Two Factor Security Fingerprinting Device

Lauren A. Henderson and Dr. Richard Perry

Dept. Of Electrical and Computer Engineering, Villanova University

Acknowledgement: Research topic independently conceptualized, pursued and funded through the efforts of undergraduate researcher and faculty advisor.

Abstract

Fingerprinting technology has become a widely accepted method for security and identification purposes. Because of the uniqueness of the fingerprint, it has long been regarded as a highly reliable and accurate measure of identification. The rapid and extensive adoption of fingerprinting, however, makes it an easy target for cybercrime. In a security breach suffered by the Office of Personal Management in 2015, cybercriminals stole 5.6 million peoples' sensitive fingerprinting information. Because we are not able to change their fingerprints, it is extremely difficult to reestablish confidence in the right identity after having information stolen. Current fingerprinting devices do little to bar security breaches because they are single-factor, meaning that the fingerprint is the only thing required as a proof of identity. If someone's fingerprint is stolen, there is no other way to verify that person's identity. These are the issues that have been addressed in a two-year long student conceptualized research project funded by Villanova's Department of Electrical and Computer Engineering. A second factor of security has been integrated with an already existing fingerprint sensor, attempting to resolve most security threats to current fingerprinting technology.

Solution and the Second Factor

Two factor authorization reduces the likelihood of cyber-attacks significantly because obtaining a single factor like a password or code would be insufficient to break into a system. The challenge, then, was identifying a single second verification method that would accomplish the following:

- Not extractable through manipulation or coercion
- Provide precision equivalent to fingerprinting sensors
- Obstruct security breaches using fabricated fingerprints
- Detect when a someone is incapacitated

After researching and discarding the possibility of integrating a keyboard, a humidity sensor and a temperature sensor, the conclusive solution was found to be an LED pulse oximeter for detecting heart rate and oxygen saturation in the blood. Fake or removed fingerprints would be rejected because they have neither blood flow nor pulse. Additionally, according to research conducted by the ALERRT Center at Texas State University and the Endocrine Society, there is a correlation between stress, adrenaline and blood oxygen levels. If heartrate and saturation levels are too low, it may suggest that someone is unconscious—results due to shallow breathing and a resting state—whereas high heartrate and saturation levels may signal a person under duress, for example, being held at gunpoint, brought on by hyperventilation and elevated amounts of adrenaline. Blood oxygen levels cannot be fabricated or extracted so integrating an LED pulse oximeter would resolve most security obstacles threatening the success of fingerprinting as an authentication technology.

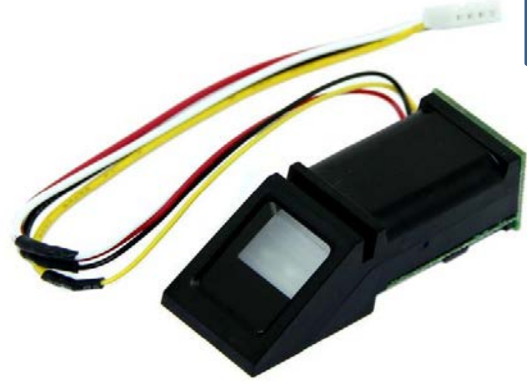


Figure 3: Fingerprinting Sensor (*Image by Seeed Studio*)

Hardware

The following hardware is being used in development:

- Raspberry Pi 3 Model B Single-Board Computer
- ZhianTec ZFM-20 Fingerprinting Sensor (*Figure 3*)
- MaxRefDes117#: Heart-rate and Pulse-Oximetry Monitor (*Figure 4*)
- Arduino Uno Rev3

