Project Magic Stick

by

Sean Barr
Kyle Ryan

Submitted to
the Faculty of the School of Information Technology
in Partial Fulfillment of the Requirements for
the Degree of Bachelor of Science
in Information Technology

Sean Barr _____ 05/01/2019
Sean Barr Date

Kyle Ryan _____ 05/01/2019
Kyle Ryan Date

_____ 05/01/2019
Bogdan Vykhovanyuk Date

University of Cincinnati
College of
Education, Criminal Justice, and Human Services

April 2019

TABLE OF CONTENTS

Section	**Page**
Abstract	1
1. Problem Statement	1-1
1.1 Introduction	1-1
1.2 Project Description	1-1
1.3 Problem	1-1
1.4 Solution	1-2
1.5 User Profile	1-2
1.6 User Case Diagram	1-5
2. Project Management	2-1
2.1 Budget	2-1
2.2 Objectives/Deliverables	2-2
2.3 Project Schedule	2-3
3. Technical Elements	3-1
3.1 *Network*	3-1
3.2 Application	3-1
3.3 Database	3-2
3.4 Security	3-2
3.5 Hardware	3-3
4. Application	4-1
4.1 Administrator Station Application	4-1

TABLE OF CONTENTS (cont'd)

Section	Page
4.2 App View	4-3
5. Test Plan	5-1
5.1 Overview	5-1
5.2 Scope	5-1
5.3 Objectives	5-1
5.4 Testing Procedure	5-1
5.5 Results	5-2
5.6 Generating TOTP	5-6
5.7 Biometrics	5-7
5.8 Final Beta Testing	5-7
6. Conclusion	6-1
6.1 Fall Semester 2018	6-1
6.2 Spring Semester 2019	6-1
Appendix A. Additional Info (Code, Tech Info, Screen Shots, Poster)	a
Appendix B. References	b

List of Illustrations

TABLES

Item		Page
Table 1.	Project Budget	2-1
Table 2.	Testing	5-3

FIGURES

Item		Page
Figure 1.	User Profile	1-4
Figure 2.	Use case Diagram	1-6
Figure 3.	Project Schedule and Gantt Chart	2-3
Figure 4.	Device Schematic	3-3
Figure 5.	Device Drawing	3-4
Figure 6.	Wire Frames	4-1
Figure 7.	Application	4-2
Figure 8.	Password Field Mac	5-4
Figure 9.	Device Logged in Mac	5-5
Figure 10.	Password field Windows	5-5
Figure 11.	Device Logged in Windows	5-6

ACRONYMS AND ABBREVIATIONS

P.M.S. Project Magic Stick

IAM Identity Access Management

TOTP Time-based one time password

MFA Multi-Factor Authentication

ABSTRACT

Passwords are not safe, and create vulnerabilities, yet, we rely heavily on them in nearly everything we do. A good password will exceed 10 characters, use a combination of numbers, upper case, lower case, and special characters. Good practice tells us not to reuse passwords. This is a lot to remember when accessing various tools and accounts in our work and private lives. Can a large company trust that a person is not using the same password when accessing company assets as they are at home? This issue is solved by using a MAGIK STICK as a multifactor authentication device that eliminates the need for employees to remember passwords for a company network. MAGIK STICK solves this conundrum by authenticating users via biometrics and generating a token for accessing applications and devices. This token is based on a TOTP (time based one-time password) algorithm.

1. PROBLEM STATEMENT

1.1 Introduction

The insider threat is one of the greatest information security threats to any organization in today's high-speed cyber workspace. Employees can cause their organization harm in a variety of ways but "Insider-threat" doesn't necessarily mean that employees are acting with malicious intent, it can also be due to technical ignorance. Employees are increasingly becoming victim to compromised or stolen credentials. An employee may become victim of an elaborate phishing or social-engineering campaign, which would allow the threat actor to harvest the user's credentials giving the malicious entity access to the organizations network.

1.2 Project Description

Design and develop a prototype multi-factor authentication to eliminate the need for credentials on a closed intranet environment such as those used by large enterprise level organizations.

1.3 Problem

There are other devices out there such as yubico for multi-factor authentication, however these all lack physical device protection. Once paired you only need plug it in or tap a button on it to get access. While convenient for access it creates a security problem if the device is stolen. They also lack a logging feature if someone else obtains the key.

1.4 Solution

Project Magic Stick aims to remove the need to remember credentials, in a secure manner. Project Magic Stick is a multi-factor authentication device that can replace the need for credentials on an enterprise level environment. The device will be centrally provisioned from a single administrator workstation to use the software that is required to authenticate and provision new devices.

The main goal of this device is to eliminate the insider threat due to user error, neglect, or ignorance. It will help to protect unknowing users against social engineering and phishing email campaigns that will attempt to harvest employee credentials and gain access to the organization's network or specific tool. It can also prevent the use of shared credentials amongst employees as there will be no need for a user to have his/her own credentials to log in to a tool or program on the network. The access rights will be provisioned into the MFA device that we are developing from a centrally located administrative console that only authorized users will use to add and provision new devices.

1.5 User Profile

Figure 1: User Profile, illustrates the user profile for Project Magic Stick. It identifies potential users of the application, related experience and similar applications that the user may have previously used, the tasks the user is expected complete when operating Project Magic Stick.

Key Solutions Incorporated

Application

Project Magic Stick

Potential Users

- Corporations and Small Startups

Related Experience

The Project Magic Stick is targeted for corporations and small business with employees that have multiple login credentials.

experience with similar applications

Users may have experience with similar security-based devices or programs such as:

- LastPass
- RSA SecurID
- Yubico
- Google 2-Factor Authentication

TASK EXPERIENCE
The administrative user of Project Magic Stick will need to have experience dealing with multiple employees, login credentials and security. Experience in the subfield of information security, identity access management, is extremely helpful. Users will be able to plug in and access login quickly and easily.

FREQUENCY OF USE
The setup for P.M.S. in its beta phase, is intended to be used to demonstrate the automatic credential login process for the user. Future development of the application will only require the setup once, and from then on, the IAM Administrator will be able to control access from the admin machine from then on.

key interface design

- Accessible on multiple devices
- Intuitive UI
- Optically pleasing for users of all ages, and visual limitations
- Fast Setup

1.6 USE CASE DIAGRAM

Figure 2: Use Case Diagram presents the project use case diagram. Project Magic Stick has a primary user and an administrator. The administrator can easily create or enter in credentials for a user and choose from other options in the setup phase depending on what the company is looking for. The administrator has access to all credentials and logs. All users will share the same experience of plugging in the device and having access to all their credentials. The user can also see their own alerts if the device is compromised.

