Functional Specification

Year: 2025 Semester: Spring Team: 20 Project: Encrypted USB Drive

Creation Date: January 25, 2025 Last Modified: January 25, 2025

Member 1: Abhijay Achukola Email: aachukol@purdue.edu

Member 2: Brandon Liu Email: liu3394@purdue.edu

Member 3: Stanley So Email: sos@purdue.edu

Member 4: Joshua Wai Email: waij@purdue.edu

Assignment Evaluation: See Rubric on Brightspace Assignment

1.0 Functional Description

Encrypted USB Drive is a USB drive with multiple security features that allows different individuals to access separate files from the same device, without allowing others from viewing those files as well. The device is composed of a display that informs the user on how they can select which user they’re trying to log in as, whether log in attempts is successful, and whether the device is unlocked or locked. The user can input either their password or use their fingerprint to gain access to their data, at which point the device can be utilized as a standard USB drive and allows the user to also change their password or fingerprint attached to their profile. These features are also available to up to four separate users.

A diagram of a computer

Description automatically generated

2.0 Theory of Operation

Our fingerprint sensor will go through a lot of states. At the moment, we are thinking about the following states: Startup, User Select, Receiving Password, Unlocked, Change PIN, Change Fingerprint, and Locking. A state transition diagram helps to organize all of these states. It shows each state inside an oval and shows how you can transition between each state with a labeled arrow. The state transition diagram for our device is shown below.

A diagram of a software system

Description automatically generated

In the startup state, the GPIO pins are configured to whatever communication protocol they need to do. In the User Select state, the LCD display displays “Select User” and the device waits for the user to press a number on the keypad from 1-4. In the Receiving Password state, The LCD screen will show “Enter Password” and the screen will display what the user types on the keypad. The keypad input the LCD screen displays will be replaced with a dot as the numbers get typed. In the unlocked state, all the files for that user can be accessed.

3.0 Expected Usage Case

Our encrypted USB drive is expected to be used as a portable and secure storage device for up to 4 users per device in a preferably dry, indoor environment. It is expected that the user will have a basic level of technical literacy capable of using USB drives, managing passwords, and performing simple file operations. The device is deigned to be used mostly by IT professionals, military or government personnel, business corporations, healthcare institutes, legal professionals, and educational institutes to protect their sensitive data and intellectual property.

4.0 Design Constraints

4.1 Computational Constraints

To start off, the computational constraints will use a linear scan algorithm to check user id against all known records and then comparing passwords. Additionally, the goal is to have at least 100kB/s speed for reading / writing files between the computer and the flash drive. The microcontroller should be able to allow each user should have at least 4Gb of memory via allocation (no partitioning). However, the fingerprint sensor takes care of storing fingerprints and comparing fingerprints already so the microcontroller doesn’t have to do that.

4.2 Electronics Constraints

Our thumb drive will use an STM32 microcontroller to interface with a fingerprint sensor, LCD display, keypad, USB-A host, and flash memory. The fingerprint sensor will communicate using UART. The LCD display will communicate using SPI or I2C. We will interface with the keypad by polling each row and checking the corresponding column. The USB communication will be handled by the onboard peripheral inside the microcontroller itself. The flash memory will communicate using SPI. There will be a 5V to 3.3V regulator to provide power to the microcontroller and whatever peripherals need it. There will also be a crystal to make sure the USB data is transmitted at the correct frequency. There will also be a mosfet so we can turn off power to the fingerprint sensor with a GPIO pin when it’s not needed.

4.3 Thermal/Power Constraints

The input voltage from the USB should be between 4.75V and 5.25V. The device should draw less than 500mA from the USB. The maximum operating temperature should be at least 110 degrees Fahrenheit. The minimum operating temperature should be at most 32 degrees Fahrenheit. The device is powered by the USB so there is no battery.

4.4 Mechanical Constraints

Our device is intended to be preferably used in a dry, indoor environment where the temperature is room temperature. It should also be able to work outdoors provided the weather is not too extreme and not too wet. We also want to ensure that keypad & fingerprint components do not physically impede the device’s ability to connect to a laptop / computer via USB port. We aim to make the final product pocket-size for portability as well as ensuring the weight stays below one pound. The device will also include a casing to protect our electronics from dust, debris, and spillage. While we do not aim for total waterproofing, we hope to at least prevent simple drops of water from messing up the device through casing.

4.5 Economic Constraints

Maximum budget for the product is $425 without accounting for the inflation rate. However, with the encryption functionality and market analysis, a competitive price shall not exceed $150. Given the market rate, it should cost around $70-$100.

4.6 Other Constraints

5.0 Sources Cited: