MOBILE PASSWORD ACCOUNT MANAGER v.1.3.0

Christina M. Restauri
Florida Institute of Technology
CIS 5150 Mobile Applications Design and Implementation
May 1, 2022

Mobile Password Account Manager (MPAM)

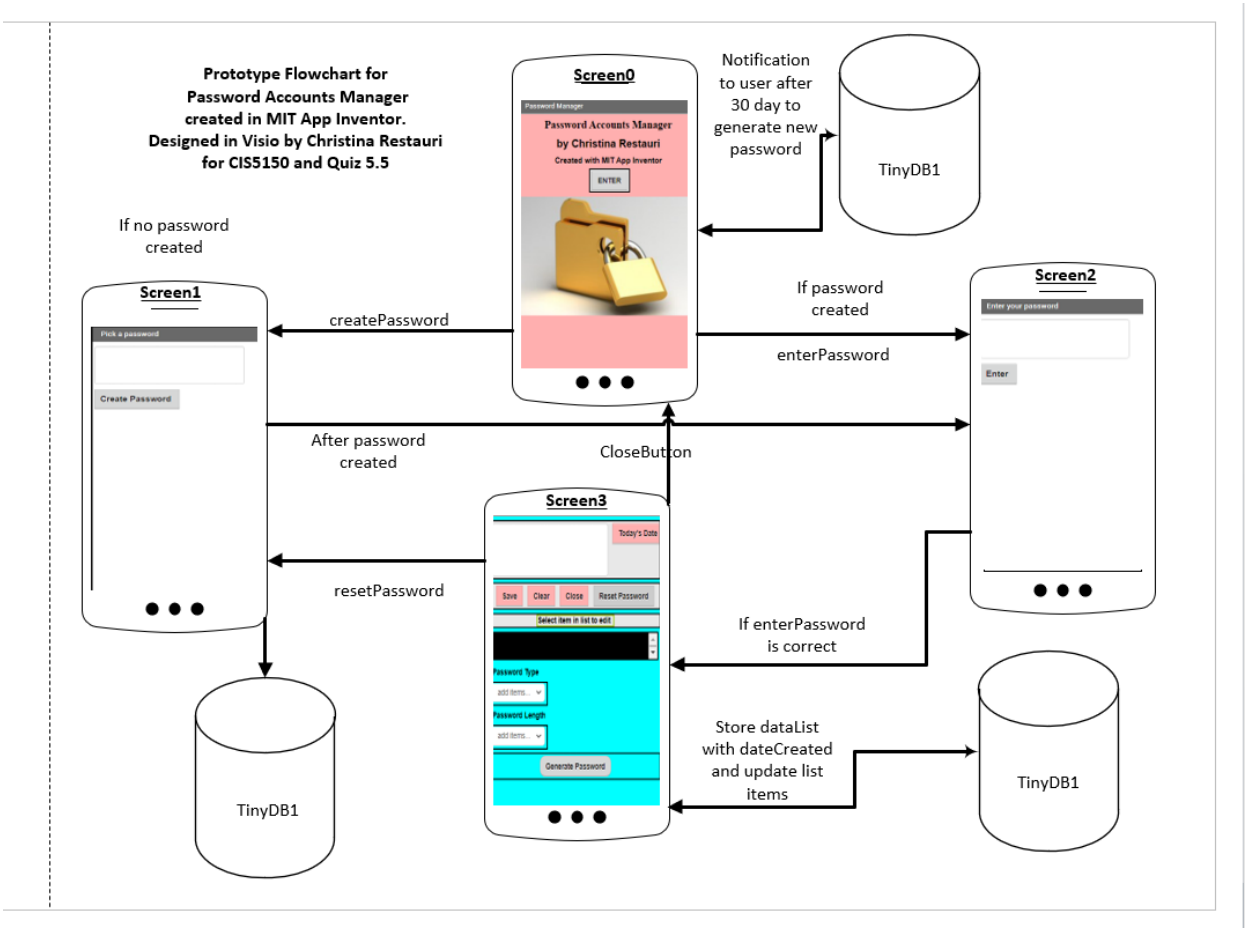
This paper will provide information about the Android Mobile Password Account Manager (MPAM) version 1.3.0 application designed in Android Studio for class CIS 5150 Mobile Applications Design and Implementation at the Florida Institute of Technology. MPAM's version 1.3.0 is the first release with three updated features from the prototype in Figure 1. These features will be identified later in this paper. The objective of this project was to provide a more convenient and better method to store, view, create, and update passwords for all user accounts. The benefits of using passwords to secure our information are in their ability to change and update to avoid attacks like brute force or social engineering. Users should be responsible for modifying and updating their passwords using strict password security policies. However, this is currently still a problem for users because of the number of password accounts they have to keep track of. For this reason, their passwords are usually done with the least of security in mind.