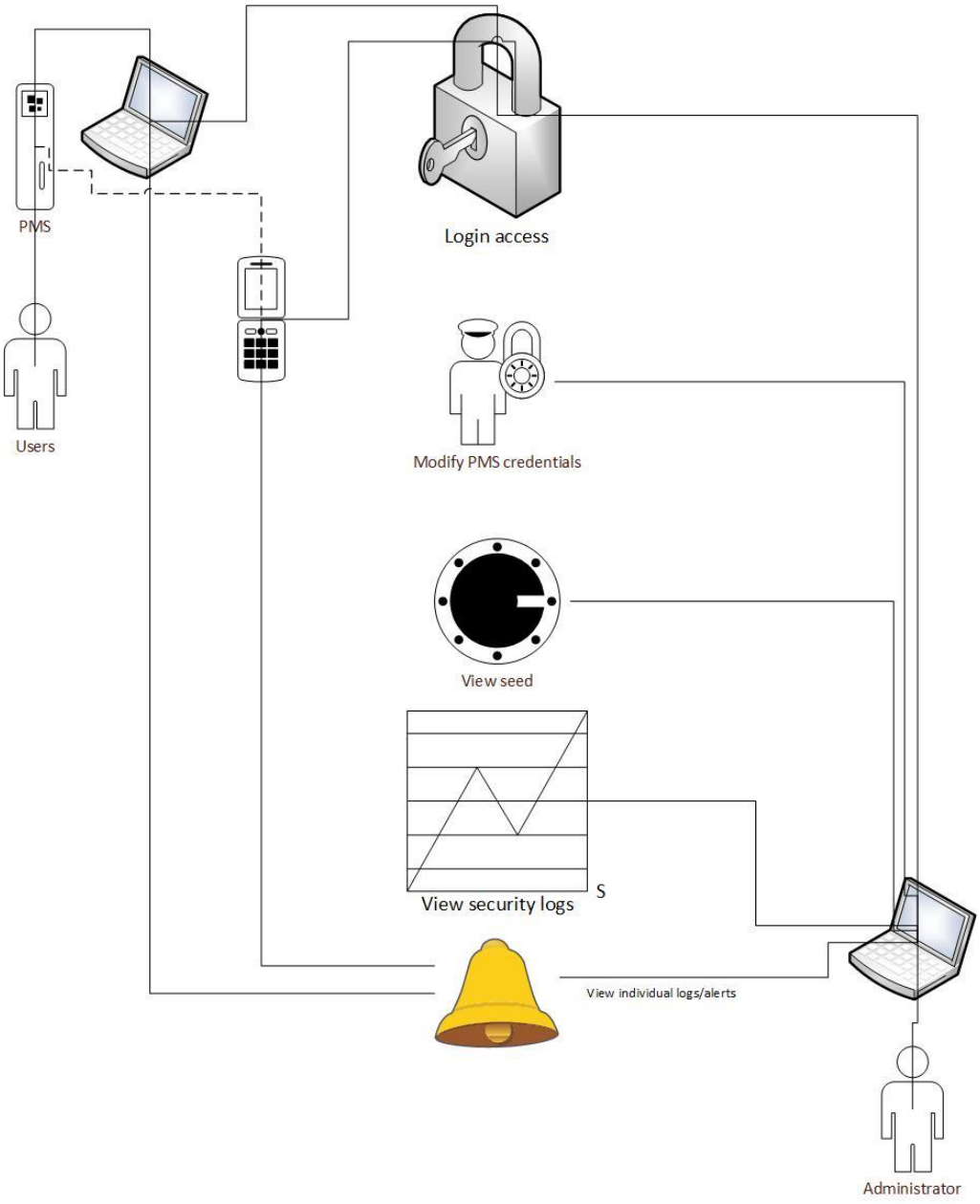


Figure 2: Use Case Diagram

2. PROJECT MANAGEMENT

2.1 Budget

Table 2: Project Budget represents the project budget. To start we each needed an Arduino to work on and a BLE module. We only needed one fingerprint scanner for the final product. This does not represent working costs as we are all working for free. Everything has fallen within our $200 budget.

Table 1: Project Budget

ITEM	UNIT #	COST	TOTAL
Arduino micro	3	$20	$60
BLE module(Bluetooth)	**3**	$18	$54
TOTAL($200)			$114

2.2 Objectives/Deliverables

The primary deliverable is to have a device that can create the TOTP tokens. This step would be 11. program encryption method in Figure 3: Project Schedule and Gantt Chart. Once this is complete our device will be capable of generating a TOTP token. From here we can begin working on making it push the credentials to devices, and developing the apps associated with it.

2.3 Project Schedule

Figure 3: Project Schedule and Gantt Chart is our project schedule.

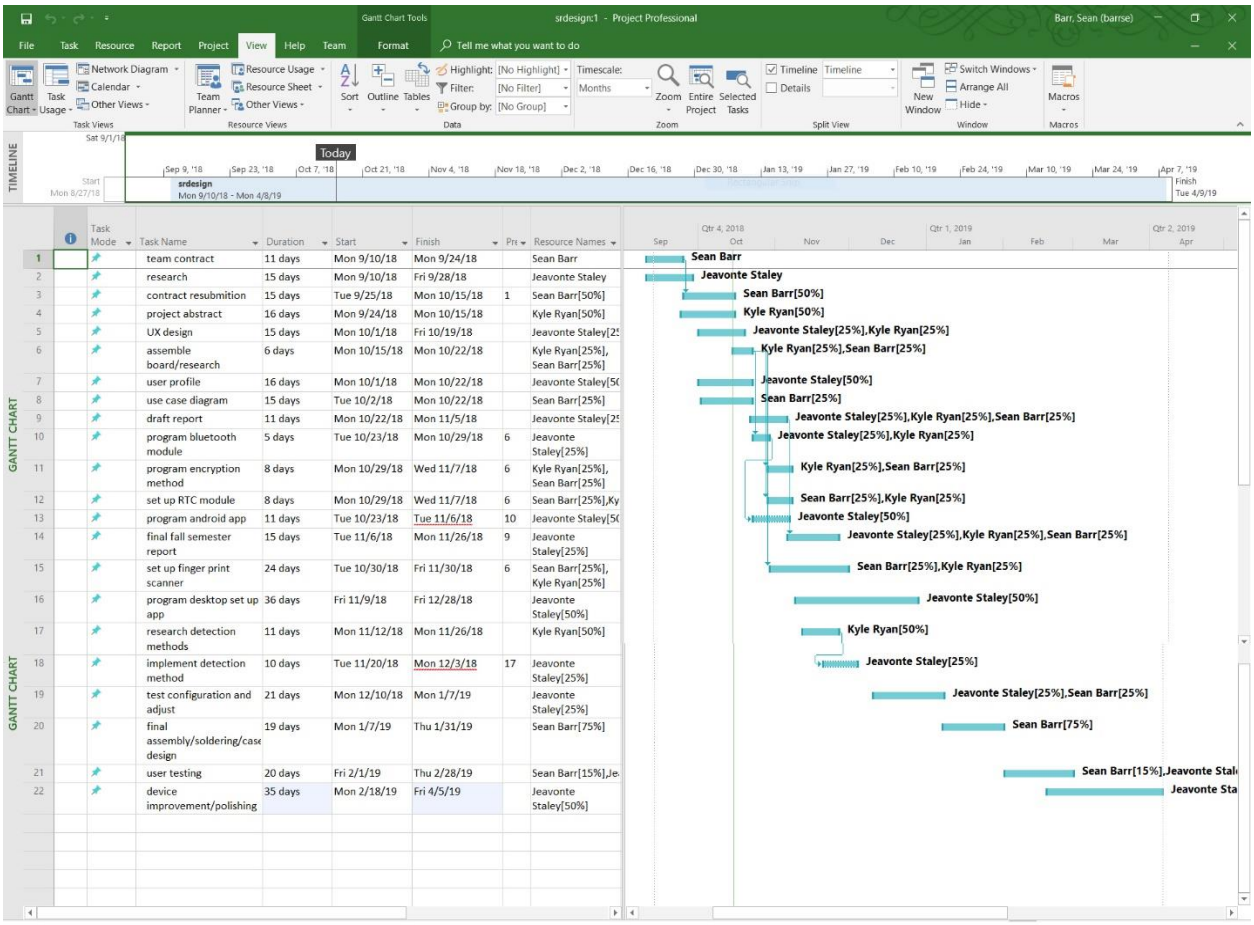


Figure 3: Project Schedule and Gantt Chart

3. TECHNICAL ELEMENTS

3.1 Network

TOTP secrets can be stored with passwords on the server. When a user tries to authenticate it will compare credentials and the TOTP code that is generated to verify the user. The extent of the network usage will be allowing the system that is hosting the actual administrative hub to connect to the backend database during the process of initializing a new user and adding or editing any further provisions. The administrative host machine will be registered when the final version of the admin user interface is implemented. There will be security measures implemented to protect this machine from unauthorized access. It will likely be on a secure private subnet all its own.

3.2 Application

There will be multiple applications associated with the Magic Stick. The desktop application for administrators will be designed for setting up the Magic Stick with necessary credentials and initiating a mobile device to be paired with it. In future updates it will also be used for logging Magic Stick security data.

The mobile application for users will allow for users to authenticate via pin in case of false-negatives associated with biometrics. It will also allow users to push credentials to USB connected devices, and mobile applications.

3.3 Database

To incorporate Active Directory into Project Magic Stick, it will have Active Directory Domain Service to manage the various Project Magic Stick devices within the network. The Active Directory Certificate Services will distribute and manage the digital certificates to the Project Magic Stick device through the Public Key Infrastructure. The Active Directory Federation Services is what will allow the IT Administrator to share resources to their employees or, allow their employees to access resource within other organizations. Web single sign-on allows employees to use their existing company credential to log into web applications, while creating trust relationships between the employee's organization and the application they are logging into.

3.4 Security

The device will utilize TOTP to create one-time passwords. It will also leverage biometric and pin entry for securing physical devices. This will help eliminate the need for credentials in an enterprise environment. The device will combat reverse engineering by applying encryption to sensitive data and going as far as hiding serial numbers or other unique device identifiers from being recovered by those attempting to reverse engineer the device.

