Black Box – A Porch Package Protection System

Adam Cuellar, Jacky Li, Louis Rondino, Nathan Chong

University of Central Florida, Department of Computer and Electrical Engineering, Orlando, Florida, 32816, U.S.A.

***Abstract* — The main focus of this paper is to detail the design process of the Black Box and how it provides countermeasures to porch package theft. It contains unique functions to how the user can unlock the box and provides a creative method for postal carriers to deliver valuable mail. Package security is provided by the locking mechanism and the fingerprint scanner while the barcode scanner grants feasibility for mail carriers to access the box by scanning the authorized barcode on the package. By having Wi-Fi capabilities, a dedicated server, and a mobile app, the user can obtain useful information regarding ambient temperature inside the protection system, the time and date the box was accessed, and can manually open the box through the app. Using these features all together, the Black Box produces a practical approach to discourage mail theft.**

***Index Terms* — Bar codes, consumer protection, fingerprint recognition, mobile applications, wireless communication**

I. Introduction

Purchasing valuables through online services is a common practice in this day of age. However, millions of Americans experience porch package theft quite too often since in many cases, he/she was not present to receive it. To provide countermeasures to this crime, the Black Box is created using innovative methods and technology.

A main board using the ATMega2560 microchip is designed and created to integrate peripherals it must have. These peripherals include: the fingerprint sensor, barcode scanner, Wi-Fi system on chip, locking mechanism, and power supply. These components are carefully placed inside a 22 x 19.5 x 17 in. sturdy, lightweight box. The initial state of the Black Box is in standby mode, in which it waits for an instruction by the user (to unlock it) or by the postal carrier by which he/she will use the barcode scanner to scan the authorized barcode on the package. The ESP8266 Wi-Fi system on chip allows wireless communication with a dedicated server that contains relevant information such as expected barcode(s), the time it was unlocked, and more. There are three ways Black Box will open: (1) authorized fingerprint used on fingerprint scanner; (2) matching barcodes from the package and the expected barcode; (3) unlocking feature in mobile app.

II. System Components

This section briefly describes the individual components or modules that were either designed or bought to integrate. Each component is necessary for realizing the capabilities and functions of Black Box.

A. Microcontroller

The most crucial component to any embedded system is the microcontroller. Thus, the ATMega2560 is mainly chosen because of the flexibility it provided for choosing modules to interface it with. It comes with 4 UART, 5 SPI, and 1 I2C digital communication peripherals. Having these many options allows for any design team to comfortably choose other modules to integrate with. Additionally, the ATMega2560 contains a sufficient amount of flash memory and nonvolatile memory paired with a clock speed of 16 MHz. This speed is necessary because it is desirable for the MCU to verify barcode matching when postal carriers deliver parcels.

B. Locking Mechanism

A locking mechanism is needed to keep packages safe and secured when postal carriers make their deliveries to Black Box. Researching and using a locking mechanism that is easy to integrate into the overall system is an ideal characteristic. Thus, the Atoplee electric door lock, as shown in Fig. 1 is chosen due to its simple yet effective design. It operates at 12 volts DC at a current of 2 amps, according to the product details. Additionally, the lock contains two sets of red and black wires which signify the power line connections while the other pair signifies the limit switch.

C. Barcode Scanner

The barcode scanner is a module that postal carriers will be interacting with the majority of the time with the system. Thus, a reliable barcode scanner module is needed which is why the Waveshare barcode scanner is chosen. It operates at a voltage of 5 volts with an operating current of 135 mA. Furthermore, with a dimension size of 53.3 x 21.4 mm, this module can easily be placed at convenient areas of the Black Box.

Fig. 1 Atoplee DC solenoid locking mechanism uses a latch and has an emergency lever to trigger the lock

D. Fingerprint Sensor

The fingerprint sensor will be used to keep Black Box secured by granting access only to the user's fingerprints. Thus, the Flash Tree fingerprint scanner is chosen to fulfill this role. By simply scanning the user's unique fingerprint, entry to Black Box will be gained. A high-powered DSP chip does the image rendering, calculation, feature-finding and searching. It can connect to any microcontroller using TTL (transistor to transistor logic) interface. The user stores fingerprints by using a Windows software and provides great synergy with Arduino boards such as the ATMega2560. This is because a library exists in the Arduino IDE. It operates at a voltage range of 3.6 - 6 volts, an operating current ranging from 120 - 150 mA and can store 162 fingerprints which is stored in its' flash memory of 256 bytes.