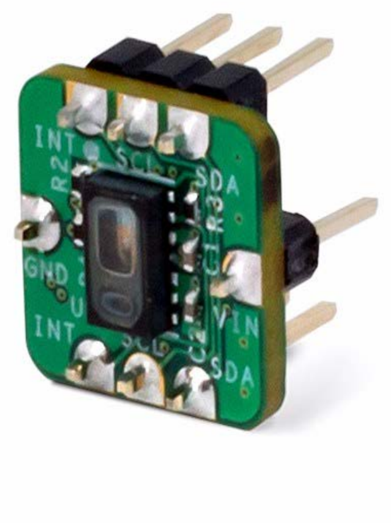
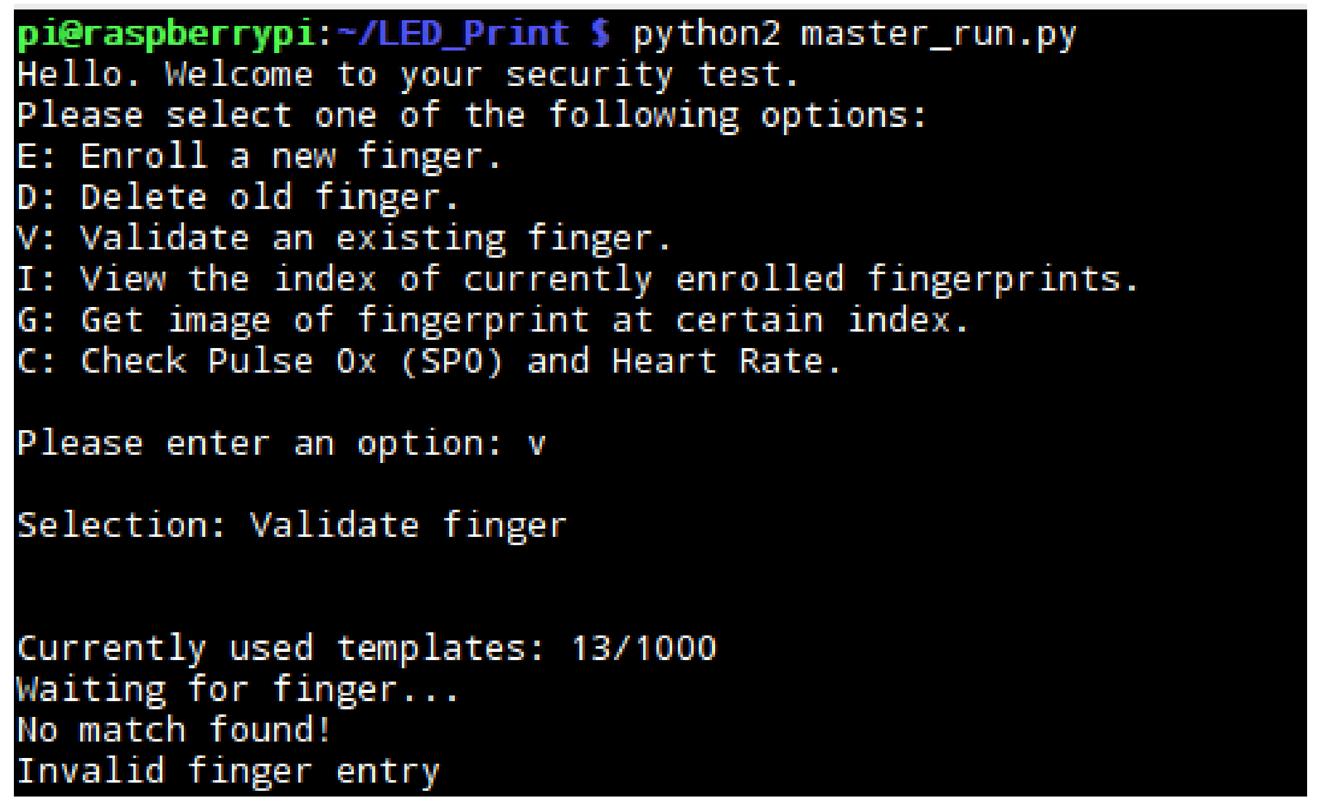


Figure 4: LED pulse oximeter integrated on-board. (*Image by Seeed Studio*)



```
pi@raspberrypi:~/LED_Print $ python2 master_run.py
Hello. Welcome to your security test.
Please select one of the following options:
E: Enroll a new finger.
D: Delete old finger.
V: Validate an existing finger.
I: View the index of currently enrolled fingerprints.
G: Get image of fingerprint at certain index.
C: Check Pulse Ox (SPO) and Heart Rate.

Please enter an option: v

Selection: Validate finger


Currently used templates: 13/1000
Waiting for finger...
No match found!
Invalid finger entry
```

Figure 5: Example output for invalid finger attempt

Security Risks

Those who wish to do so can reconstruct fingerprints using readily available 2D (*Figure 1*) or even 3D (*Figure 2*) printers. Because of the level of sensitivity on fingerprinting sensors, it is not unreasonable to believe that they can be breached using these methods. Additionally, the databases where fingerprints are stored can be attacked by cybercriminals. Because fingerprints are physical and not mental like a password or pin, in the extreme case, victims can be purposely incapacitated or even killed in order to subject their fingerprints to usage or removal.

Figure 1: 2D Printed Replicated Fingerprint

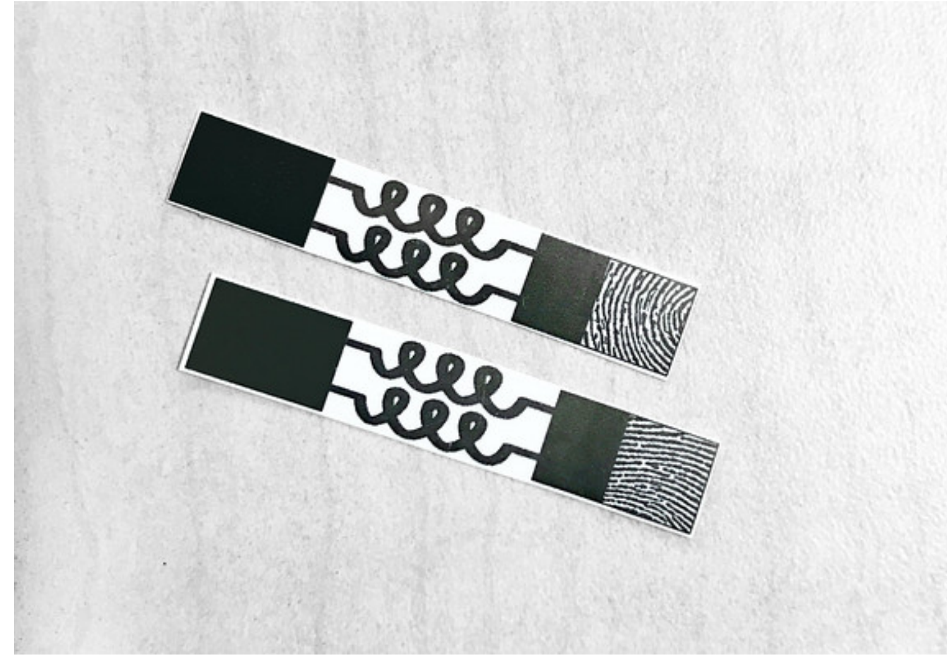
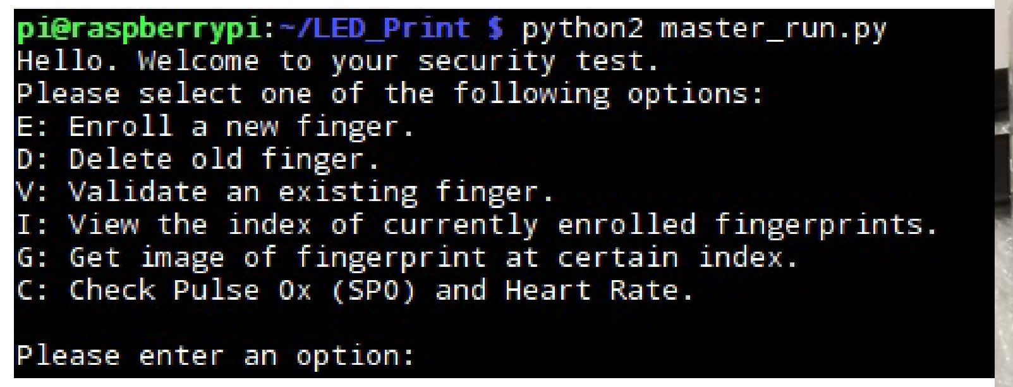


Figure 2: 3D Printed Fingerprint Used on a Scanning Device (*Image by Michigan State University*)

Challenges

There were many unforeseen obstacles elongating the research period to almost 2 years. The following are some challenges that hindered the progress of the project:

