Password Manager Planning Document

Overview

Stemming from a dissatisfaction in the current state of many of the password management systems that are currently available, the goal of this project is to implement a password management system that keeps user's password data secure, available, and intact. Ideally, this project will result in a more user-friendly presentation while maintaining the highest expectations of standard security practices.

Current Development Team

Matthew Bare — Project Lead/Security Specialist
Worked for the Cybersecurity Education and Research (CEDAR) laboratory for roughly 2 years, and contributed to various research and community outreach projects while there. Enthusiastic about this project and excited to lead the development team.

Tyler O'Dowd — Systems Specialist

Cody Danielson — Database Specialist

Minimum Viable Product:

The minimum viable product for this project is a password management application that has the following features:

- A local database that stores the user's passwords
- A strong encryption scheme that protects the aforementioned database
    - Currently planned to utilize AES-256 for encryption paired with SHA-3 for hashing
- Secure means of authenticating individual users across multiple devices.
    - Currently using Firebase for mobile and web apps
- Syncing of this database across multiple devices
    - Security is paramount here, as such we are researching methodology in delivering this feature in the most secure manner we can.
- Compatibility across many operating systems
    - Currently prioritizing Android, iOS, and chromium based web browsers
        - Desktop client is planned for later development
- Expanded user functionality, including but not limited to:
    - User account management systems
    - User device management systems
    - Updated UI
    - Management systems for the stored password databases

Additional functionality that we would like to add to the project, time allowing, include:

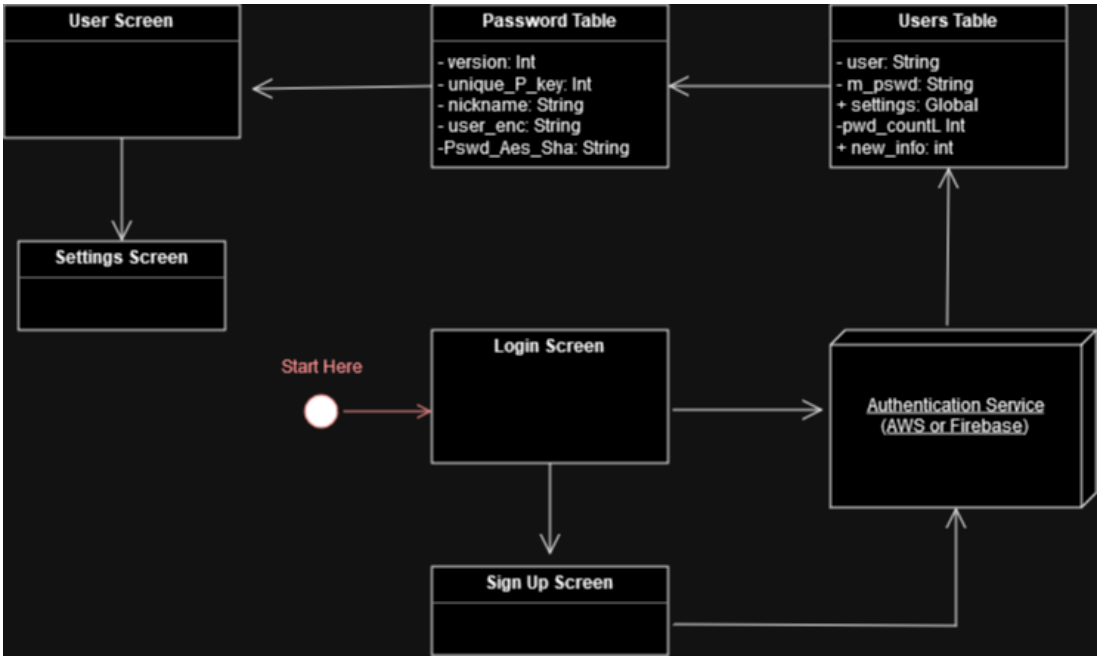
- Allowing multiple users on a single device securely
- Data corruption/loss handling
- Alternative methods of authenticating users
- An automated testing suite
- Database conversion system (version roll-up)
- Alternative methods of syncing tables across devices
- General user quality of life functions, these include but are not limited to:
    - Secure password generation
    - Ability for passwords to expire from the database
    - User password organization features such as grouping or tagging
- Publish the application on platforms such as Google Play or Microsoft Store

