PEI - Milestone 3

FreePass - A Random and Replicable Password Manager

1. Introduction

In our last milestone we discussed and defined our system requirements and architecture, since then we have been working to create prototypes of the programs we want to include in our project. The main programs we have been working on are a password generating algorithm; a chromium browser extension and an android mobile application. In order to better organize our work we decided to elect project leaders for each program. We still work collaboratively in every part of the project, but the leader oversees most changes in their respective program and ensures everything is working according to the plan we previously agreed on. In the next section we will discuss each program's prototype progress in depth.

2. What we've done so far

2.1. Password Generating Algorithm

Making this algorithm was relatively easy because of the help of our supervisors and their guidance to other projects. That said, we still found some issues namely how we could use the user inputs to generate a better and stronger password. This specifically happened with the workbench input that we found hard to introduce in the generating part of the algorithm but after discussing with the supervisors we were able to resolve the issue.

2.2. Android Mobile App

To develop the project's android mobile app we decided to use Android Studio as the development environment, we made that decision because it is a widely used, very robust and user-friendly tool. Even though Android Studio has all those advantages it still has a learning curve, however the team member that was elected this program's leader already had some experience with it so we were able to mitigate some of the initial hardships we would normally find with any new programming environment.

The android app includes three text fields where the user can enter a website's URL; their username and a master password; they are also given the option, presented in the form of checkboxes, to exclude lowercase; uppercase; numbers and symbols from the generated password. They are also required to indicate the desired length of the generated password and how many times he changed it in the form of a counter. Lastly after the password is generated the user has the option to reveal it, as it originally appears censored, and to copy it to their phone's clipboard.

At the moment the prototype does the most basic but most important functions required, it receives inputs from the user, generates a password based on those inputs and allows the

user to reveal and copy it. The checkbox options, the length selector and counter are still not working as intended because of unexpected bugs.

2.3. Chromium Browser Extension

All that's been done on the extension so far is mostly related to the layout and its visual aspect. The extension contains a form with the same fields as the Android App, where the website URL is automatically collected, since it's possible to verify which website the user is currently navigating.

No other functionality is currently implemented.

3. Future Work

3.1. Password Generating Algorithm

For our future work for the algorithm we want to make the generated password more customizable for the user. We also need to make our code more secured for false or bad inputs from the user.

3.2. Android Mobile App

In the future we will make the already mentioned password generating options functionable, add a workbench option and also have the option to log in into an account so that the user will be able to save his non-password credentials between uses and devices. Lastly we also have some tasks with lower priority like making the app be compatible with older android devices and multiple screen sizes.

3.3. Chromium Browser Extension

Eventually, the extension will be able to generate a password based on all the input fields. Similarly to the App, it will be able to save non-password credentials. Apart from that, we want it to automatically detect if there's a login form in the page the user is browsing and prompt the user with the Password Generating Form, possibly with the non-password credentials already loaded.

4. Contacts

- João Morais
  - 93288
  - antoniojoao10@ua.pt

- Miguel Ferreira
  - 93419
  - migueltf@ua.pt

- Pedro Coutinho
  - 93278
  - pmacoutinho@ua.pt

- Pedro Paixão
  - 73227
  - pedropaixao@ua.pt