E. Wi-Fi SoC

The ESP8266 is a Wi-Fi system on chip that grants Wi-Fi connectivity to MCUs that lack this ability. This chip ca be used to host an application or offload Wi-Fi networking functions from other applications processors. It provides great synergy with the ATMega2560 since a library exists within the Arduino IDE. Additionally, it can communicate using SPI, UART, I2C, and I2S serial interfaces, providing much needed flexibility. The operating voltage and current are 2.5 to 3.6 volts and 20 microamps to 170 milliamps, respectively. With a clock speed of 80 MHz, the ESP8266 can perform calculations to verify barcode matches and to retrieve and transmit relevant data to the server.

F. Temperature Sensor

A temperature sensor is needed for Black Box to let the user know the temperature inside it. This helps the user keep in mind of temperature sensitive mail. The STS30-DIS is a valid option as it measures an acceptable range of temperature from 32 – 149 degrees Fahrenheit. Average temperatures nationwide ranges from a low 26.6 ºF to a high of 70.7 ºF in which this sensor can detect. It operates at a voltage range of 2.15 – 5 volts drawing about 600 – 1500 microamps. Additionally, it uses I2C communication with a communication speed of 1 MHz. With this speed, the sensor can keep an updated heat measurement to the user.

G. Equipment Enclosure

An enclosure is needed not only to house all the equipment, but also, to be able to hold most packages that come in different sizes. To do this, about 70% of different sized boxes from Amazon needed to fit inside a box large enough to accommodate. The enclosure measures 22 x 19.5 x 17in which is enough. In practical purposes, the enclosure will have to be drilled into the ground to prevent thieves from picking up the box itself.

III. System Concept

This section describes how the Black Box works as a complete system. Based on Fig. 2 the Black Box behavior is cyclical and this process can be summarized in four steps: lock, verify, unlock, repeat.

During the initial state of Black Box, it is assumed that the system has already established Wi-Fi connectivity via the ESP8266EX module with the user's router. When Black Box is closed and locked, the system is in standby mode. At this time, if the postal carrier is delivering a package, he/she would have to scan the barcode of the package. A button is placed near the barcode scanner to turn it on to begin scanning. If the barcode is correct, the main board will send a signal to the locking mechanism to unlock. If it is incorrect, the system will not open. Once the delivery person carefully closes Black Box, a recording of this event will take place. The software running in Black Box will notify the dedicated server the time that it was accessed along with other information such as current temperature. For a more detailed

explanation on the software, Section IV Software in Detail, gives more technical details.

