60 beats per minute.
- Condition yellow: a heighted state of alert where the body recognizes or anticipates a form of stress. Heartrate approximately at 90 beats per minute.
- Condition red: an attack is imminent or in progress. Motor skills begin to deteriorate, and adrenaline makes the body faster, stronger and more sturdy.

  Heartrate averages 120 beats per minute.
- Condition grey: situation is becoming overwhelming for the body to handle with cognitive processing beginning to deteriorate. Heartrate around 150 beats per minute.
- Condition black: system and sensory overload. Environment is beyond overwhelming. Heartrate is at or above 175 beats per minute.

When introduced to a stressful environment such as a hostage situation, adrenaline is released into the blood stream, causing increased heartrate and the contraction of blood vessels to increase blood flow in the body [30]. Adrenaline appreciably raises oxygen consumption, CO_2 production and lactic acid elimination

[17]. The purpose of pulse oximetry is to check how well your heart is pumping oxygen through your body [26]; when adrenaline is flowing through the bloodstream, the heart's ability to pump oxygen is compromised. The heightened consumption of oxygen affects the hemoglobin saturation levels in the blood, which an LED pulse oximeter can read. Using the heartrate specifications above, plus the parameter for what is considered "normal" blood oxygen values [12], algorithms can be placed utilizing the data pulled from the LED pulse oximeter to authenticate a user.

Elevated heartrate to the point of condition red, grey or black indicates a person under duress i.e. in a stressful situation with adrenaline causing increased blood flow, possible hyperventilation and raised heartrate. The same logic could be applied for heartrate and blood oxygen levels that are too low. When someone is asleep or under the influence of incapacitating drugs, breathing rates lower and the heart slows, introducing the conditions that border and exceed the range of normal, stable vitals [24] [27] [18] [25]. These algorithms will further defend fingerprinting scanners against users who are being forced to use their fingerprints and incapacitated persons through means of force or drugs. This flow of authentication can be seen in *Figure 2*.

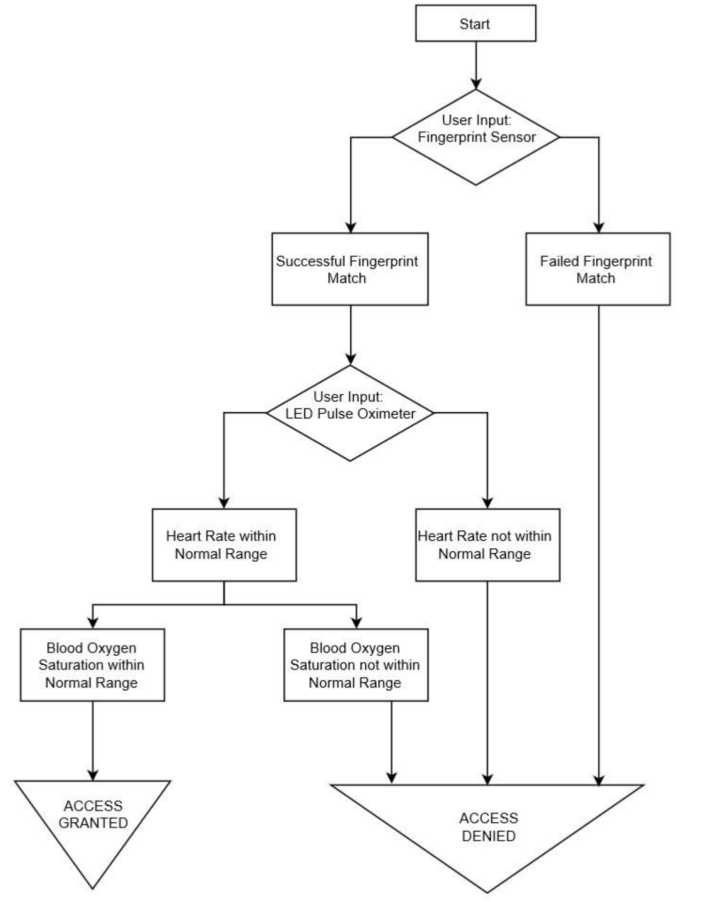
Start
User Input:
Fingerprint Sensor
Successful Fingerprint Match
Failed Fingerprint Match
User Input:
LED Pulse Oximeter
Heart Rate within Normal Range
Heart Rate not within Normal Range
Blood Oxygen Saturation within Normal Range
Blood Oxygen Saturation not within Normal Range
ACCESS GRANTED
ACCESS DENIED

Fig. 2.1 Flowchart of authentication algorithm

For the purpose of experimentation, a ZhianTec ZFM206SA fingerprinting sensor and a CONTEC CMS50D+ LED Pulse Oximeter were used together to test the algorithms presented here. These sensors are not top of their line nor do they have 100% efficiency, so first, they were tested to find their success rate for measurement. Out of 100 tests, a finger with a valid fingerprint enrolled was successfully accepted 90 times, putting the efficiency at 90% for the fingerprinting sensor. Alternatively, 100 out of 100 tests with an invalid fingerprint were not accepted. Using that metric, there is a 0% chance of a false positive. For the LED pulse oximeter, 95 out of 100 tests read accurate values, putting the efficiency at 95%. Taking both of those values into account, out of 100 tests using the algorithms described in this section, a person under normal conditions will successfully pass a security test 94 times. The 6 tests that failed did so because of sensor misreads. With better quality sensors that are closer to 99% or 100% efficiency, this success rate would be higher.