Mobile password account managers are convenient, secure, and more likely to be successful than any other method simply because user's always have their mobile phones with them. That is what makes MPAM a convenient reminder alleviating the work that goes into resetting passwords online. MPAM is simple enough that when the user first opens the application and signs in, they can view all of their passwords with one glimpse without having to go into multiple screens. In these days, reusing passwords are not recommended which makes keeping track of them much more difficult. MPAM stores the password accounts locally so as to avoid risks that may occur in the cloud. Another feature that is being developed is the ability to reset the application without losing all of the information. Additionally, a method to export password account and information from the mobile device to a CSV file via direct connect from the mobile device to the computer.

The tools used to design this MPAM application were mainly Android Studio and Java. However, MIT App Inventor was a valuable tool in prototyping this application's initial design. A visualization of this prototype is presented in Figure 1.

Figure 1

Illustration of MPAM Prototype Structure



Note. The TinyDB1 in this illustration is now Shared Preferences in the modified app created in Android Studio.

The MPAM application begins with a Splash Screen. In the prototype, an initial idea for the design shared by Edjed's Instructables, lets the user enter the application through an "Enter" button. Next the application will display a Create Password screen. If the user has created an initial password, the Create Password screen will not be displayed unless the user wants to reset his password. However, if the user has not created a password, the Create Password screen is the first screen the user sees after the Splash Screen. Once the user has created their password, they will be presented with the Enter Password screen. This screen asks the user to enter their password; if the password is incorrect, the user will receive a notification. If the password is correct, the user will proceed to the next screen, which is the main screen interface of the MPAM application.

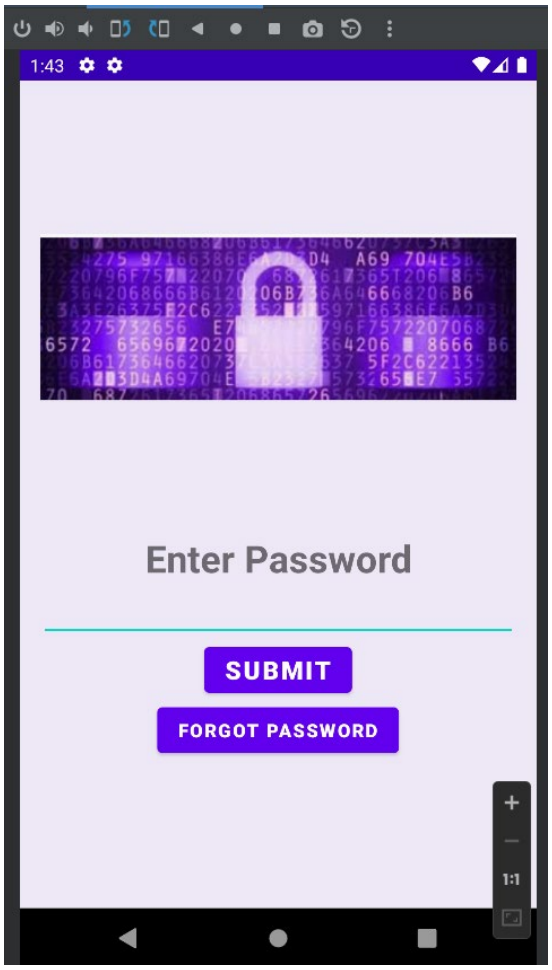
On the main screen of the MPAM application, the user will have the option to create lists for all of their username and password accounts. They can also generate a new secure password, edit existing password accounts, and close the application. A critical aspect of this application is that the user must always enter the date of when the password account was created or updated. This will allow the 30-day notification to be sent to the user to remind them to update their password for security reasons. When the user is finished, they can close the application and their information will be saved and stored in Shared Preferences.