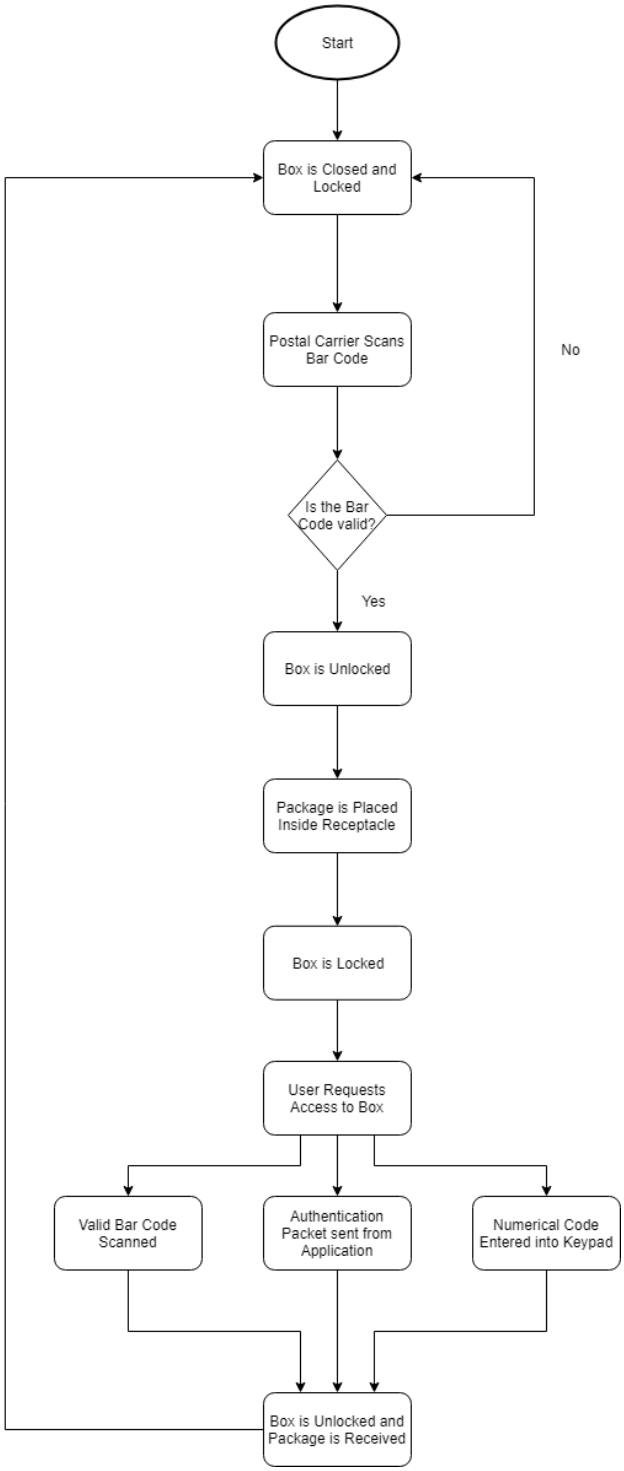

Fig. 2 Transitional Flow of each block

The user is given two choices to unlock the Black Box. One way is through the fingerprint scanner. By placing a registered fingerprint on the scanner, the verification process begins, which leads to the main board to send a signal to unlock the locking mechanism. It is important to note that the user must register his/her fingerprint prior to use. The other method is to use the mobile application which communicates with the server and the Black Box. The mobile application allows the user to press a button labeled "Unlock Box" which triggers the locking mechanism. Further details are mentioned in Section V Software in Detail under the mobile application sub-category. After the user has opened Black Box to retrieve the ordered valuables, the cycle restarts back to it being closed and locked, waiting for a new package to be delivered.

IV. Hardware In Detail

This section will further describe the modules briefly discussed in Section II System Components without the description of the microcontroller, since each technical description will incorporate how the modules connect and communicate with the MCU. Each module explanation will incorporate how they are connected with the MCU and they function with it.

A. Locking Mechanism

As shown in the lock contains two sets of red and black wires with one set signifying the power line connections while the other set of lines are for the limit switch. The limit switch lines are important to the MCU as it tells the MCU when the locking mechanism is opened or closed. It is normally closed (locked) which means that the switch is on; thus, a signal is transmitted to the MCU. When it is opened, the switch is off, and the transmission signal is no longer being carried to the MCU. This way, if there is an issue with locking, for example if the mail carrier does not fully close the box, the user can be alerted that the lock is not set.

Even though the product details described the lock having an operating voltage of 12 volts with an operating current of 2 amps, multiple tests were made to test the accuracy of those results. When the voltage is at no load, it is measured with a value of 11.96 volts. With the load of the latch, the voltage dropped to approximately 9 volts. By taking the average of the voltage drop under loads, it was concluded that a voltage of 10.36 volts is needed to allow the locking mechanism to trigger. Additionally, these tests provided data for how much current is drawn under load which resulted to a current of 1.02 amps.

One last characteristic that needed to be tested before this lock was implemented to the system is the potential

negative current that will be sent back through the device. A common problem with solenoid mechanisms with an inductive load is that when circuit switches open, the collapse of the magnetic field causes a negative current. To test this problem, the voltage is measured when switching the lock on. In, this test is demonstrated and measured. This is seen in Fig. 3.

This test concluded that a fly back diode is necessary, as almost -1 volt is produced when switching off the solenoid. Given that the measured internal resistance of the solenoid is ~5.9Ω, this translates to ~170mA of reverse current.

