Multi-Party, Multi-Factor Authentication Lockbox

By

Shelby Doty

Noah Hill

Akshay Sundaram

Project Proposal for ECE 445, Senior Design, Fall 2022

TA: Zhicong Fan

14 September 2022

Project No. 17

1 Introduction

1.1 Problem

Governments and government agencies, banks, hospitals, or companies may have rooms, safes, or vaults requiring controlled access to protect their contents. This may include sensitive information, security and surveillance equipment and their controls, critical facility infrastructure equipment for telecommunications or power distribution, or hazardous materials. Restricted areas may include server rooms, data centers, or rooms housing industrial control systems. These areas and their contents are prone to physical security attacks such as severance of critical cables, theft of communication equipment, or theft of data servers. Security attacks may be conducted by a malicious insider, resulting in devastating data breaches. According to IBM Security's "Cost of a Data Breach" report in 2020, 10% of malicious data breaches between August 2019 and April 2020 were the result of a physical security compromise while 7% were caused by a malicious insider. The 2021 "Cost of a Data Breach" report by IBM Security noted that the average time to identify and contain a breach caused by physical security compromise was 292 days while a breach caused by a malicious insider took on average 306 days to identify and contain. Existing methods to protect physical systems from malicious insiders include auditing, job rotation, and separation of duties. Auditing access to a restricted area is reactive and does not prevent unauthorized access from occurring. Job rotation and separation of duties only limit prolonged access to certain areas or physical systems.

1.2 Solution

Multi-factor authentication (MFA) is an electronic authentication method used to grant an individual access to an application or place only after successfully presenting multiple factors for verification purposes. Multi-party authorization (MPA) requires multiple individuals to authorize access to an application or place. An example of multi-party authorization usage occurs in banks when one accesses a lockbox. This requires both a bank official and the lockbox owner to act together to open the lockbox.

Our idea is to create an electronic lock mechanism that provides a proactive approach to physical access control by employing both MFA and MPA methods. Access is granted only when a configurable number of individuals (multi-party) successfully authenticate with an inherent factor and a disconnected software token received via SMS text (multi-factor). The inherent authentication factor will be a fingerprint. This locking mechanism would be applicable to a lockbox in a bank, for example, which already requires multiple parties to authorize access. However, the inherent authentication factor used for authentication in this design, the fingerprint, is not easily lost or misplaced as lockbox keys are.