3.5 Hardware

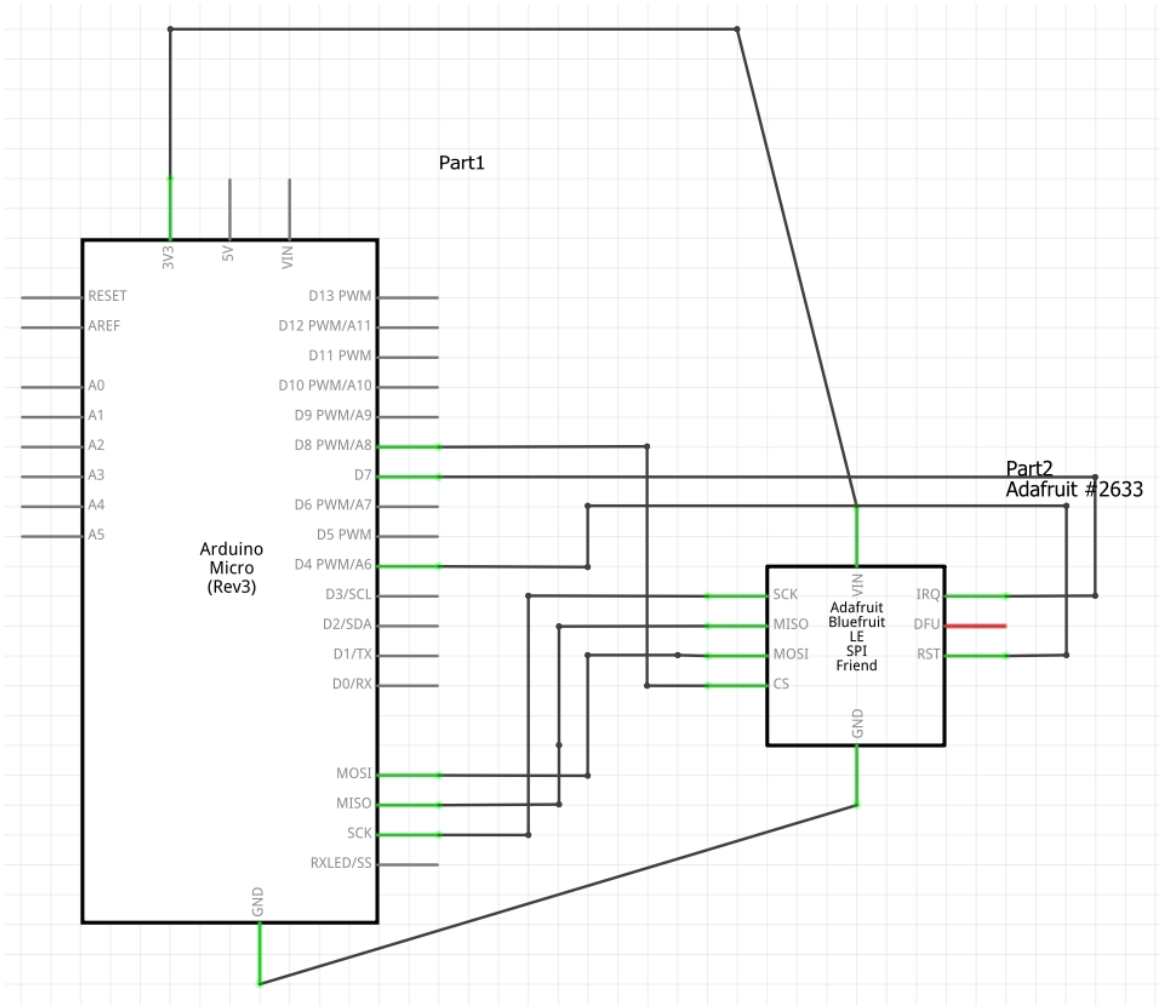


Figure 4: Device Schematic

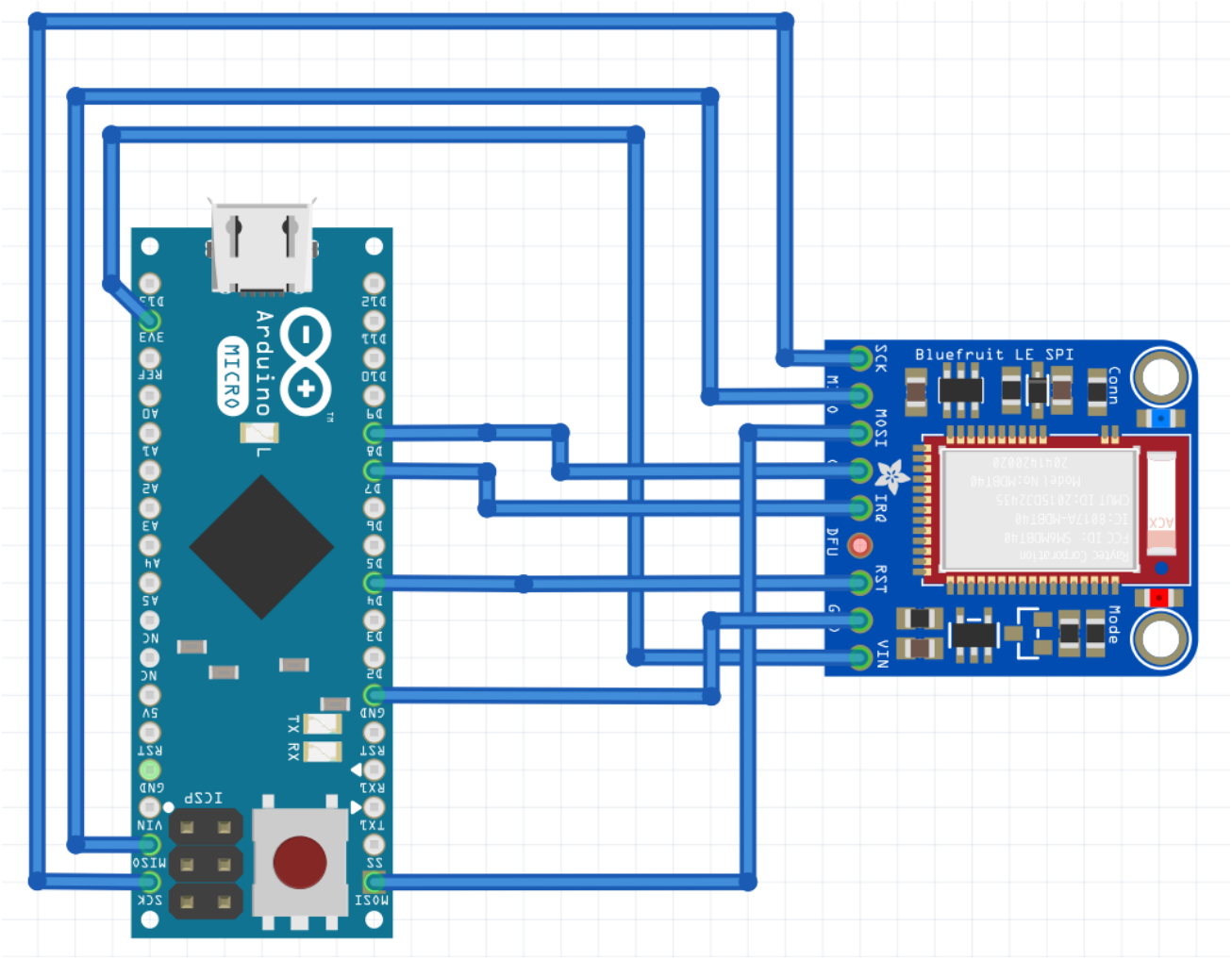


Figure 5: Device Drawing

Project Magic Stick will be developed on an Arduino Micro. This is because the Arduino Micro comes in a size close to what we want for the final product, its microprocessor can be used for Time-Based One Time Passwords(TOTP), as well as storing other credentials. In addition, the Micro allows us to connect any modules we might need. The module we have chosen to connect to the Micro (left) is an Adafruit Bluefruit SPI Friend (right) Figure: 4 Device Schematic Figure: 5 Device Drawing.

The Bluefruit module will be used to connect the users' phone to Project Magic Stick over Bluetooth. This connection will let the user authenticate on their mobile phone.

4. APPLICATION

4.1 Administrator Station Application

Figure 6: Administrator Station Wire Frames

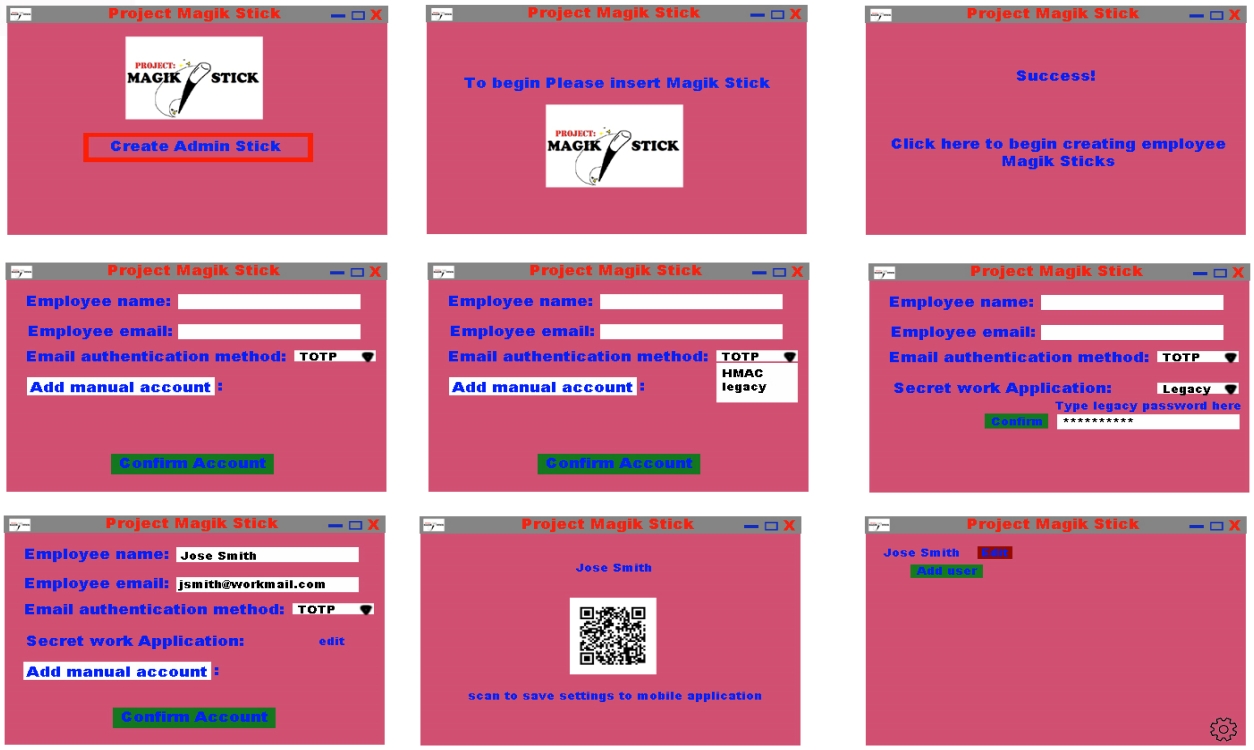


Figure 6: Wire Frames

4.2 App View

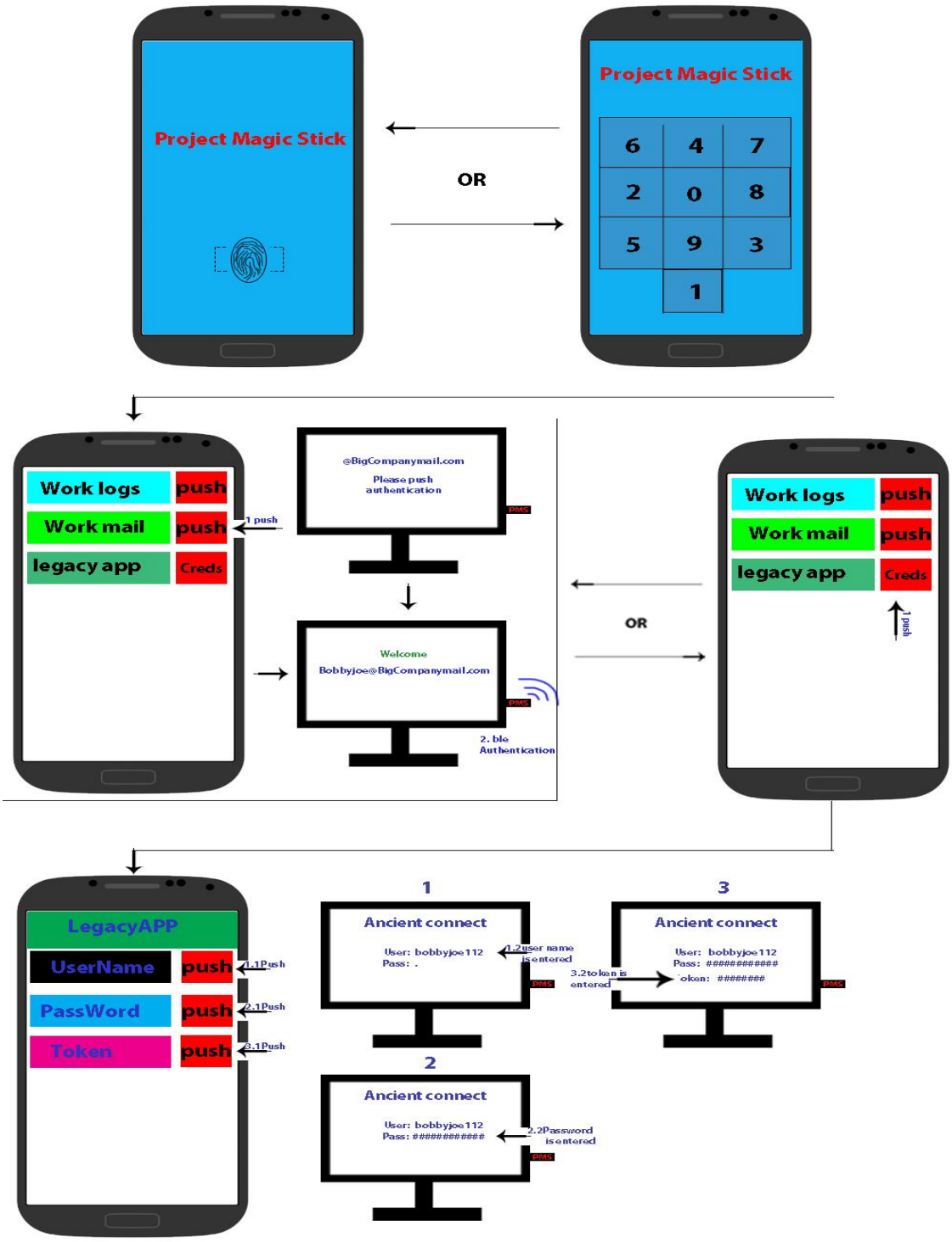


Figure 7: Application

5. TEST PLAN

5.1 Overview

This section will explain testing of the Magik Stick and why we chose these methods. It should be used as a reference for administrators managing and distributing Magik Sticks to employees, or individuals utilizing this tool for personal use. Future testing will be needed as mobile applications are developed. This testing is to confirm the hardware can perform as intended.

5.2 Scope

The scope of our testing will be to verify if the Magik Stick can type and enter the password on its own, on different operating systems. We will be testing on Mac and Windows. We decided this because Mac and Windows are the two most common operating systems. We will broaden our scope once our mobile applications are up and running.

5.3 Objective

The objective is to test if the hardware functions properly as a keyboard to enter passwords automatically for users. A pass for this will be once the Magic Stick is inserted it will type the password into the selected field, press the enter key by itself, and allow entry to the chosen operating system.

5.4 Testing Procedure

We began by locking our computers and placing the cursor in the password field. Next the device is inserted into the computer. Once inserted the device will automatically type the password and press the enter key.

5.5 Results

On both Mac and Windows, the device succeeded. The only thing worth noting is when plugged into a mac that is already logged in, it will ask to set up the keyboard. We found that by clicking “cancel” it did not pop up again, and Project Magic stick was able to type to password fields and press the enter key without any problem.

Table 2: Testing

	YES	NO	Comments
Hardware			
Does the device power on when inserted?	X		
Does the device type credentials when button is pressed?	X		A mac logged in will request keyboard setup. Cancel and device works normally.
Software (mobile)			
Does the application give access upon correct biometric verification?	X		
Does the application successfully connect to the Magik Stick via Bluetooth?	NA		
Does the application make the Magik Stick print credential with button click over Bluetooth?	NA		
Does the application tell the Magik Stick to print the corresponding credentials from the application?	NA		
Does the application update the Magik Stick with the correct time(verify TOTP code)?	NA		
Software (desktop)			
Does the desktop application set up an administrator Magik Stick properly?	NA		
Does the desktop application let you create a new user?	NA		
Does the desktop application allow manual accounts to be added? (in comments inform of limits)	NA		
Does the desktop application present a QR code when account is confirmed?	NA		
Does the QR code set mobile application with proper authentications?	NA		
Does the desktop application allow for all accounts to be securely (encrypted) saved to drive internal and/or external?	NA		