As for the security risk of cyber criminals breaking into databases that contain sensitive information, after implementing this second form of security, stealing sensitive information will mean nothing in terms of gaining access to a system. While this is a breach of confidentiality, it will not risk further loss of data that a stolen fingerprint would normally provide access to. With currently mainstreamed scanners, if there is a security breach, a cybercriminal can deceive a scanner using one of the stolen fingerprints, however, this two factor device will prevent against that using the methods presented here.

Chapter 4

Advantages

Instead of using an LED pulse oximeter, consider using something a user knows or something they have. A keyboard or a pin pad could have been integrated on a card or chip reader. However, considering that one of the major above-mentioned security risks is manipulation or coercion to gain the use of a victims digits, it is not unreasonable to assume that a victim could not also be manipulated into forfeiting their physical device, password or pin. These two categories of factors fail to prevent against such a threat.

Now, as opposed to an LED pulse oximeter, consider using a

different form of biometric security. Voice recognition or iris scanners could be introduced just as easily as an LED pulse oximeter, however no one of the other available biometric measures offer the level of analysis proposed. LED pulse oximeters are able to authenticate more than just the identity of a user; they are able to evaluate the state of the user using the projected algorithms. Using another form of biometrics still leaves the possibility of incapacitation, compulsion, fabrication and force. None of the above factors allow for the level of security and precision that the proposed device offers.

The primary focus of the devices listed in Section II is that of authentication rather than authorization; authentication being proof of identify while authorization decides if the person gaining access has permission to do so [16]; they focus on identification, not verification. Most of the applications previously mentioned are those of patient identification: the fingerprint sensor working to identify the patient and the LED pulse oximeter doubly working to evaluate health. Contrary to the device proposed in this paper, these devices do not protect the user against any security threat they may face.

Other devices mentioned that are more aligned with the purposes listed here, again, fall short of the range and scope presented here. Applications thereof are specific to mobile devices and gauge their security on number of user inputs (sensors/factors of authentication) rather than quality of input by the user. Additionally, other devices that use multifactor identification with fingerprinting devices, while they do eliminate some aforementioned security threats such as 3D or 2D printed fingerprints and the use of stolen fingerprints to break a system, they do not prevent against all of the vulnerabilities presented here. The device mentioned not only protects against more security threats, it has a wider application range than devices currently patented.

Fingerprinting technology has potential to be an efficient method of protecting sensitive information, but not if it cannot be secured with the utmost confidence. Everywhere fingerprinting scanners are currently used is a potential application for the proposed device. For example, smart phones, personal computers, USB flash drives, vehicles, padlocks, safes, lockers and doors. The application of biometrics in everyday life is expected to grow as manufacturers devise new ways to incorporate technology. Additionally, pulse oximeters are already incorporated into some everyday devices such as phones and fitness trackers to monitor heart and breathing rates [10]. Samsung's Galaxy Note8 already has a fingerprint scanner and an LED pulse oximeter integrated on-device. An application on the phone even evaluates stress level using the sensors and methods similar to those proposed here [7].

Chapter 5

Conclusion

Cybersecurity is an exponentially growing field with new innovative technologies being discovered every day. In order to ensure the success of these technologies, their security must also be ensured. Multi-factor security is a safe, easy way to make the most common to the most advanced technologies more secure as it is harder for cyber criminals to break into two-factor security systems rather than a single-factor ones [4]. As fingerprinting technology becomes a more widely accepted means of securing sensitive information, it’s important to protect against security risks early on so that they do not become a major issue when potential lives depend on the successful securing of information. This is what the proposed device aims to accomplish.

References

[1] "About Touch ID Security on IPhone and IPad." Apple Support. Apple, 02 Nov. 2015. Web. 7 Nov. 2016.

[2] Basilio-Ramirez, J., et al. “Multifactor Authentication System Based on Biometrics and Radio Frequency Identification.*” 2016 9th International Kharkiv Symposium on Physics and Engineering of Microwaves, Millimeter and Submillimeter Waves (MSMW)*, 11 Aug. 2016, doi:10.1109/MSMW.2016.7538169.

[3] Bolluyt, Jess. "Smartphone Fingerprint Scanners: Are They Secure?" The Cheat Sheet. N.p., 01 June 2016. Web. 6 Nov. 2016.

[4] Chipurici, Cristina. "Why You Should Start Using Two-Factor Authentication Now." Heimdal Security Blog. N.p., 29 Nov. 2016. Web. 25 Jan. 2017.

