Topic: *Password Manager and Generator for Mobile Devices*

Author: *Diego A. Santiago Uriarte*

Date *8/26/2022*

Problem Background

- *An increasing number of platforms require users to create accounts with usernames and passwords and additional information; This leads to People losing track of their usernames and or passwords constantly.*
- *Having to constantly reset their user information can be very inconvenient and in some cases causes users to lose access to their accounts completely.*
- *Current Password Management systems exist in servers containing encrypted information; the security of this sensitive information is highly developed but not 100% guaranteed and people aren't trusting of third party companies to manage their sensitive information.*
- *More than 80 percent of U.S. companies indicate their systems have been successfully hacked in an attempt to steal, change or make public important data.*
- *People make their passwords easy to remember which results in passwords being more easily cracked.*

Target

- *The Goal to be achieved is to develop a mobile application both on iOS and Android devices that stores all the sensitive account information from various platforms securely and completely locally.*
- *This application will involve a very sophisticated and user friendly GUI to generate complex credentials and manage all the usernames and respective passwords alongside any additional information.*
- *This application would be completely free and open source*

Causes

Problem: Users don't have strong and or secure login credentials They also do not have a way to store their **many** usernames and passwords in a single digital space which they can trust.

Why: User forget their passwords constantly if it is too complex, thus they choose simpler passwords.

Why: Users choose simple passwords as to not forget them which causes them to be less secure and often repeat the same credentials for multiple platforms.

Why: Simple passwords are much more easily stolen or hacked than complex passwords. Despite this people don't use any digital service to store all their usernames and passwords

Why: Users are not very trusting of third party companies to store their sensitive information.

Why: Servers, although they offer high-level encryption are more likely to get hacked than any one specific user.

Countermeasures

- Develop Password Generator for optimizing the security of account information if the user desires to create new credentials.
- Use case specific ASCII symbols for passwords with specific requirements.
  Example: A password that must contain 1 capital letter, 1 lowercase, and 1 special symbol
- Categorize credentials in specific categories such as social media, streaming services, banking information and establish different levels of security depending on the specific category.
  Example: *social media requires only a pin to access, streaming services requires a password and banking information would require the highest level of authentication such as Facial Recognition alongside sending a code through email to validate access.*
- *Implement copy to clipboard functionality for easy copy and paste use*
- *Implement these features in a user friendly and visually aesthetically pleasing mobile application so the user doesn't have to struggle with using a complicated framework.*

Check/Evaluate

- Users will use this app to keep track of passwords for multiple platforms such as social media, streaming services, and more
- To keep track of the efficiency of application, each time a passwords is deleted or updated the application will prompt the user to submit the reason why
- The success of the app will be measured in how many times credentials are changed and why

Act/Standardize

- Based on these user surveys / reports the application can be optimized accordingly, to prevent the issues that merit the use of a password manager in the first place.
- Simple levels of encryption to reduce any security risks.
- Include support in Android and iOS devices