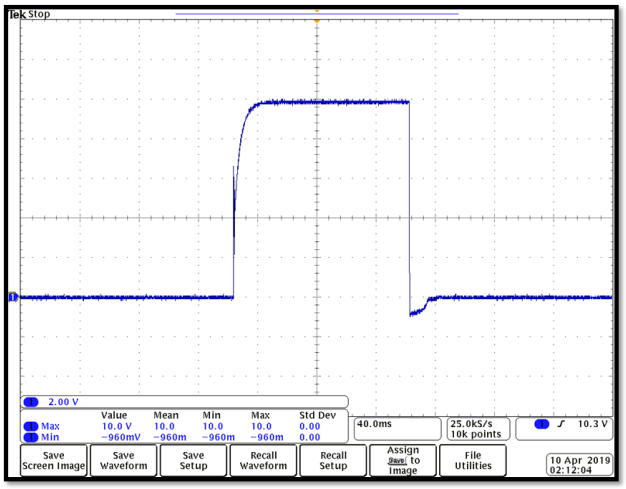

Fig. 3 Voltage Waveform reverse current

For breadboard testing, the MOSFET used is the IRF630B. Thankfully, with a drain current of 9A and drain-to-source voltage of 200V max, this MOSFET has enough voltage and current capacity to drive the lock for these tests. Since the gate-to-source voltage is high, however, an input resistor for this test is not used. This is done to maximize the signal current from the GPIO of the microcontroller. Due to the low frequency on time of less than one quarter of a second, this resistor should not be needed to protect the microcontroller. To dissipate capacitance and act as a pull-down resistor, a 10kΩ resistor is attached between the source, which is grounded, and drain of the MOSFET. As a result of the previous tests and measurement of the reverse current, a standard 1N4148 diode is used with the cathode at 12V across the inductive load that is the lock.

The resulting waveforms shown in Fig. 4, concludes that the design for the lock switching mechanism works with the ATMega2560. Set to pulse the lock for 100ms, less than the half second maximum specified by the manufacturer, the lock accurately executed an unlock and the MCU was able to read the status of the lock from its internal limit switch

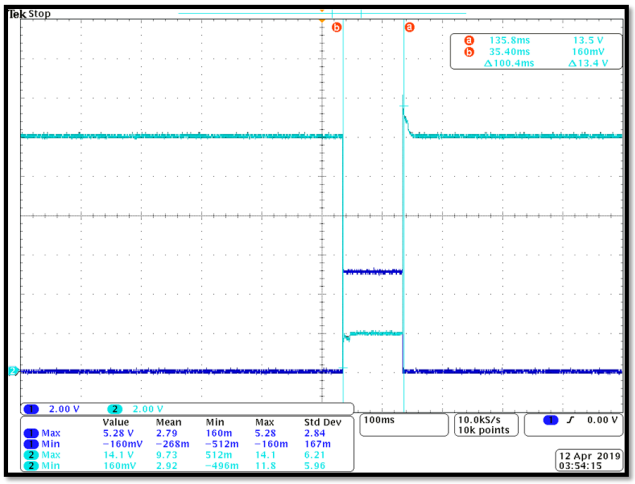

Fig. 4 Lock Response to Microcontroller Response

Since the feedback from the lock is a simple limit switch, the input can be pulled to a GPIO pin on the ATMega2560 high through a 10kΩ resistor and let the limit switch pull it low when actuated. Since the lock is an inductive solenoid requiring 12V, a MOSFET is needed to actuate it. The chosen MOSFET is capable of "logic level" actuation with a V_{GS} of 4V at R_{DS} (on) of 100mΩ. The 4V is well above the 3V logic high level specified in the 5V logic standard but still below 5V enough that a current limiting input resistor of 220Ω can be utilized. An additional 10kΩ resistor is added between the gate and source of the MOSFET to help dissipate capacitance.

The IRLL024NTRPBF also contains an internal zener diode to help against reverse current from its self-inductance. Since the battery voltage is plenty for the locking mechanism, simply supplying the lock with 12V through the header straight from the battery and back through the N-channel MOSFET on the low side is enough. From the prototyping tests, it was discovered that the DC solenoid inductive lock does return reverse current when the MOSFET is opened. To mitigate this, a flyback diode is added to prevent the current from reaching the MOSFET or worse the MCU. Similar in characteristics to a 1N4148 diode used in prototyping, the MMBD914LT1G has a forward current of 200mA and forward voltage of 1V. This is plenty to mitigate the low reverse current supplied by the breakdown of the solenoid's magnetic field. Thus, this circuit allows actuating the locking mechanism of the system safely, easily, and fast.

B. Barcode Scanner

The Waveshare Barcode Scanner Module is capable of decoding one-dimensional and two-dimensional barcodes on paper or screen with great accuracy. It is versatile in the sense that in can be plugged through its onboard USB and UART interface. Additionally, due to its small dimension of 53.3mm × 21.4 mm, the device can be easily integrated into types of devices. A white light is used with a light intensity of 250 lux and can scan a typical serial barcode such as a Code 39 at a maximum distance of 25.0 centimeters. In general, the minimum distance required for scanning is about 6 centimeters. Since UART serial communication will be used with the MCU, the default parameters of the interface are at a baud rate of 9600 bps, data bit: 8, and a stop bit: 1.

C. Fingerprint Sensor

The Flashtree fingerprint sensor makes fingerprint detection and verification simple. Two requirements are necessary for putting the module into use.

(1) The user must enroll his/her fingerprint – this is done by assigning ID numbers to each print which will be used for query later
(2) The user can search for fingerprints – searching involves asking the sensor to identify which ID is photographed.

To enroll fingerprints, the user must use their software that is only available to Windows. The user manual contains a code used for programming the fingerprint sensor to begin scanning and assigning IDs to fingerprints. This sensor uses simple communication with MCUs by using GND, RX, TX, and VCC wires.

D. Wi-Fi SoC

The major issue of integrating the ESP8266 is seen when considering that the microcontroller runs at a 5V logic level and the ESP8266 runs at 3.3V. Though the ESP8266 may work most of the time when 5V is input to it, the datasheet does not specify that it is a 5V tolerant device. Therefore, in order to safely communicate using UART between these two devices, the logic level must be converted. There are integrated circuits available that can do this for use; however, since regulated voltages are what are being worked with, there must be a simpler way to convert these signals. When sending data from the ESP8266 to our MCU, the 3.3V signal is lower than 5V and safe for the device. It is also above the 3V logic high threshold for 5V logic and will correctly register a high versus low logic signal. Since these voltages are regulated, it is safe to say that the 3.3V signal triggers a high signal successfully. On the receiving end, or going from the 5V MCU to the 3.3V ESP8266, this higher voltage can possibly damage the Wi-Fi module. To remedy this, simply use a voltage divider to step down the 5V from the MCU to a safe 3.3V for the ESP8266.

$$V_{out} = \frac{R_2}{R_2+R_1}(V_{in}). \quad (1)$$

When testing in the lab, resistor values of 1.8kΩ and 3.2kΩ were used to generate a 3.2V signal into the ESP8266. The 3.2V as opposed to 3.3V allowed a good margin of error to not risk damaging the ESP8266 by going above 3.4V. Furthermore, since the logic level is 3.3V, a 2V signal is considered high by this device. Testing this voltage divider system as a logic level converter helped understand the different communication requirements used in modern systems. In Fig. 5, it shows how the connection for our wireless module is configured. Using the standard size 2.54 female two by four header opposite of the male Wi-Fi module header, the ESP8266 can be plug and play once the PCB was printed. The idea of this is if the Wi-Fi module has a possibility of being faulty, it can easily be replaced by just pulling it off and plugging back a new Wi-Fi module back to the 2x4 header. Additionally, having the antennas for our Wi-Fi on a completely separate board helped avoid unwanted signal loss or noise due to the inductive nature of the locking mechanism and MOSFET.

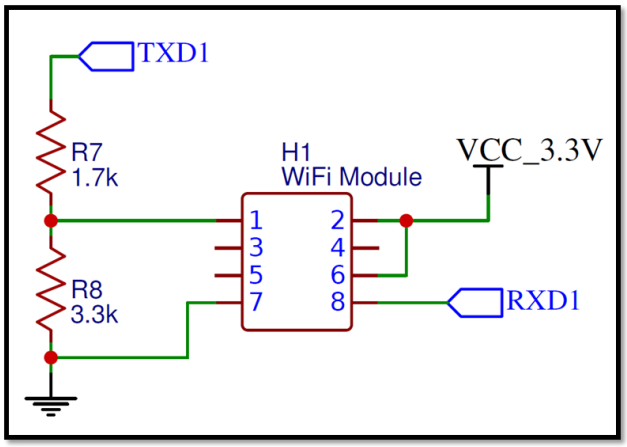

Fig. 5 Wi-Fi Module Header

E. Temperature Sensor

The STS-30-DIS is a board mount temperature sensor designed by SENSIRON. Its functionality includes enhanced signal processing, two distinguished and selectable I2C addresses, and a communication speed of 1

MHz max. To see how this sensor is integrated with the MCU, Fig. 6 is shown.