1.3 Visual Aid

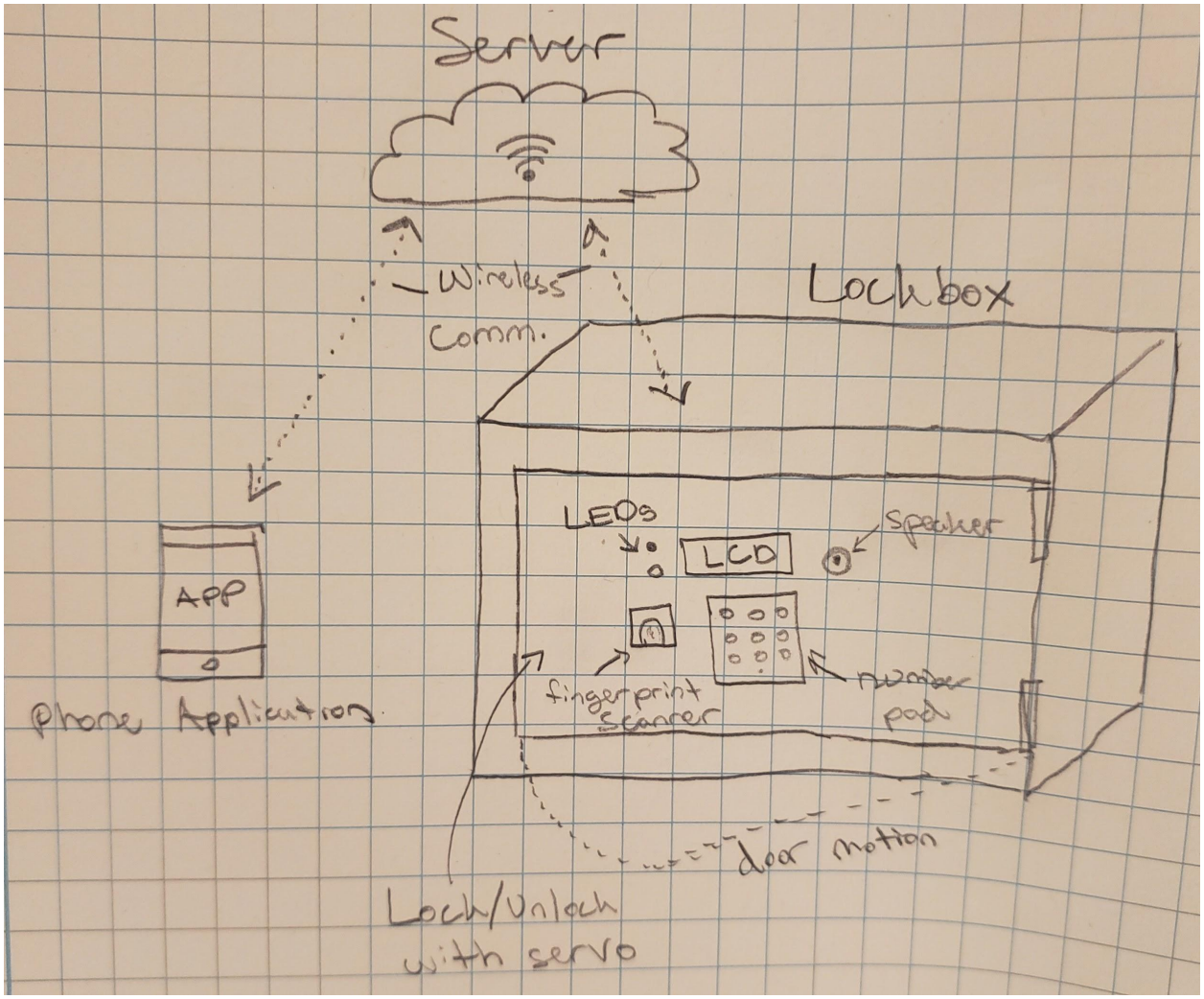


Figure 1: Drawing of Ideal Design

1.4 High-level requirements list

1. Authentication

Locking mechanism should unlock after verifying all users' fingerprints and confirming successful input of a one-time token. One-time token will be generated by a random-number generator and wirelessly sent to the user authenticating within reasonable time. Fingerprint scanning accuracy must be at least 90% or more. Additionally, it should have LED indicators for when it is locked and unlocked.