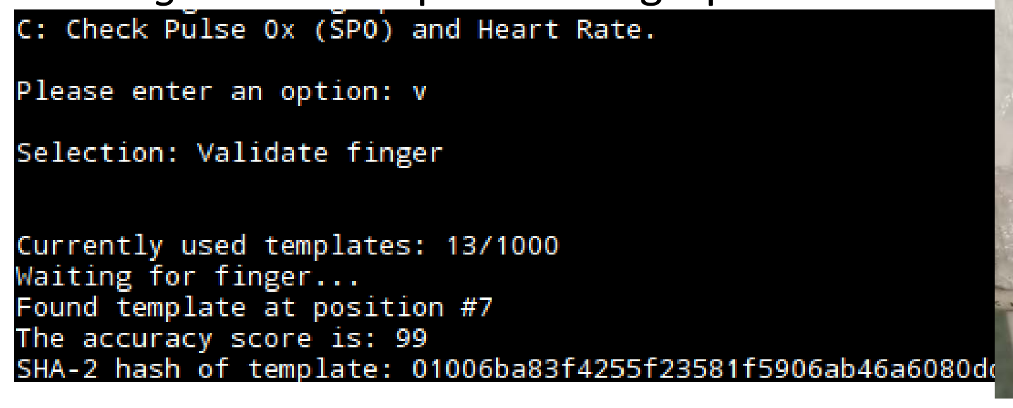
1. Some hardware was difficult to find or took a lot of time to get
2. A lot of the software that various hardware components used was not compatible on hardware that other components needed
3. LED pulse oximeters are normally sold fully integrated; availability for an LED pulse oximeter sensor (*Figure 4*) that was either extractable from the device or sold independently proved scarce
4. Various software packages, for example the package to interface with the fingerprinting sensor versus the LED sensor, were written in different languages so trying to find a way to run both cross-platform was a major issue
5. The LED sensor was made to be run off of an Arduino. A large portion of the project was focused on considering whether it would be more efficient to try and interface with the Arduino through the Raspberry Pi's serial ports or to try and convert the Arduino and helper C++ files into something that could be run on the Pi using I2C protocol



```
pi@raspberrypi:~/LED_Print $ python2 master_run.py
Hello. Welcome to your security test.
Please select one of the following options:
E: Enroll a new finger.
D: Delete old finger.
V: Validate an existing finger.
I: View the index of currently enrolled fingerprints.
G: Get image of fingerprint at certain index.
C: Check Pulse Ox (SPO) and Heart Rate.

Please enter an option:
```

Figure 6: Example of a Fingerprint Test

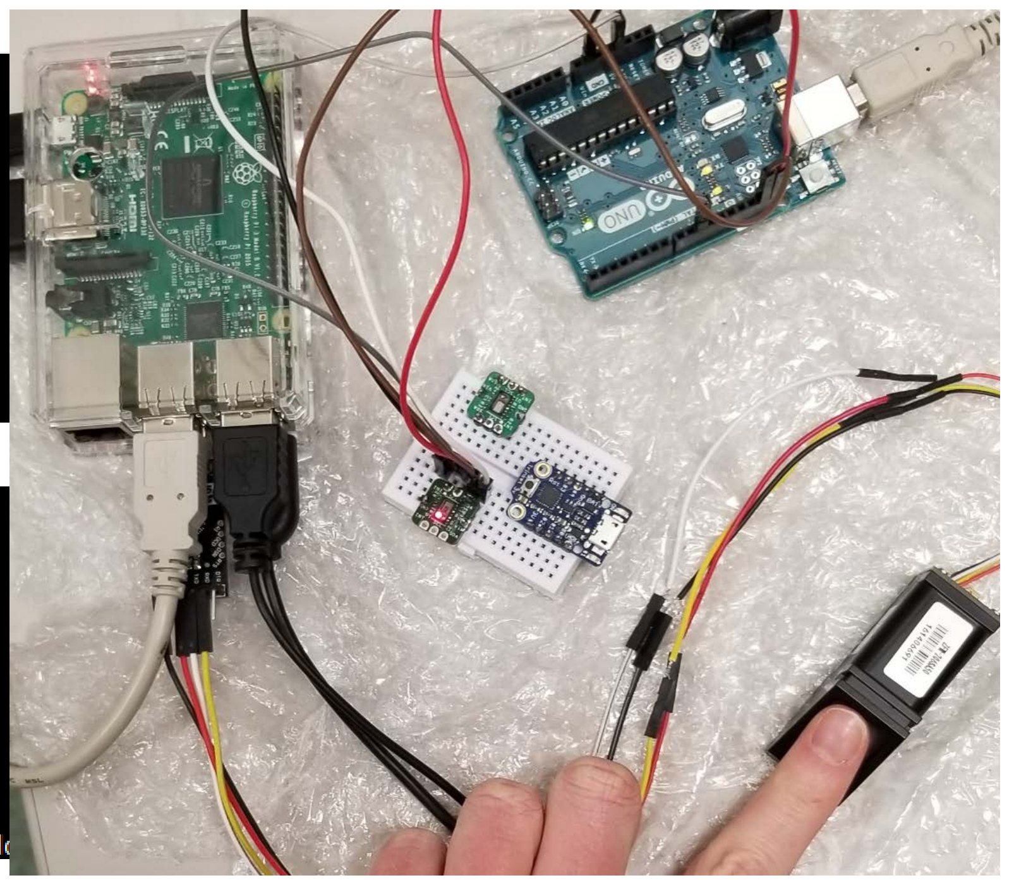


```
C: Check Pulse Ox (SPO) and Heart Rate.

Please enter an option: v

Selection: Validate finger


Currently used templates: 13/1000
Waiting for finger...
Found template at position #7
The accuracy score is: 99
SHA-2 hash of template: 01006ba83f4255f23581f5906ab46a6080dd
```