The MPAM uses the Shared Preferences interface to store password accounts persistently throughout the application's lifetime. It does not use the internet or the cloud and is solely for use locally on the user's mobile device. The application is designed to initiate a one-time password to protect it. A forgot password option will allow the user to reset their password if they forget. This function is still in the development process but will provide the user an email or text-based PIN option for password reset without resetting the app and losing all of their stored information. Fingerprint and facial recognition are also in development to add additional secure methods for setting or restoring a password on the application.

Initially, ideas for the design were shared by Edjed's Instructables and Technobytes and used in the preliminary stages. These designs had features that gave the idea for the Mobile Password Account Manager or MPAM. However, these initial designs were prototypes and did not provide the functionality for such things as editing separate accounts, closing the app, selecting accounts for updating, password authentication, a password generator, and a notification every 30 days to update the user's password. These features have been added or are being added to the design, like the forgot password feature and the 30-day notification. Careful considerations are being evaluated for the password reset option when users forget their passwords. An early objective was not to overwhelm the user with a complicated interface when the user forgets their password. Such is the simplicity of a note reminder application which gave way to the MPAM's design. The concept is that users are more likely to avoid password managers and write their passwords down or try to remember them, making the forgot password reset option a significant feature. Users are easily frustrated when forgetting their passwords making them less likely to use password managers. Other considerations like a password hint option are also being made available to provide convenience from having to reset the password. See the current design of the Enter Password screen in Figure 2 below.

Figure 2

Illustration of MPAM Enter Password Structure



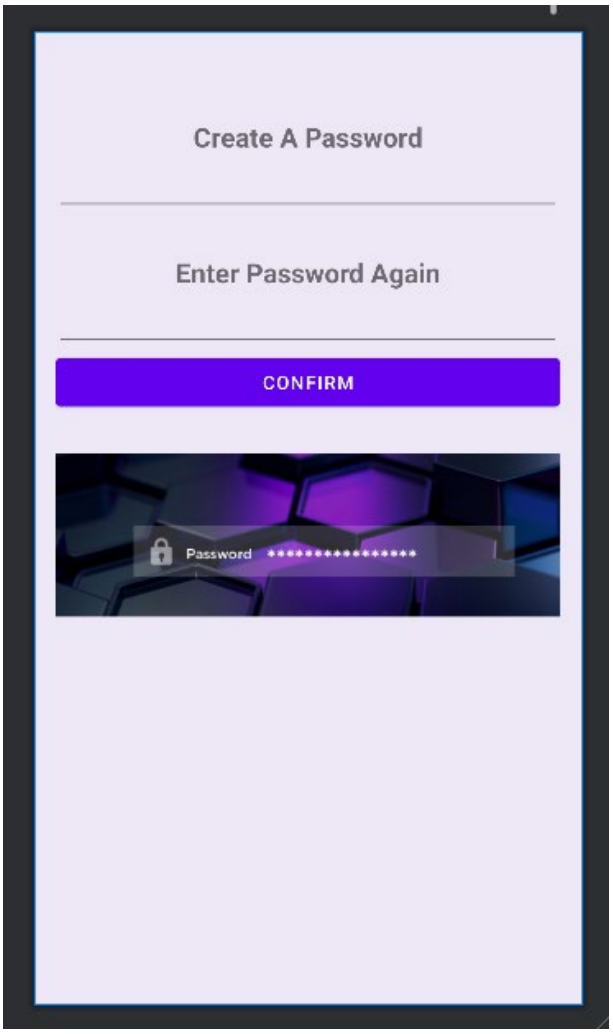
Note. The hint for the user to remember their password is in the process of being added to this screen as well as the forgot password feature.

The above Enter Password screen only requires the user to enter and remember a master password which is why password managers were developed. They relieve the trouble of having to remember many different passwords and make available to the user their entire password database (Agholor, et al., 2016).

Unlike the Enter Password screen on the prototype, this Enter Password screen looks different and there are future plans that will include other options. One of them will be a user hint as well as a choice to sign in with their fingerprint or facial recognition if one was created at the beginning. Those options will be included when the user first sets up their password on the Create Password screen in Figure 3.