2. Wireless Connections

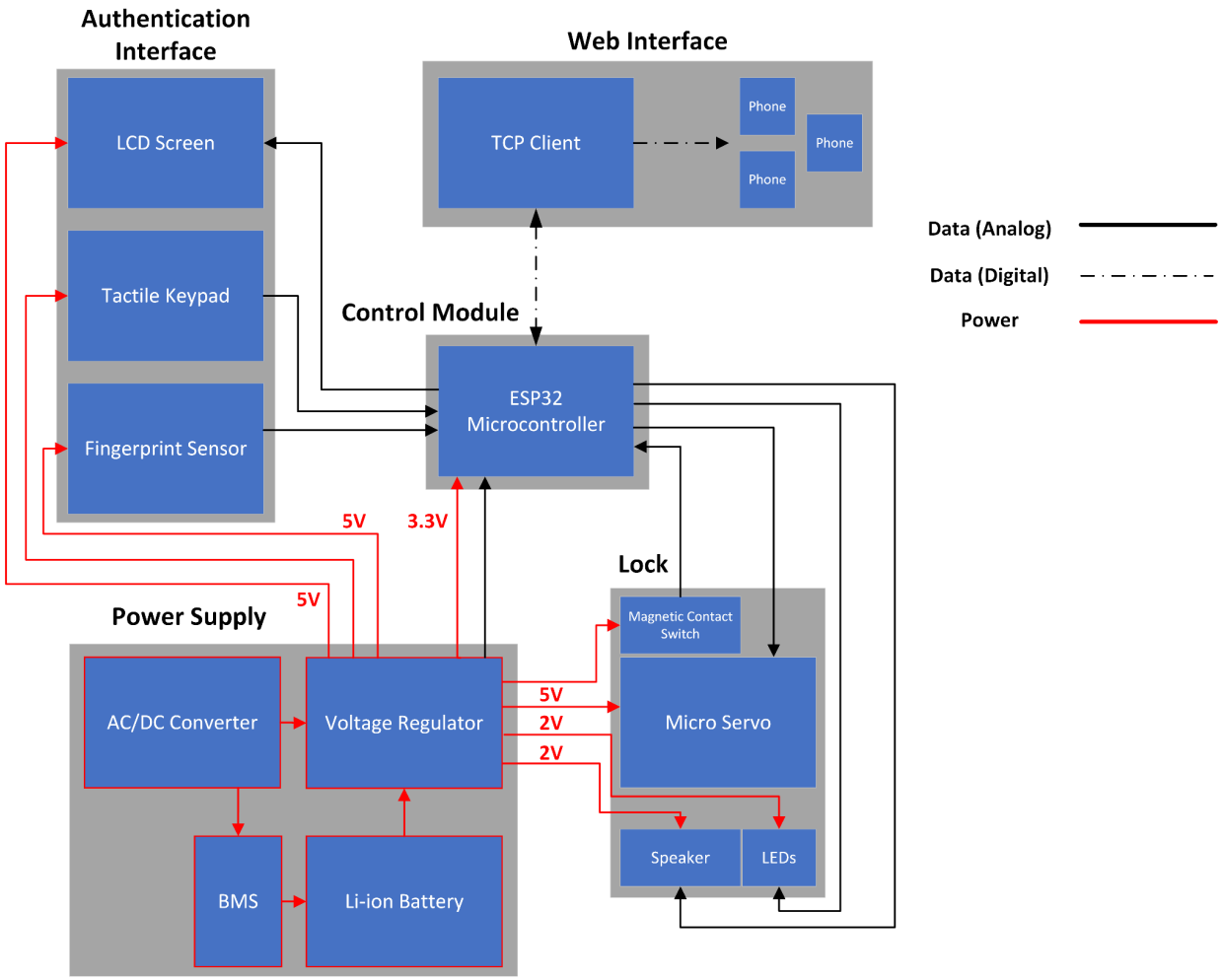
Send and receive messages via Wifi connection, link to TCP server, and then to someone's mobile device within a reasonable amount of time, <30 seconds.

3. Power

Powered by both wall outlet and back-up battery; Device can be powered by both conventional 120V AC wall outlet, or a DC power source such as the test bench power supply or a battery powered back-up.

2 Design

2.1 Block Diagram



2.2 Subsystem Overview

2.2.1 Control Module

The control module receives data from the user interface subsystem via the fingerprint sensor and tactile keypad and sends data to the web interface subsystem over WiFi. The control

module controls the LCD screen from the user interface and the servo/solenoid from the mechanical relay & lock status indicator for locking/unlocking. The control module consists of a microcontroller, the ESP32, which uses Wi-Fi connectivity and acts as a TCP client to provide the TCP server with data regarding user identity and authentication success/failure when an authentication attempt is made. Upon successful biometric authentication, the ESP32 microcontroller and the user authenticating receive a one-time token sent via SMS to be input on the tactile keypad. Access is granted/denied depending on whether the user inputs the correct token generated by the TCP server.

Requirement 1: ESP32 must communicate with TCP server at speeds over 5 Mbps.
Requirement 2: ESP32 must properly control the locking mechanism, lock status indicators, and LCD screen.
Requirement 3: ESP32 must process data coming from the tactile keypad, fingerprint sensor, and magnetic contact switch.

2.2.2 User interface

This subsystem consists of the fingerprint sensor module for gathering biometric data, an LCD screen to display warnings and instructions, and a tactile keypad. The AS608 optical fingerprint sensor module stores biometric data, collects and renders fingerprint images, and matches fingerprint scans with those in storage. A LCD2004 character-type liquid crystal display provides user feedback regarding system status, authentication success/failure messages, remaining successful authentications before unlock, etc. The 3x4 tactile keypad allows users to enter a one-time token received via SMS.