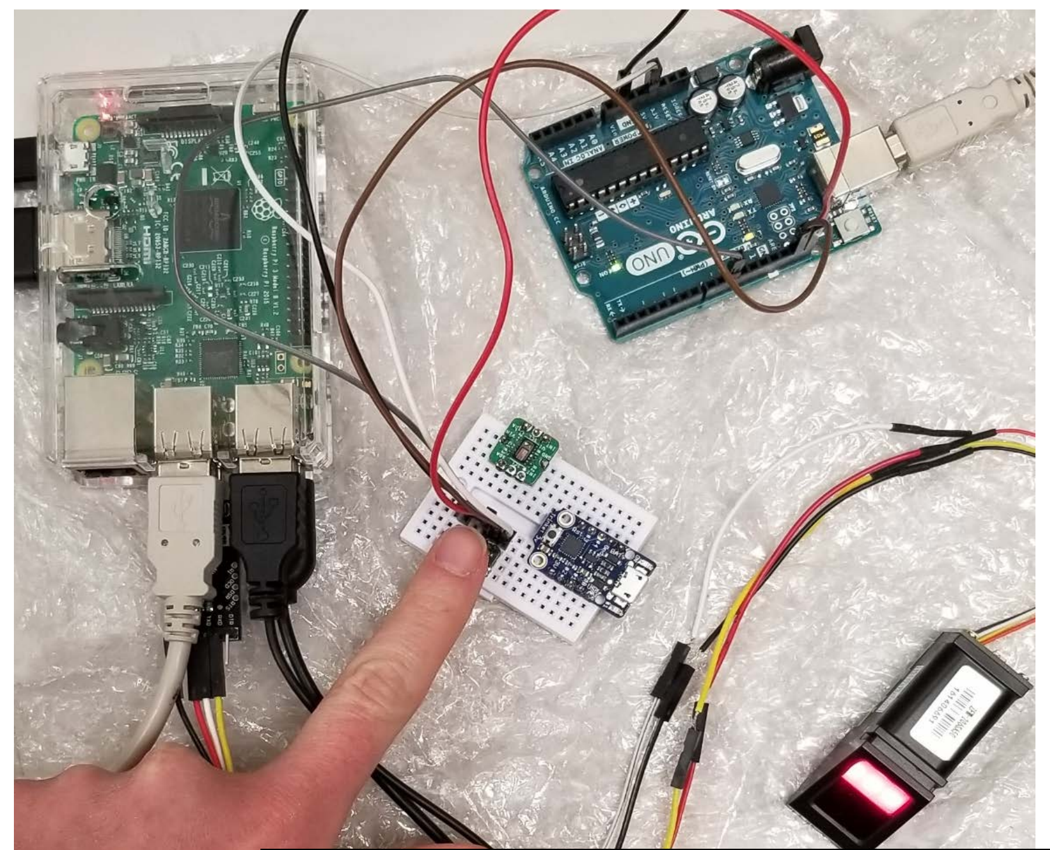
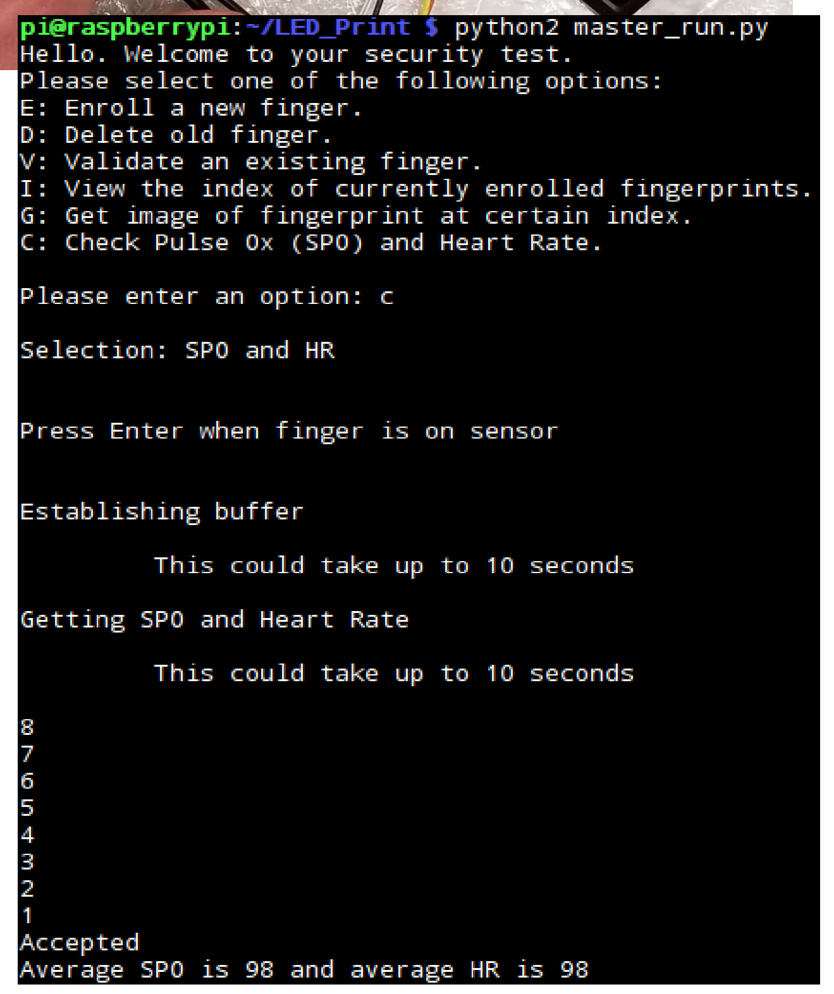