[5] Cronin, John, and Seth Melvin Cronin. *Pulse Oximetry and Contactless Patient Biometric Monitoring System.*

[6] Eddy, Max. "Here's How Hackers Steal Fingerprints From Your Phone." PCMAG. PC Magazine, 11 Aug. 2015. Web. 7 Nov. 2016.

[7] Evans, Sean. “Here's How the Samsung Galaxy Note8 Can Help Keep You Healthy.” *Men's Health*, 3 Nov. 2017, www.menshealth.com/health/a19541170/samsung-galaxynote8-review/.

[8] Garver, Gary Tschautscher, and Jayant Pathasarathy Minnetonka. *Sensor and System Providing Physiologic Data and Biometric Identification*. 12 Feb. 2009.

[9] Gerber, Stephen C., and Ronald B. Koo. *Multi-Factor Authentication Sensor for Providing Improved Identification*. 24 May 2016.

[10] Goodner, Stanley. “Finger Scanners: What They Are And Why They Are Gaining in Popularity .” *Lifewire*, 28 Dec. 2018, www.lifewire.com/understanding-finger-scanners-4150464.

[11] “How Pulse Oximeters Work Explained Simply.” *How Equipment Works*, www.howequipmentworks.com/pulse_oximeter/." Industries Using Biometric Fingerprint Software." M2SYS RSS2. M2SYS, n.d. Web. 6 Nov. 2016.

[12] “How to Interpret Pulse Oximeter Readings.” *Amperor USA*, www.amperordirect.com/pc/help-pulse-oximeter/z-interpretingresults.html.

[13] "Industries Using Biometric Fingerprint Software." M2SYS RSS2. M2SYS, n.d. Web. 6 Nov. 2016.

[14] Katarow, Frank. *Combination Fingerprint and Oximetry Device*. 4 Nov. 2003.

[15] Kayyali, Hani. *Medical Device and Method with Improved Biometric Verification*. 25 Mar. 2014.

[16] Khillar, Sagar. “Difference between Authentication and Authorization.” *Difference Between*, 30 Oct. 2017, www.differencebetween.net/technology/difference-betweenauthentication-and-authorization/.

[17] Lundholm, Lennart, and Nils Svedmyr. “Influence of Adrenaline on Blood Flow and Metabolism in the Human Forearm.” *Wiley Online Library*, Dec. 1965, onlinelibrary.wiley.com/doi/abs/10.1111/j.17481716.1965.tb04283.x.

[18] Menard, Amanda. “Effects of Illegal Drugs on the Heart .” *ACLS Training Center*, 3 Jan. 2019, www.acls.net/effects-ofdrugs.htm.

[19] Parkavi, R., et al. “Multimodal Biometrics for User Authentication.” *2017 11th International Conference on Intelligent Systems and Control (ISCO)*, 16 Feb. 2017, doi:10.1109/ISCO.2017.7856044.

[20] Pasenchuk, Viktor A., and Danil A. Volkov. “SignToLogin Cloud Service of Biometrie Two-Factor Authentication Using Mobile Devices.” *2016 17th International Conference of Young Specialists on Micro/Nanotechnologies and Electron Devices (EDM)*, 11 Aug. 2016, doi:10.1109/EDM.2016.7538717.

[21] “Pulse Oximeters.” Institute of Physics, 2012.

[22] Rouse, Margaret, and Michael Cobb. "What Is Two-factor Authentication (2FA)?" SearchSecurity. WhatIs.com, Dec. 2016. Web. 21 Jan. 2017.

[23] Russo, Anthony. *System for and Method of Securing Fingerprint Biometric Systems against Fake-Finger Spoofing*. 17 Mar. 2009.

[24] “Sleep Renewal Clinics Sleep Studies South Africa.” *Sleep Renewal*, Renewal Institute, www.sleeprenewal.co.za/oxygenlevels.

[25] Snow, J. “The Breathing And The Pulse Under The Influence Of Chloroform.” *Medical Journal*, vol. s3-3, no. 118, 6 Apr. 1855, pp. 313–318., doi:10.1136/bmj.s3-3.118.313.

[26] Stephens, Carissa. “Pulse Oximetry.” *Healthline*, 2 Aug. 2017, www.healthline.com/health/pulse-oximetry.

[27] “The Need For Supplemental Oxygen.” *UCSF Health*, UCSF Medical Center, www.ucsfhealth.org/education/supplemental_oxygen/the_need_for_supplemental_oxygen/#5.

[28] "Three Stages of Disaster Response." Avoid Deny Defend. ALERRT Center, n.d. Web. 5 Nov. 2016.

[29] Trader, John. “5 Ways Biometric Technology Is Used in Everyday Life.” *M2SYS Blog*, KernellO Identity, www.m2sys.com/blog/guest-blog-posts/5-ways-biometrictechnology-is-used-in-everyday-life/

[30] "What Does Adrenaline Do?" Hormone Health Network. Endocrine Society, n.d. Web. 5 Nov. 2016.