Requirement 1: Correct number must be displayed by the LCD screen when it is pressed on the tactile keypad.
Requirement 2: Fingerprint scanner must be at least 90% accurate.

2.2.3 Mechanical relay & lock status indicator

This system will be controlled by the control unit and responsible for securely locking and unlocking the lockbox using a LD-20MG Digital Servo or a MP001162 Linear Solenoid. LEDs indicate to the user when the lockbox is locked or unlocked. A speaker emits a beeping noise if the lockbox door is open longer than a predetermined amount of time. Both parts can be found in the ECE210 lab kit. A magnetic contact switch completes a closed circuit when the lockbox door is shut, sending a signal to the control module to engage the servo/solenoid lock. Each of these components were chosen because of their relatively cheap costs, and their ability to perform their function while not requiring an excessive amount of power to operate.

Requirement 1: Servo/Solenoid must create enough linear motion such that the door cannot open when engaged and can be easily opened when not engaged.
Requirement 2: Magnetic contact switch should only send a signal to the control unit when the lockbox door is closed.

2.2.4 Power Supply

The power subsystem plays a crucial role, powering the control unit, user interface, and the mechanical relay & lock status indicator subsystems. As stated previously in section 1.4, our lockbox will be primarily powered via an AC/DC wall outlet power supply, but also have a back-up battery so it remains functional if it loses power from the wall outlet. The Talent Cell 6000mAh 12V DC Li-ion battery pack can charge and power components at the same time. This functionality is compatible with our design because the lockbox must remain plugged in and while it is plugged in it should charge the backup battery and power all of the lockbox components. Included with the Talent Cell battery pack is a AC/DC 12.6 1A charger which satisfies our need to charge the battery pack, and/or power our other subsystems. Since the charger comes with the battery pack, there is no risk for us picking out the wrong one which could cause it to be damaged. Furthermore, the Talent Cell has a built in BMS with overcharge, discharge, and short-circuit protection.

The control unit needs to be powered with 3.3V while all of the other components need to be powered with 5V, excluding the linear solenoid which requires 12V. In order to achieve these voltages, we will need a voltage regulator. First, we will need to step down the 12V supply to 5V. To do this we will use a LM7805CT voltage regulator coupled with a 0.33uF and 0.1uF capacitors as stated by the datasheet [6]. To get the desired 3.3V to power the control unit, we will use an LM3940IT-3.3 voltage regulator to step down from 5V to 3.3V coupled with a 0.47uF and 33uF capacitors as stated by the datasheet [7].

Requirement 1: Power all other subsystems with their respective voltage requirements.
Requirement 2: Operate while plugged or unplugged from AC wall outlet.

2.2.5 Web Interface

The ESP32 microcontroller will act as a TCP client and connect to the TCP server over Wi-Fi. On initial connection, the user configurations will be stored on the server. Each user configuration will include a signal alerting the server to a correct/incorrect fingerprint scan for that user and the user's phone number. This will be distinct for every user. On future connections, the TCP server will receive the signal from the TCP client and will then generate a software token containing a 4-digit randomized pin code. This TCP server will send this token to the ESP32 microcontroller over Wi-Fi and to the phones via SMS message.

Requirement 1: The TCP server must be able to communicate with the ESP32 microcontroller over Wi-Fi at speeds over 5 Mbps.
Requirement 2: The TCP server must be able to store at least 3 distinct user configurations.
Requirement 3: The TCP server must be able to generate a software token containing a randomized 4-digit pin code.
Requirement 4: The TCP server must be able to send SMS messages to the configured phone numbers.

Phones will receive SMS messages from the TCP server with randomized 4-digit pin code to enter into the tactile keypad. Phones will also receive an alert from the TCP server if fingerprint scan is not correctly authenticated.

Requirement 1: Phones must receive the correct 4-digit pin code by SMS message only when fingerprint scan is authenticated.
Requirement 2: Phones must receive an alert if fingerprint scan is not authenticated.