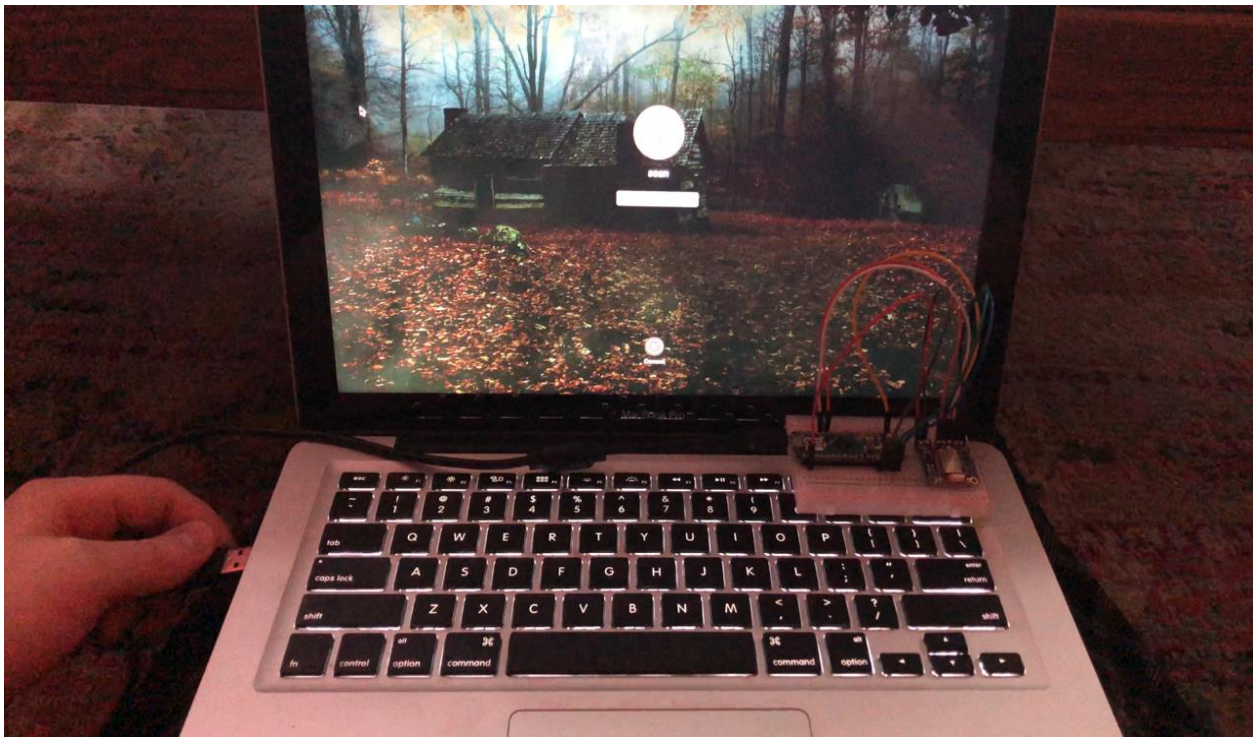


Figure 8: Password Field Mac

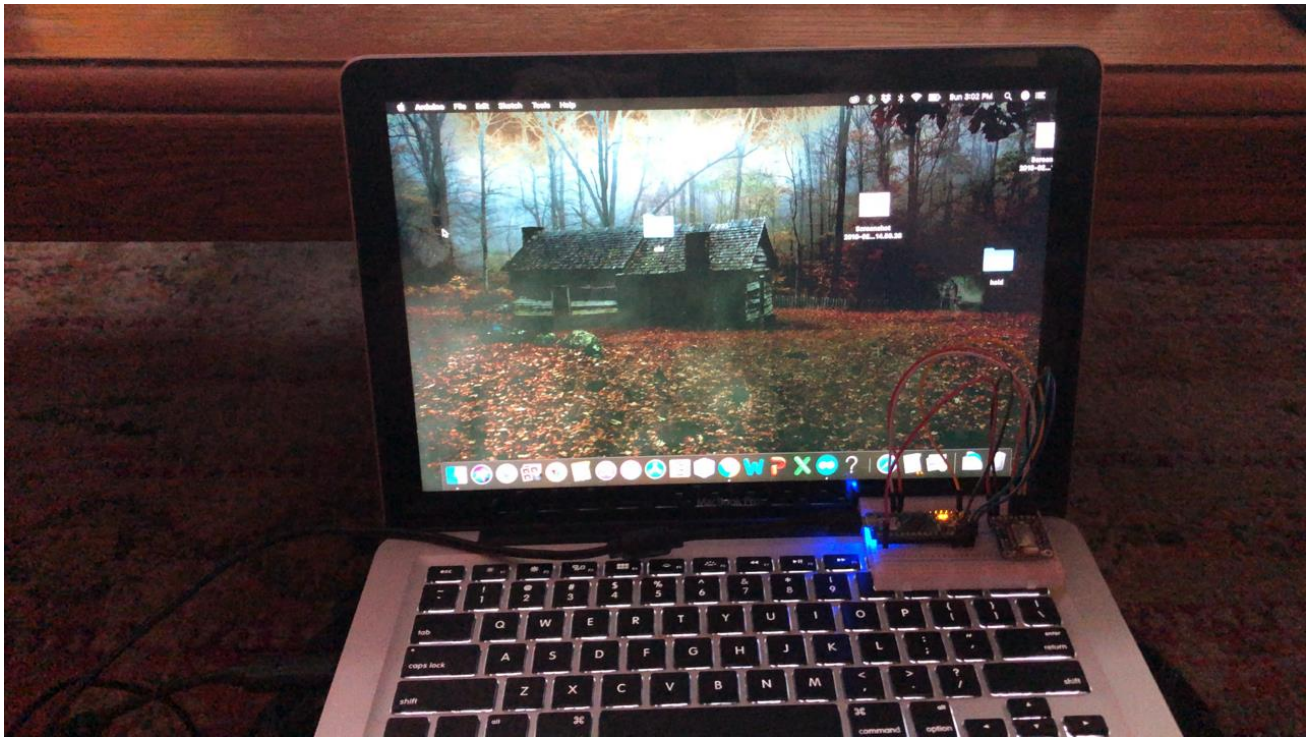


Figure 9: Device logged in Mac

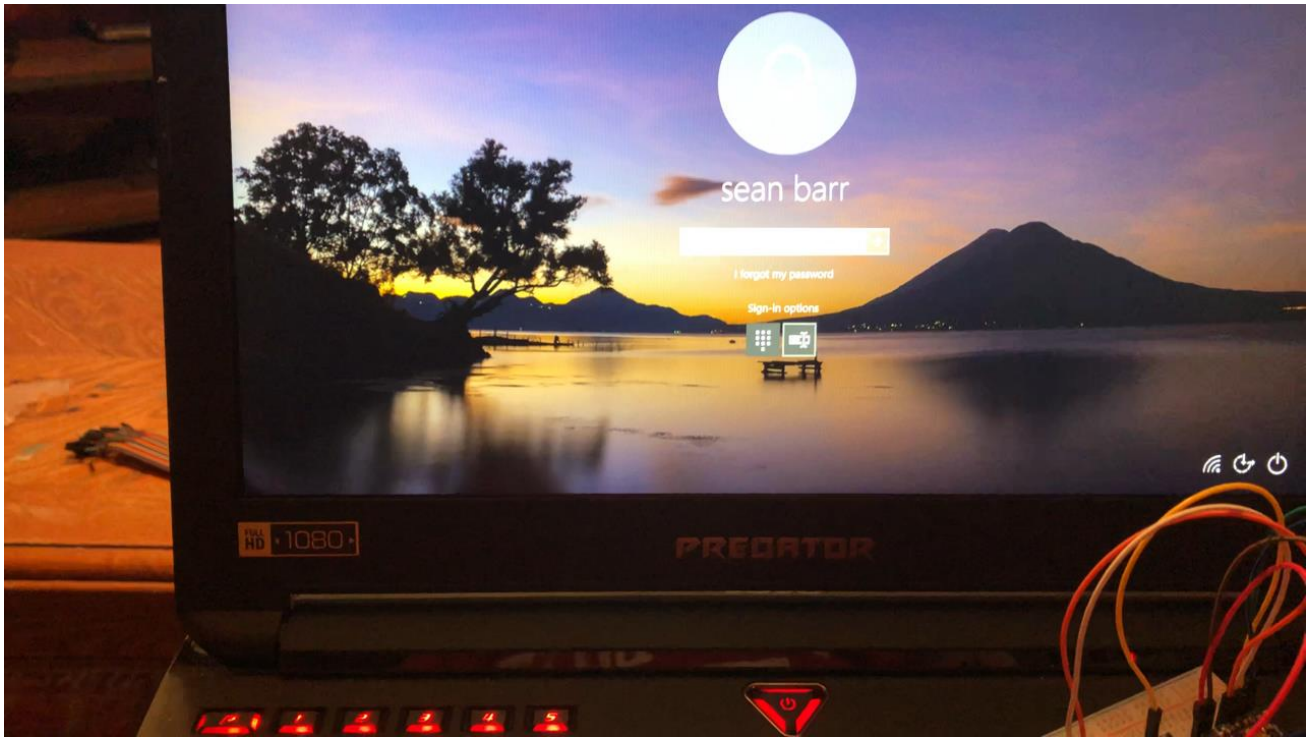


Figure 10: Password Field Windows

Figure 11: Device logged in Windows

5.6) Generating TOTP:

This test is primarily aimed at having a backend credential database, such as Microsoft's Active Directory, generate a new time-based one-time password for a user each time they are logged in. We believe that this portion of development on this project will take the most time and effort, therefore it has a higher priority.