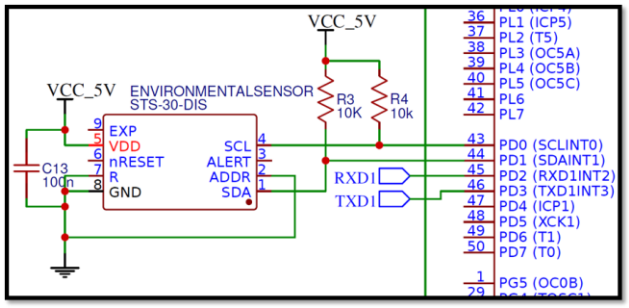

Fig. 6 Temperature Sensor Header

Pin 1 is connected along with a 10k pull up resistor for the SDA pin which is the serial data pin where it send and receive data. Pin 2 is connected to ADDR which can specify a different address depending on whether it is pulled high or low. Arbitrarily, it is pulled low for the address 0x4A. Pins 3 and 6 can be left untouched since they are used if the STS-30-DIS is preprogrammed for an alert threshold. Pin 4 is connected to SCL along with a 10k pull up resistor as required on the data sheet provided. Pin 8 is dedicated to ground. Pin 7 is R which is has no function but needs to be connected to our VSS or GND. Pin 5 is connected to a constant 5V source which is our VCC pin. Lastly EXP pin is consider the die pad so this pin is also connected to the ground or floating. It doesn't matter but it is recommended that it be soldered to the pad for mechanical reasons. C13 is required to reduce noise going into the chip power, which could adversely affect the readings received.

F. User and System Feedback

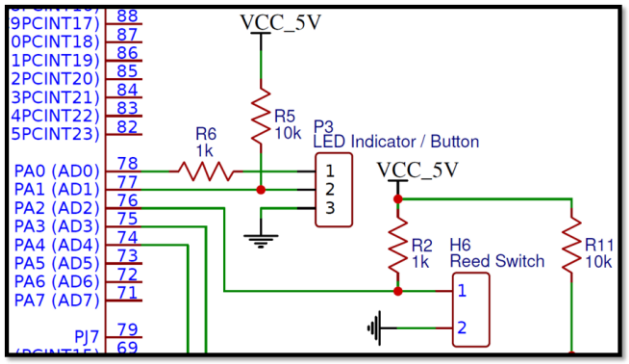

Fig. 7 User and System Feedback

Black box relies on sensors and visual feedback from and to the user to accomplish its goals. This is facilitated by two different switches which can detect if the box is opened or closed and if the lock is locked or unlocked. For this part of the schematic shown in Fig. 7, the components included are the inputs for a reed switch to detect the state of the lid of the box, a button input to detect when a user is trying to scan a package, and an LED to display to the user when the box is unlocked.

The LED and button are simple components which are mounted to the top or front of the box and connected to the main board through cables. Since they both are located in the same relative area of the box and both require a ground connection, they share the same header on the main board. The LED utilizes pin 1 on the header, which connects through a 1kΩ current limiting resistor to a general-purpose input and output register on the microcontroller. The button, however, connects directly to another GPIO pin on the board while being pulled normally high to VCC through a 10kΩ resistor. The reed switch works in the same manner as the user input button; however, it is actuated by a magnetic field triggered by a magnet on the lid of the lock. In the same manner as the button, it is pulled high with a 10kΩ resistor. This allows the user to both know when the box is closed and when it is locked to avoid unrecommended states such as the box being open, and the lock locked, or the box being closed and the lock unlocked.

V. Software Detail

This section will describe in depth how the software interacts with each module. Additionally, the server and the mobile application will be discussed.

A. Embedded Software

To program the main board, C language is used in the Arduino IDE as well as the process of bootloading. Before the bootloading process was initiated, a 16MHz crystal and two 22pF capacitors are needed to make a functional clock for the microprocessor. These components are placed in their respective pin destinations based on the datasheet of the ATMega2560.

Boot loading involves using an in-system programmer to install firmware into a blank chip. This is demonstrated as an example in Fig. 8.