Figure 7: Example output a successful Pulse Ox reading



```
pi@raspberrypi:~/LED_Print $ python2 master_run.py
Hello. Welcome to your security test.
Please select one of the following options:
E: Enroll a new finger.
D: Delete old finger.
V: Validate an existing finger.
I: View the index of currently enrolled fingerprints.
G: Get image of fingerprint at certain index.
C: Check Pulse Ox (SPO) and Heart Rate.

Please enter an option: c

Selection: SPO and HR


Press Enter when finger is on sensor


Establishing buffer

        This could take up to 10 seconds

Getting SPO and Heart Rate

        This could take up to 10 seconds

8
7
6
5
4
3
2
1
Accepted
Average SPO is 98 and average HR is 98
```

Impact

Fingerprinting technology uses have expanded significantly in the past decades, ranging from inmate proof of identity in prisons to the cell phones that millions of people carry in their pockets. It is efficient method for protecting sensitive information, but not if it cannot be secured with the utmost confidence. Multiple factor identification has the potential to be used in conjunction with both biometric security processes such as eye scans and any security system that uses single factor security. Two factor security is safer and more secure as it is harder for hackers compromise both factors. The applications range from car doors, which can be designed to require a key and a fingerprint, to computer logins, which could utilize the camera for facial recognition in addition to a password. This includes systems that require physical security like padlocks and key-codes or passwords and passcodes on phones. This project is just the start to a whole field of research, one that is increasingly being called upon as technologies grow and breaches in security and cyber-attacks become more frequent.