
# IOWA STATE UNIVERSITY

## AEROSPACE ENGINEERING DEPARTMENT

## Computational Techniques for Aerospace Design

## AERE 361

## Project Proposal

## High Voltage

---

*Team Member Names:*
Jani, Moksh
Kacmarynski, Wyatt
Latcham, Wren
Modi, Mihir
Pelkey, Tristan

# Contents

# I ABSTRACT

Team High Voltage's project provides a solution to keeping passwords safe while allowing quick access. Passwords have always been an annoyance to keep track of, so people reuse the same passwords for different websites, increasing their vulnerability. Our proposed solution is to use an RFID tag to access then decrypt a file with all the user's passwords, and send those passwords to the user's smartphone or computer using Bluetooth Low Energy. The file will be encrypted to ensure it is safe while stored on the board. The user will no longer have to worry about using the same password and have the confidence that their passwords and online accounts are secure.

# II INTRODUCTION

Passwords are used to keep all of our information secure, from our emails to files we want to keep safe. Human behavior often reduces the effectiveness of the passwords we use, as people should use a different password for each system, but people rarely do so. For our project, we will be creating an offline password manager. This will allow us to be able to keep control of the many passwords we regularly use. Our team consists of Mihir Modi, Wren Latcham, Wyatt Kacmarynski, Moksh Jani, and Tristan Pelkey.

To create this password manager we will use Radio Frequency Identification (RFID) and Bluetooth Low Energy (BLE) to communicate with our device. This device will then be able to decrypt a password file and send that file to a phone or other Bluetooth device using BLE.

# III FEATURES

Table 1: Three Key (Required) Features

| |
|---|
| 1. Use RFID/NFC (or a password sent over BLE) |
| 2. Decrypt a Password File |
| 3. Send requested Password(s) to a Phone using BLE |

Our project will first have to be able to accept a valid authentication token (either a password sent over BLE, or an RFID/NFC badge being scanned). This ensures the password file can only be opened by someone who has been granted access. If there is not a valid authentication token presented, the device will not proceed further, and after a certain number of tries can be disabled for a length of time to prevent further attempts, increasing security.

The file will be kept encrypted until it is requested. Since the file will be kept encrypted, it will have to be decrypted when the user requests access. This will keep the password file from being compromised by an unauthorised user trying to gain direct access to the device.

After this, the user will be able to request what file they want through a BLE terminal connection. The microcontroller will then send the password over the same BLE terminal to

the user's phone, allowing them to use this password. It will then re-encrypt the password file.

Table 2: Three Stretch Goals

| |
|---|
| 1. Implement Two-Factor Authentication |
| 2. Send Whole Files |
| 3. Wireless File Management |

In addition to the 3 key features (see Table 1), our group decided to add stretch goals that we hope to finish, but drastically increase the difficulty of the project, these features are listed in Table 2. The first (comparatively simple) feature, would be the addition of Two-Factor Authentication. Ideally a login includes something you have, and something you know; we can implement this by requiring the user both scan a RFID/NFC badge, and enter a password. The second additional feature would include adding the ability to send whole files. While this would be slow, this would add another feature and allow users to store multiple files on the device instead of just one. The final (and most difficult) additional feature our group wants to add is the ability to manage this device over WiFi. This would be a much more convenient way to manage the device, allowing a user to manage what other users are allowed access, and/or passwords/files are stored on this device.

# IV PROBLEM STATEMENT

For years, people have tried to hold themselves to the standard of using different, safe passwords for each of their online accounts. However, in a study done by Gaw and Felton at Princeton University where they surveyed 49 undergraduate students, they found that the majority had less than 3 passwords, and frequently the passwords were re-used across different account logins [2]. While this study might be considered old in some fields (it was published in 2006), its primary focus is on human behavior relating to password security, which has not changed significantly since then. The meaning behind this study is that many people, while claiming to want a different password for each of their accounts, quickly realize that re-using one or two passwords is easier. Most people only think of human attackers and not automated tools that can try thousands of passwords a second, so their passwords are relatively insecure due to their misunderstanding of how their password can be cracked[2].

Another context that aggravates this reuse of passwords is the online versus real world interactions. When using passwords in the real world, such as at an ATM, unlocking a phone, or a keypad lock to a computer lab, the human mind can learn to correlate that specific password pattern to the physical stimuli surrounding it (eg: location, or phone) when the passwords are used regularly. In this way, the passwords do not have to be the same but the person's mind will easily remember it. For an online interaction, where website after website all start to blend together, having a multitude of passwords can be hard due to the rarity at which people visit specific websites, leading to people choosing to reuse the same handful of (often insecure) passwords[2]. A study from Carnegie Mellon University confirms this, stating that users understand they should create a different password for each

distinct website, but most do not. They go on to state, "these behaviors are likely rational coping strategies for users who are asked to make far more distinct, complex passwords than they could possibly remember." [6]

In the context of an industry, an example of poor password management leading to a company disaster is the Equifax data breach from September 2017. According to the Federal Trade Commission, a data breach at that time exposed 147 million people's data and the settlement for that included up to $425 million for people affected by it[1]. Additionally, over 70% of employees reuse personal passwords at work and this correlates strongly with breaches, as 81% of hacking breaches are due to weak passwords[3]. Because people's personal passwords are not very secure, when these same, insecure passwords are used to access important company files, it makes the company vulnerable to attacks on its data, similar to what happened to Equifax. Another example of this is the recent Dropbox data breach, where a reused user password led to 60 million credentials being stolen[3]. Poor personal password management is starting to lead to poor password practices in many industries, which is a high-risk security issue for the companies.