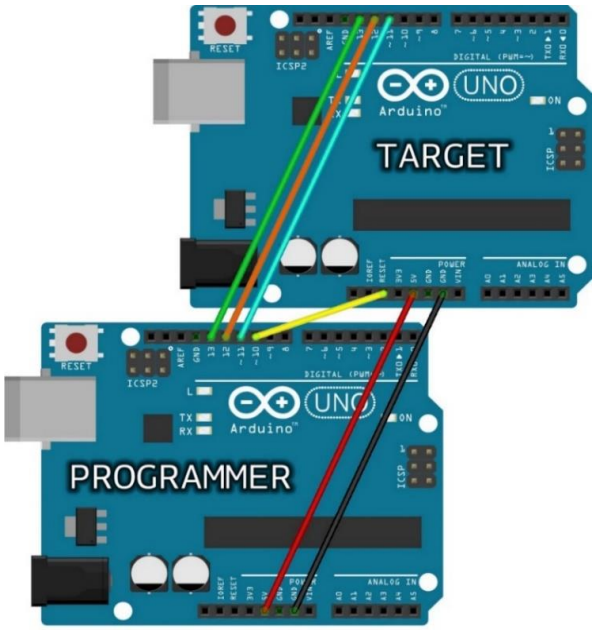

Fig. 8 Arduino Uno used as an ISP to bootload firmware to target board

The target board has no functions until the bootloader on the programmer board loads in bootloader. Many development boards have an all-in system programming header within the development board. For Atmel, they introduce a circuit seral programming header for many self-made projects, helping users jumpstart with a breeze.

To read or write over UART, it is necessary to set up serial communication parameters to match exactly with the other modules used in the system. Shown below is the exact configuration used within Tera Term.

- Baud Rate: 9600
- Data: 8 bit
- Parity: None
- Stop Bits: 1 bit
- Flow Control: none

This allowed for the most effective communication between the ATMega2560 MCU and the components purchased that involve serial communication.

B. iOS Application and Server Testing

Testing the iOS Application and web server come hand in hand due to the nature of the application relying solely on the web server. The iOS application is tested using the XCode IDE. The web server is tested using Advanced Rest Client to ensure that the HTTP requests are implemented as intended. Both the MCU and the application are used to communicate to the web server to ensure the efficiency of the handling of data.

To ensure that communication is established with the ESP8266, ATMega2560, and the sample serve, a sample iOS application that allows HTTP requests to be sent over the iOS device is created. The application sends HTTP requests just as Advanced Rest Client would do and can send/receive JSON packages. If a JSON packet is received, then it is properly decoded and processed by the application. If a JSON packet needs to be sent, then the necessary information is encoded accordingly. Using the app, it was obvious to notice that the ESP8266 was communicating with the ATMega2560. The app was able to tell the board to set the built in LED to high or low depending on the user's preference.

Using the information gathered by this testing, it is ensured that the information received from system's modules can be implemented to what the iOS application is capable of. Ideally, the application will be able to send and receive these HTTP requests to interact with the Black Box using the web server as a medium. It will also be able to display all the necessary information being sent from the Black Box to the server. Thus, these ideas were implemented to the mobile application and is completed.

Implementation of secure software for the Black Box is imperative to its design. Secure code is written to prevent users, and malicious third parties, from gaining access to software or information they should not normally have access to. In this instance, data such as tracking numbers, fingerprints registered, timestamps, recorded temperatures, are kept secure and only accessible by the user.

The sensitive data tied to the Black Box are saved on the server; therefore, malicious attacks such as SQL injections can be detrimental to the user's information. A SQL injection is when a malicious user intentionally crafts an input that is known to be used in an SQL query. To prevent SQL injections the software implements sanitizing data which causes any freeform user inputted data to be interpreted as plain text.

The configuration of the SQL database is also performed very carefully. Many database management engines contain an admin account which, if not properly configured at set up, can become a major liability and lead to disastrous data leakages or corruption. In order to prevent this, our database system is secured with access to editing data from only one account with protected credentials.

In Fig. 9, the completed mobile application is shown. Starting from left to right:

(1) Login Screen – the user inputs his/her username and password to login.