Figure 3

Illustration of MPAM Create Password Structure

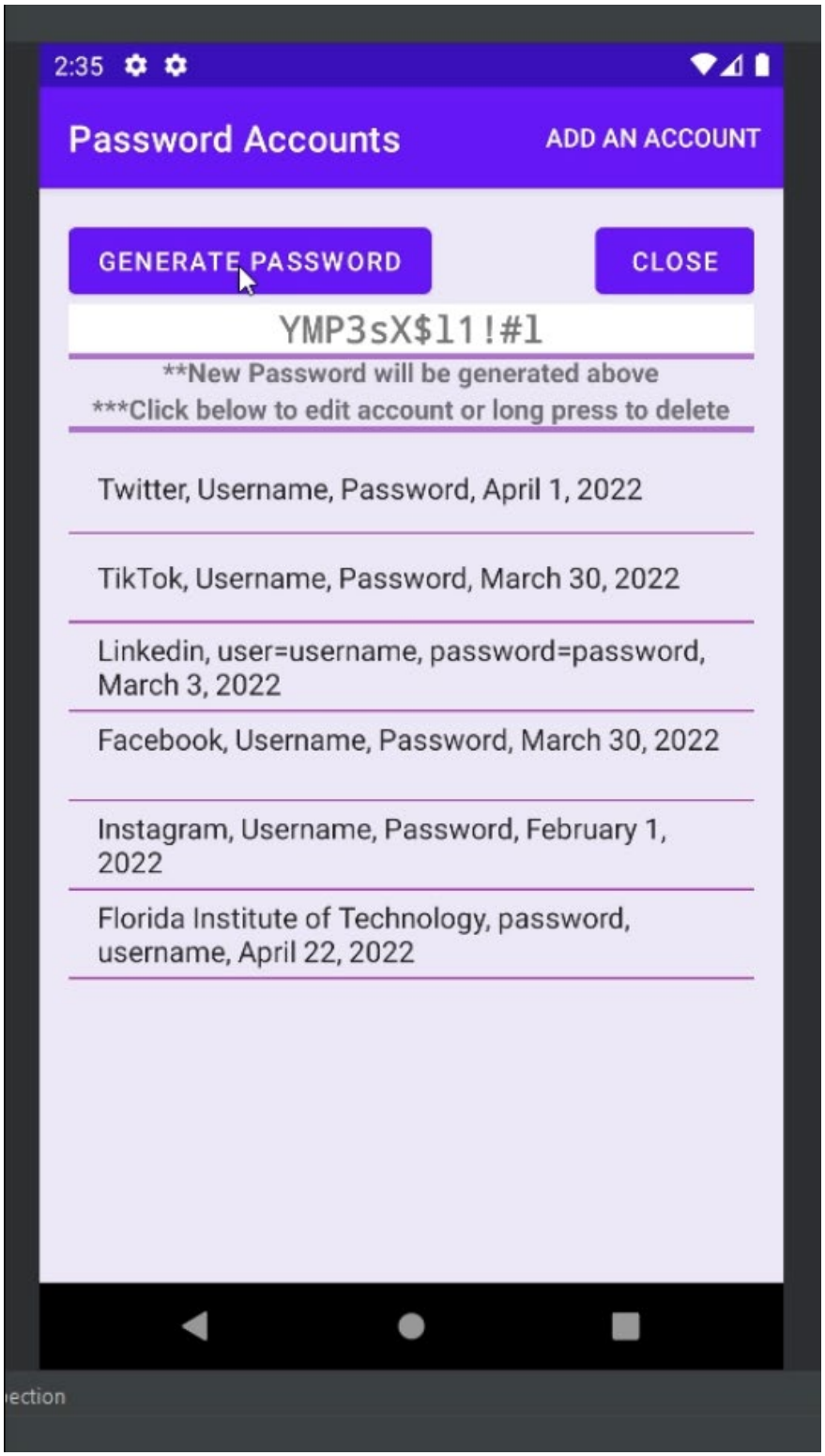


Note. This screen will include the setup for the user's password, password hint, fingerprint, and facial recognition as well as email and pin registration.

The ability to offer users various means of password authentication will enable more security methods and give user's more options for signing in or resetting their passwords. The security of passwords is their ability to change which is why a secure password generator was added to the application and can be seen in Figure 4 of the main screen.