2.3 Tolerance Analysis

Supplying the system with adequate and uninterrupted power is imperative in ensuring the proper functionality of authentication methods, continuous communication with users, and preservation of biometric data. A standby uninterruptible power supply (UPS) will turn on to power the system when utility supply voltage has fallen below a predetermined level. When the UPS is not powering the system, a rectifier will convert AC to DC to charge the UPS.

The uninterruptible power supply will be composed of protected 18650 lithium ion batteries due to their high energy density and high voltage. To estimate the amount of power required to facilitate the lock system, a “worst-case” tolerance analysis was performed. Design components requiring power were placed at their tolerance limits to calculate the range of potential wattages demanded by the load.

Four key components were considered:

- AS608 optical fingerprint sensor module
- LCD2004 character-type liquid crystal display
- Micro DC motor / Push-pull solenoid
- ESP32-S2-MINI-1 microcontroller

Voltage requirements for the fingerprint sensor module range from 3.6 - 6.0V while current drawn ranges from 120 - 150mA.

Voltage requirements for the display range from 4.5 - 5.5V while current drawn ranges from 2 - 5mA.

Voltage requirements for the motor/solenoid vary from 6 - 12V while current ranges from 40 - 300mA.

The ESP32 microcontroller input voltage varies from 3.0 - 3.6V and current drawn varies from 68 - 310mA.

Using P = IV, the greatest and least possible load power consumptions by these components were determined. These components, at minimum, will consume 0.855W 20%. At most, they will dissipate 5.6435W 20%. The additional margins provide a more encompassing tolerance estimate regarding the variation of the necessary power supply, increasing the probability of continuous power in the presence of solenoid voltage spikes or lithium-ion self-discharging.

3 Ethics and Safety

We will make sure “to treat all persons fairly and with respect”[1] when conducting ourselves as a team both between ourselves and with all others. We will also be sure to “hold paramount the safety, health, and welfare of the public”[1] when designing our lockbox in accordance with the IEEE and ACM Code of Ethics.

Since this will be a lockbox that opens using biometric data, a fingerprint, it must be able to both secure the contents, but equally important it must keep the biometric data secure. In alignment with sections 1.6 and 1.7 of the ACM code of ethics and professional conduct which state, “Computing professionals should protect confidentiality except in cases where it is evidence of the violation of law, of organizational regulations, or of the Code. ”[2], we will make sure that data is transferred by secure methods and data is never made public in order to preserve the integrity of our lockbox. Fingerprint data will also be kept on the hardware instead of the web server to keep the biometric data more secure to cyber attacks.

Regarding our battery pack, we will need to be safe in the lab when working with this. Our battery pack will follow the guidelines from the General Battery Safety[3] document on the ECE445 course website. We will also look through the battery’s manuals for the proper safety and handling procedures. We have chosen to implement a prebuilt battery pack with a built in BMS to avoid costly mistakes that may happen when designing our own. Batteries have hazards such as battery acid burn, flammability, and electric shock. In order to prevent injuries to users, we need to make sure the battery is safely secured onto the lockbox. Additionally, we will practice proper wall outlet safety by purchasing a AC/DC Converter and avoiding overheating components.

References

1. “IEEE Code of Ethics.” IEEE, IEEE Policies, Section 7 - Professional Activities (Part A - IEEE Policies), . [Accessed 15 September 2022]
2. “ACM Code of Ethics and Professional Conduct.” Association for Computing Machinery, ACM, . [Accessed 15 September 2022].
3. “General Battery Safety.” Safe Practice for Lead Acid and Lithium Batteries, [Online]13 April 2016, [Accessed 15 September 2022].
4. IBM Security. (2020). *Cost of a Data Breach Report 2020.*
5. IBM Security. (2021). *Cost of a Data Breach Report 2021.*
6. Texas Instruments, “uA7800 Series Positive-Voltage Regulators”, LM7805 datasheet, May 1976 - Rev. May 2003, [Accessed 15 September 2022].
7. Texas Instruments, “LM3940 1-A Low-Dropout Regulator for 5-V to 3.3-V Conversion ”, LM3940 datasheet, May 1999 - Rev. Feb. 2015, [Accessed 15 September 2022].