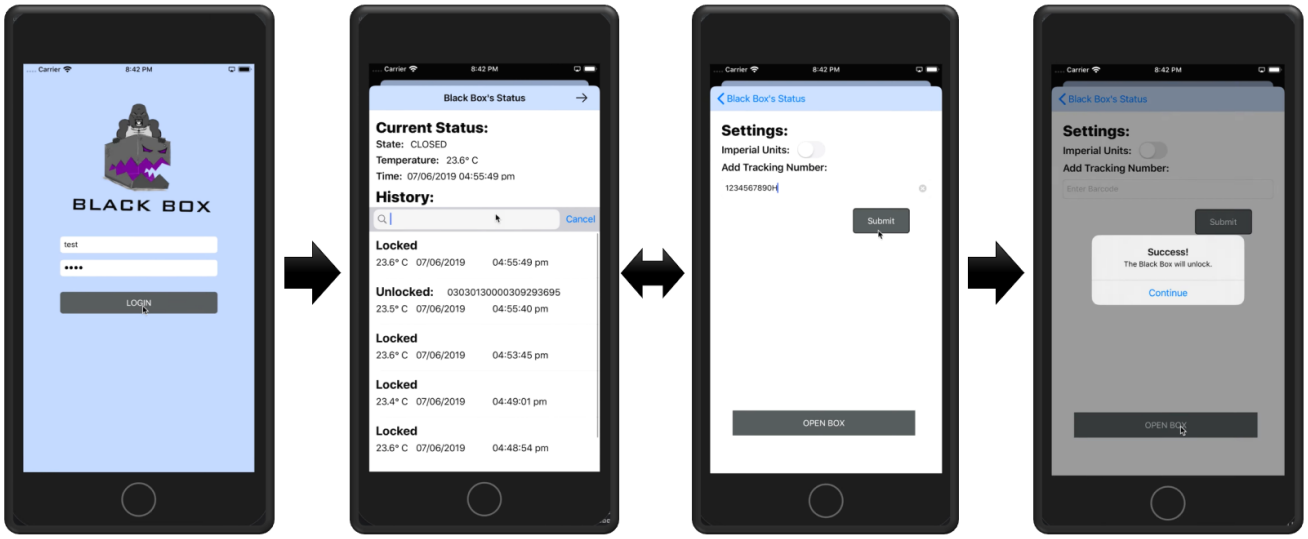

Fig. 9 Mobile Application Transition Flow

(2) Current Status & History – various information is given to the user. At the top of the screen shows the current locking status of Black Box, the temperature inside it in ºC, and the current date and time. The history section displays previous occurrences of when the box was accessed,

(3) Settings – By pressing the top right arrow in the previous state, the user can access the settings. This section allows the user to input the expected tracking number/barcode. At this point, the user can decide to go back to the previously mentioned state or can proceed to the next feature.

(4) Open Box – this allows the user to open Black Box using the mobile application. By pressing this feature, the current status and history will update

VI. Conclusion

With the motivation to design a device that will discourage and prevent thieves from stealing precious packages, the Black Box project idea was created and designed. Throughout the two semesters, the four of us in this group have met continuously, engaging in work and ideas that would eventually come together to form the ideal design. Overall, our group believes that we have provided enough research, plans, and testing to ensure an accurate representation of the Black Box project idea. From the all the research and preparation that was done, our team was able to complete the necessary requirements to complete the production of the box. There were many obstacles and challenges that approached us; however, if senior design has taught us anything, it has taught us to work together as a group to accomplish what is needed to be done which gives us a glimpse of how it will be like in the real world when working as engineers.

Acknowledgement

The authors wish to acknowledge the assistance and support of Dr. Samuel Richie, Mikael Wasfy, and Sean Szumlanski. They are recognized for their superior teaching methods and passion for teaching and guiding students to understanding difficult concepts in their respective fields.

References

[1] Neamen, Donald A. *Electronic Circuit Analysis and Design*. McGraw-Hill, 2006.

[2] "Texas Instruments CC3220 SimpleLink™ Microcontrollers (MCUs)." *Mouser Electronics - Electronic Components Distributor*, www.mouser.com/new/Texas-Instruments/ti-cc3220-MCU/?gclid=CjwKCAjw4LfkBRBDEiwAc2DSlKcljUjUy2E89LPAhVCxmgYnZf6hbnsQNQuwLedN2bjUz3g8UJlmchoCbD4QAvD_BwE.

[3] "BU-203: Nickel-Based Batteries." *Nickel-Based Batteries Information – Battery University*, batteryuniversity.com/learn/article/nickel_based_batteries

[4] https://www.arduino.cc/en/tutorial/arduinoISP