System Design:

The password management system is currently planned to span four pages or screens that the user can interact with. These interactions will all be in the form of text submission forms and clickable buttons used to navigate said pages/screens. The planned pages/screens are as follows:

- Login Screen
    - The user will provide their email address as well as a master password to be passed to the authentication system provider.
- Sign Up Screen
    - The user will provide their email address as well as a master password and a confirmation of their master password to register an account with our service.
- User Screen
    - The user screen will populate a list of clickable cards, each representing a stored password within the database. On click, the user's saved password is decrypted and copied to the user's clipboard.
    - This is also where users are able to create new password entries into their password table.
- Settings Screen
    - The user will be able to manage their account and device settings from here.

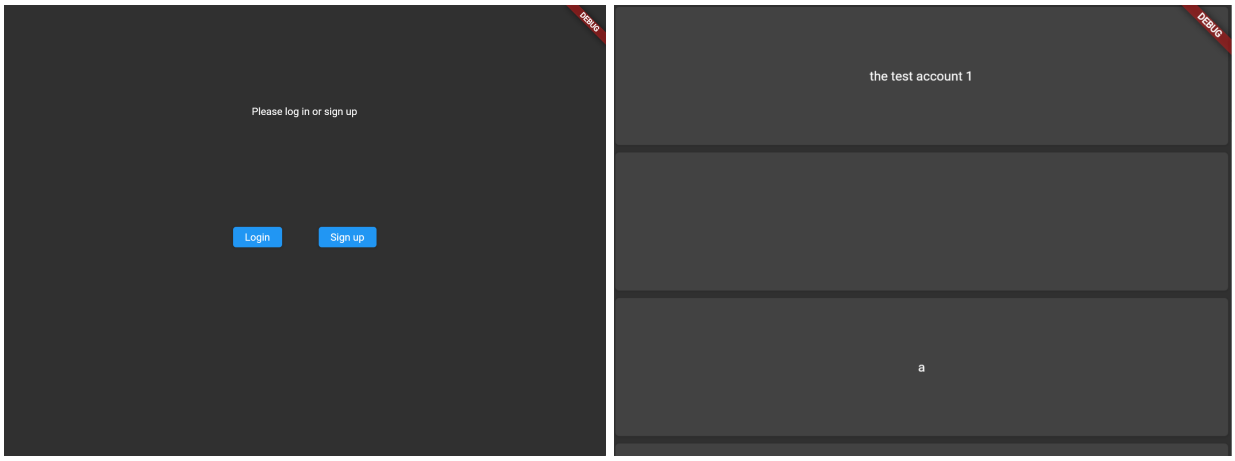
Figure A: a rough traversal diagram of the password management application



As seen in Figure A, this application will require two tables for each user. One corresponding to the user's password data and another corresponding to the user themselves and their account settings. As it is currently planned, each table will be encrypted and stored on the user's device.

In order to keep user interactions within the scope of what is planned for, the UI has been, and will be kept fairly minimal. This is to ensure that the application is both easy to use and easy to develop. Users will only be able to interact with the system through text input fields and clickable widget objects that serve to offer the functionality for the application. That being said, the current UI is bare bones at best, and impedes usability at worst. This will be continually revised and improved at every development milestone.

Figure B: The UI of the application is simple as planned, but simple enough that it impedes usability



Tasking:

Milestone 1: Security Management

- ☐ App keys abstracted to their own file
- ☐ Local database implementation
- ☐ New encryption scheme implementation

Milestone 2: Expand Current Functionality

- ☐ Implement user account settings and management systems
- ☐ OS Compatibility
- ☐ Database management systems

Milestone 3: Syncing

- ☐ Establish secure handshake methodology
- ☐ Implement database sync signaling
- ☐ Implement secure database transfer

Milestone 4: Testing and “If time’s”

- ☐ Collaborate with CEDAR lab for security testing
    - ☐ If needed, revise issues found here
- ☐ Enhance usability wherever possible while maintaining a high standard of security
- ☐ Publish application if at all possible