# Biometric Security Applications: Secured USB Flash Storage Device

**Lance Aaron See, Computer Engineering**
Mentor: Dr. Meng-Lai Yin
Kellogg Honors College Capstone Project

## Abstract

Portable USB Flash Storage Devices of various sizes have become ubiquitous in numerous industries as a means of transferring and sharing data. However, multiple high profile company hackings have shown a fatal vulnerability in the USB. These devices are typically shared to multiple computers with little or no security protocols to ensure user security, leaving companies vulnerable to attack. Although there are existing software methods to limit the devices that a USB can connect to, these solutions are cumbersome and time consuming, as the security software on every USB capable system must be modified to accommodate the new USB storage device. Biometric security measures, such as finger print sensors can alleviate this issue whilst maintaining improved security. The method implemented in this project requires only a single fingerprint enrollment at the deployment of the USB, instead of multiple security modifications, thus this method is time-efficient. The USB will connect successfully only when a fingerprint match occurs, thus allowing only authorized users to access the data. This project will demonstrate the methods, troubleshooting and results of the implementation.

## System Design

A basic understanding of how USB Flash Storage Devices work was necessary to achieve the desired function. There are four pins in a typical USB 2.0 device: power, ground, and two data pins. By manipulating both the power and ground pins, the USB device can be made to turn on and off, thus successfully limiting access. The main system design is based on an Arduino Uno R3 microcontroller, which allows for digital manipulation of the power pins, as well as an Adafruit Fingerprint Sensor to register and test fingerprints. The fingerprint sensor utilizes two of the digital input pins to communicate with the Arduino for both pairing and regular usage. A small transistor based circuit along with a separate digital output pin from the Arduino creates a digitally controlled switch. A user first registers their fingerprints using the Arduino serial monitor, which stores an image of their fingerprint onto the sensor itself. When a user wishes to use the USB Flash Storage Device, the Arduino reads the fingerprint scanned and searches for matches in the sensor's database. If one is found, the Arduino provides 5V to the power pin of the USB, thus allowing access. If not, no voltage is supplied and the the USB remains off.

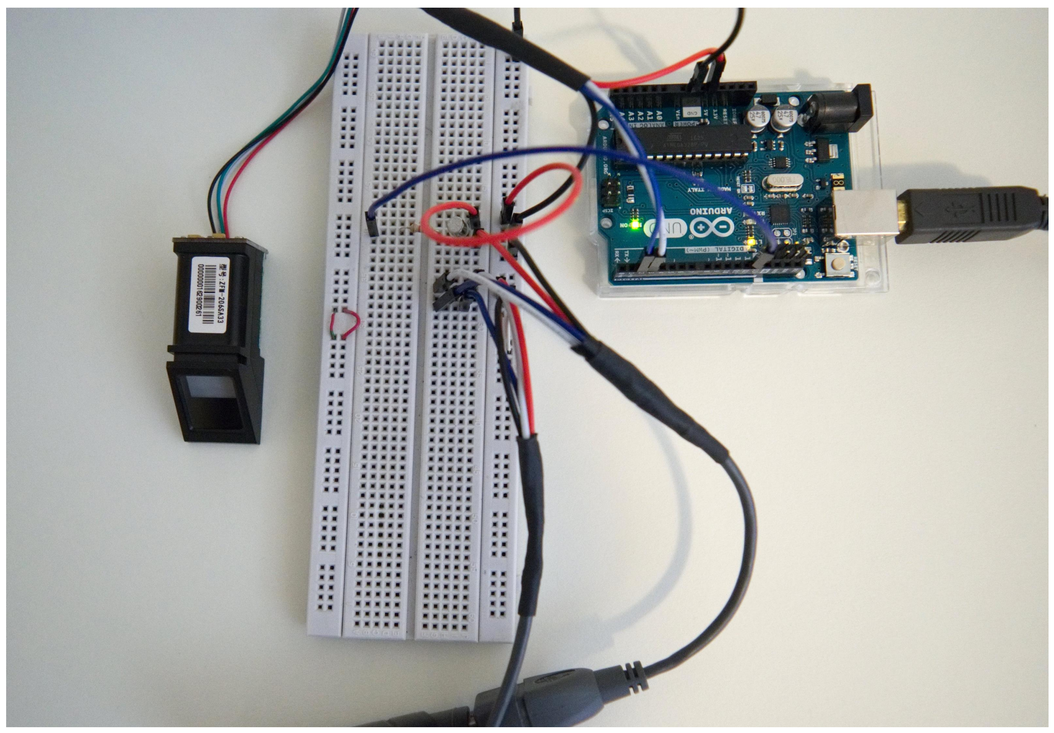

Fig. 1 - Hardware Design – System Overview

## Testing and Results

In order to test the design, the prototype shown in Figure 1 was created. By utilizing a stripped USB male and female connector, the circuit was easily wired and tested. To test the validity of this design, three different users were registered onto the fingerprint sensor by running the fingerprint enrollment code. On power up, the USB Flash Storage Device does not power on, while the fingerprint sensor flashes, indicating that it is ready to scan for fingerprints, as seen in Figure 2. Once a fingerprint is scanned, the fingerprint sensor is able to look for a match. On two of the subjects, matches were found within less than 1 second, and the USB Flash Drive was powered on by the circuit, as seen in Figure 3. However, in one case, one subject had a difficult time registering fingerprints and matching as a result of a lack of clear fingerprints. Due to the nature of the fingerprint reader, any users with damaged or unclear prints would be unable to register or use this device.

## Discussion

When designing this system, various issues were encountered. Initially, the USB Flash Storage Device was not able to power on, despite a match due to the power pass-through delivery issues of the Arduino. By utilizing the 5V supply pins directly from the host computer, this issue was resolved. In testing, a weakness in this system was uncovered, as people with damaged or unreadable fingerprints had difficulty registering their fingerprints. A possible solution would be to create a system with multiple biometric security sensors, such as an iris sensor, to function as an alternate registration system. Although this system is a proof of concept, the size of the device is much larger than a conventional USB Flash Storage Device. By utilizing a custom designed PCB that incorporates both the microcontroller and the storage device itself, the design can be condensed to a smaller size. In addition, the device is easily modified, as a prototype. Thus, the security measure can be easily circumvented. In future models, a secure enclosure can ensure that the device remains tamper-resistant.

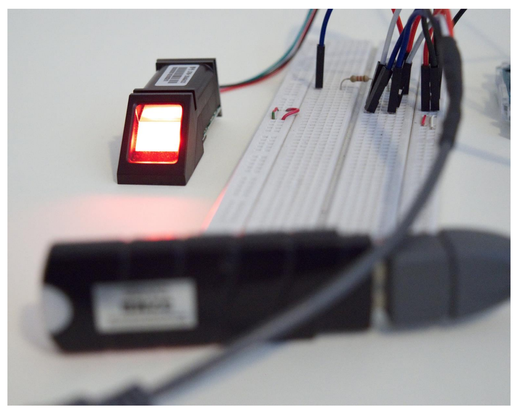

Fig. 2 – Ready for Match Test – Device Off

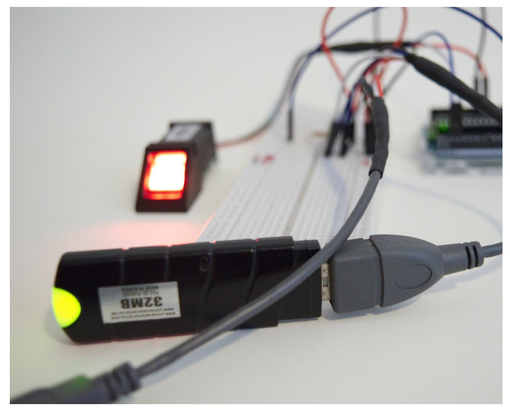

Fig. 3 – Match Found – Device On

```
p = finger.fingerFastSearch();
if (p != FINGERPRINT_OK)  return -1;

// found a match!
Serial.print("Found ID #"); Serial.print(finger.fingerID);
Serial.print(" with confidence of "); Serial.println(finger.confidence);
digitalWrite(led, LOW);
return finger.fingerID;
```

Fig. 4 – Fingerprint Testing Code

## Conclusion

This prototype shows how biometric devices, such as fingerprint sensors, can greatly improve the security of USB Flash Storage Devices. Through manipulating the power and ground pins from the USB, access can be successfully secured and controlled. However, further development are needed before this device becomes widely adopted.

## References

Arduino - Introduction". *Arduino.cc*. N.p., 2015. Web. 17 Feb. 2017.
Industries, Adafruit. "Fingerprint sensor." *Adafruit industries blog RSS*. N.p., n.d. Web. 06 Feb. 2017.
"USB pinout." *Hardware connection wirings and cables circuits*. N.p., 30 Sept. 2016. Web. 12 Jan. 2017.