# V PROBLEM SOLUTION

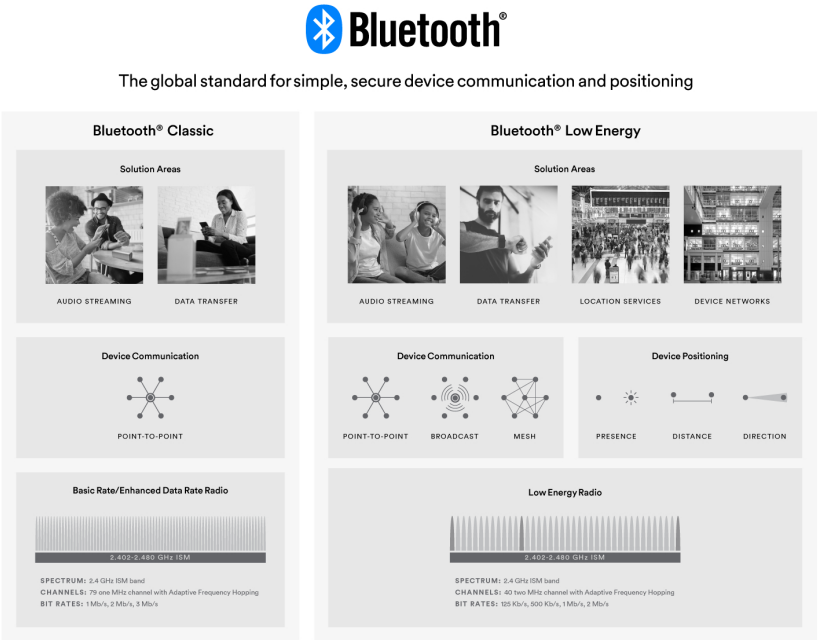


Figure 1: Overview of Bluetooth Technology

To solve this problem we have developed a system to securely store a file of all your passwords. To solve this problem, High Voltage will build a system that will encrypt a file of passwords. The chip on the Adafruit CLUE board is the nRF52840, and Nordic Semiconductor has a cryptography library we could potentially use to run SHA-256 encryption [4]. To access the file a user will have to use their RFID badge which will trigger a decryption of the password

file. Then, using BLE, the clue board will send the requested password to a phone. Now the user can safely view their requested password while keeping it safe from attacks. This allows the user the safety to not have to use the same password for multiple sites, especially since the file is only a tap away from being accessed.

In addition, BLE is capable of sending the file swiftly. According to Bluetooth SIG inc, BLE should have file transfer speeds starting at 125 Kb/sec, which is more than sufficient for reading passwords, as each character is only 1 byte, giving us 125,000 bytes/sec. [5] This can also be seen in Figure 1, which compares Bluetooth Low Energy to Bluetooth Classic.

To be able to complete this project, High Voltage will need parts listed in Table 3. This list of parts will allow our team to solve the problem with all the capabilities shown in the Section III.

Table 3: Parts needed by High Voltage

| Part description | Qty |
|---|---|
| Adafruit Clue | 1 |
| Adafruit DragonTail for micro:bit | 1 |
| AAA Battery Holder | 1 |
| USB Cable | 1 |
| Half Size Solderless Breadboard | 2 |
| Breadboard Jumper Wires | N/A |
| RFID/NFC Breakout Board<br>eg: The Adafruit PN532 | 1 |
| ESP8266 | 1 |

# VI CONCLUSION

Implementing encryption is a great way to protect sensitive data from falling into the wrong hands. Using a combination of hardware and software, we can create a secure system to easily encrypt and access user data, such as passwords. The use of this password manager would provide a great open-source multi-device offline alternative to the current closed source online password managers. In order to mitigate the chances of your accounts being compromised, it is vital to understand the importance of proper password management and avoid the reuse of passwords.

# References


[1] Federal Trade Commission. *Equifax Data Breach Settlement*. URL: https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement. (accessed: 02.21.2023).

[2] Shirley Gaw and Edward W. Felten. "Password Management Strategies for Online Accounts". In: *Proceedings of the Second Symposium on Usable Privacy and Security*. SOUPS '06. Pittsburgh, Pennsylvania, USA: Association for Computing Machinery, 2006, pp. 44–55. ISBN: 1595934480. DOI: 10.1145/1143120.1143127. URL: https://doi.org/10.1145/1143120.1143127.

[3] Bank of North Dakota. *81% of Company Data Breaches Due To Poor Passwords*. URL: https://bnd.nd.gov/81-of-company-data-breaches-due-to-poor-passwords/. (accessed: 02.21.2023).

[4] Nordic Semiconductor. *Cryptography library - nrf$_c$rypto*. URL: https://infocenter.nordicsemi.com/index.jsp?topic=%5C%2Fcom.nordic.infocenter.sdk5.v15.0.0%5C%2Flib_crypto.html&cp=5_4_1_3_11. (accessed: 02.19.2023).

[5] Bluetooth SIG. *Bluetooth Technology Overview*. URL: https://www.bluetooth.com/learn-about-bluetooth/tech-overview/. (accessed: 02.21.2023).

[6] Blase Ur et al. "Do Users' Perceptions of Password Security Match Reality?" In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. CHI '16. San Jose, California, USA: Association for Computing Machinery, 2016, pp. 3748–3760. ISBN: 9781450333627. DOI: 10.1145/2858036.2858546. URL: https://doi.org/10.1145/2858036.2858546.