Figure 4

Illustration of MPAM Main Interface Structure



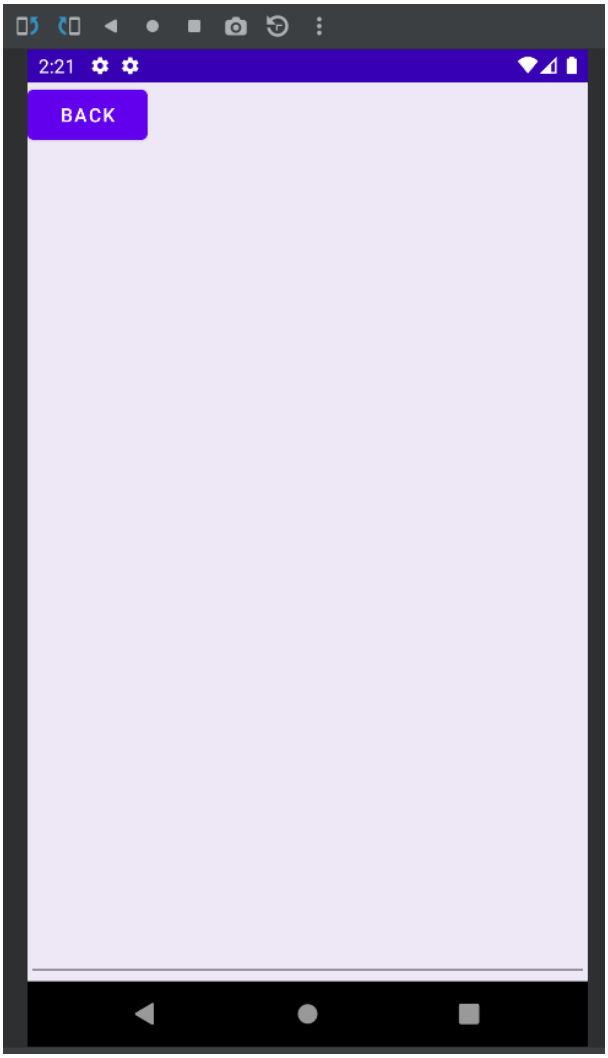
Note. This screen will have additional designs added for adding account information.

In figure 4, a generate password button allows the user to generate passwords based on the latest security principles. The user can then copy and paste their newly generated password into their password account and update the calendar date. The generate password feature was previously updated from the prototype in Figure 1.

This MPAM application also provides a separate screen when users add a new account or update their existing account. The screen in Figure 5 provides the user with editing and creating their account information.

Figure 5

Illustration of MPAM Create and Edit Interface Structure



Note. This screen will have additional design functions as well as a calendar picker.

The Add an Account and edit page were previously updated from the prototype in Figure 1 to enable adding and editing password accounts as well as a button to take the user back to the main password account screen. Whenever this happens all information is automatically saved to Shared Preferences on the device. This screen's date entry for created passwords will most likely change to provide a calendar picker which is an enhanced method for users to set dates and provide the basis for the 30-day notification.

The MPAM application is fully functional and can be used to store password accounts, edit the accounts, add the accounts, generate new passwords, and close the application. Future improvements are in the process and will include but are not limited to:

Additional features:

1. Password protection using encryption technology
2. Email and text-based PIN reset password options
3. Fingerprint and facial recognition for login and password reset
4. Multifactor authentication capability
5. Notification alarm every 30 days to update user's passwords
6. More robust design and features for the account information screen

MPAM is in the beginning phases; however it is working properly or as intended with no bugs to date. As of this date, MPAM is continually being tested and documentation will be provided to users as versions or patches take place. The application is meant for mostly personal use to provide users the benefit of storing their password and having a safer and more convenient way to keep track of their personal password accounts and any information regarding their password accounts.

References

Agholor, S., Sodiya, A.S., Akinwale, A.T., Adeniran, O.J., & Aborisade, D.O. (2016). A Preferential Analysis of Existing Password Managers from End-Users' View Point. International Journal of Cyber-Security and Digital Forensics (IJCSDF). The Society of Digital Information and Wireless Communications (SDIWC). https://www.researchgate.net/publication/322006671_A_Preferential_Analysis_of_Existing_Password_Managers_from_End-Users'_View_Point.

Developers. (2022). Android Studio. https://developer.android.com/studio.

Edjed's Instructables. (2022). How to Use MIT App Inventor to Make a Secret Notepad App for Android. https://www.instructables.com/How-to-Use-MIT-App-Inventor-to-Make-a-Secret-Notep/.

MIT App Inventor. (2021). Create Apps! https://appinventor.mit.edu/.

Technobyte. (2022). Create a Notes App in Android/.