5.7) Biometrics

The next step is to also have the device recognize the user's biometrics before there is a TOTP generated. While it might make sense to focus on this before generating the TOTP, we feel it is necessary to the success of our project that we are able to generate the token.

5.8) Final Beta Testing

During the final phase of testing, we will ensure that the device is functioning as intended. We hope to have a working, form-factor, prototype device at this point that we can deploy in a real-world setting. For our final iteration we want to make a 3-D printed casing with physical securities such as epoxy applied to hide serial numbers and other unique device identifiers. With this device in hand, we will use it to authenticate to a network and host machine with the designated methods.

6. CONCLUSION

6.1 Fall Semester 2018

Our attention has mostly been aimed at the hardware we are using and getting the device to work. We each have our devices, and personal projects to do with the devices in order to bring together and have a functioning device. Short term we want to make the device generate TOTP tokens. Once we can generate the code, we can work on how to store the seed and credentials, pushing them to chosen device, and detection methods.

6.2 Spring Semester 2019

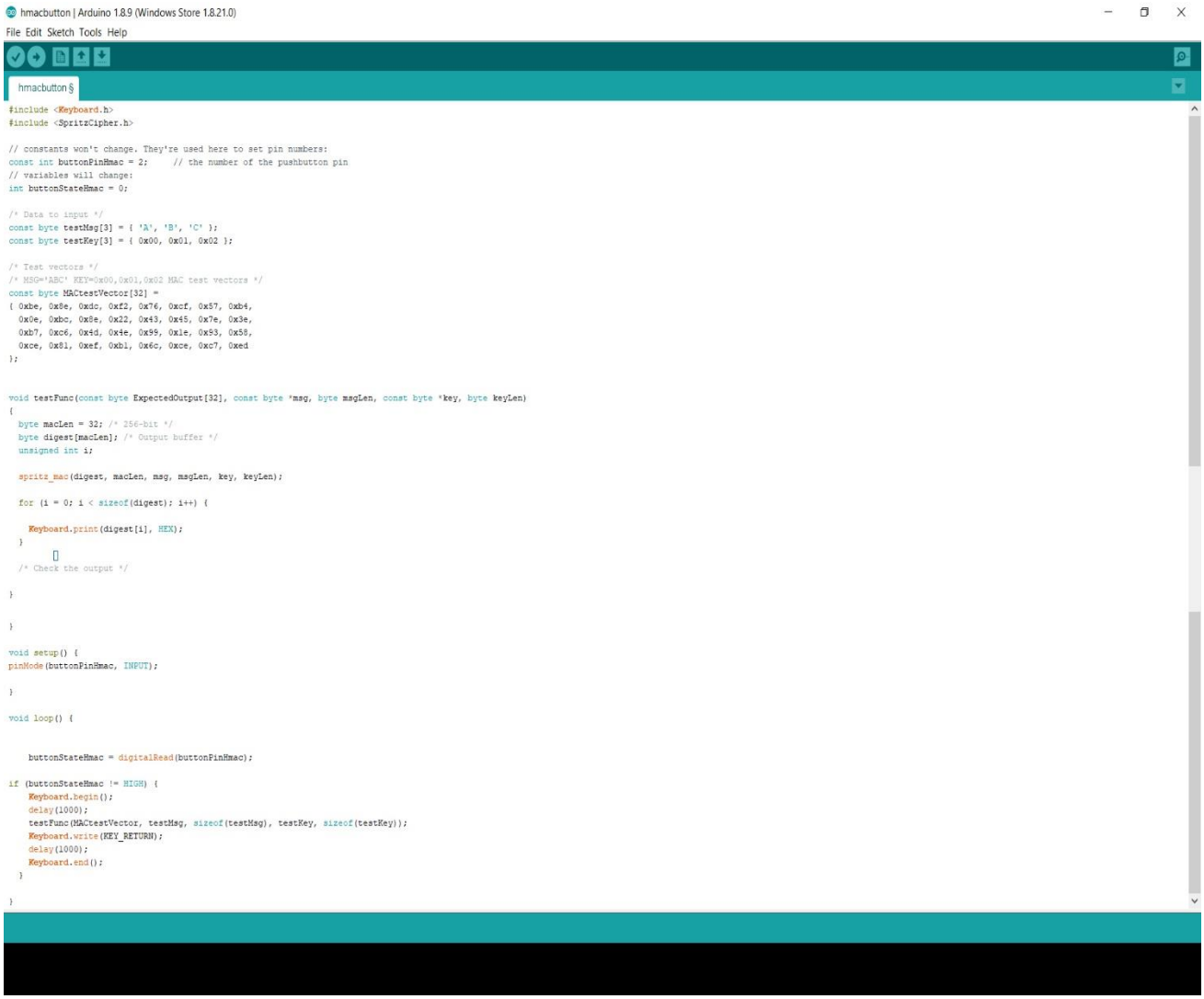
We will begin backend development and further development of our administrative console. Also, we will further develop the device to store and pass credentials properly. Currently we are using two pieces of hardware as seen in both Figure: 4 Device Schematic and Figure: 5 Device Drawing.

We ran into problems with our developer dropping from the course. This caused us to have very little time to learn how to do his portion of the work, resulting in no application or backend. We did have a functional device with a push button for proof of concept.

APPENDIX A. ADDITIONAL INFORMATION

The team contacted the following professionals for clarification and additional insight.

1. Bo Vykhovanyuk, Advisor



Arduino Code

APPENDIX B. REFERENCES

1. Courses, Microsoft Video. YouTube. January 30, 2017. Accessed December 02, 2018. https://www.youtube.com/watch?v=RPzcxdiyVCM.

2. Fritjof. "Fritjof/leostick_otp." GitHub. April 18, 2013. Accessed December 02, 2018. https://github.com/fritjof/leostick_otp.

3. Karami, Mohammad Amin. "Using a C# Application to Communicate with an Arduino." All About Circuits. February 06, 2017. Accessed December 02, 2018. https://www.allaboutcircuits.com/technical-articles/csharp-windows-application-for-arduino/.

4. Lucadentella. "Lucadentella/TOTP-Arduino." GitHub. January 16, 2016. Accessed December 02, 2018. https://github.com/lucadentella/TOTP-Arduino.