SE 3XA3: User Guide
PasswordProtectionProgram

Team 28, Tuples1
Suhavi Sandhu (sandhs11)
Shabana Dhayananth (dhayanas)
Joseph Lu (luy89)

November 28, 2017

Contents

List of Tables

List of Figures

Table 1: **Revision History**

Date	Version	Notes
2017-11-26	0.0	Creation

1 General Information

1.1 Brief System Overview

PasswordProtectionProgram (PPP) is an application that acts as an encrypted password manager, wherein a person can safely store and access all of the passwords they use with a single master password. The user's information is encrypted with a unique hash value and saved to a database. The application is intended for offline use on Windows, Linux OS and and OSX.

1.2 Document Overview

This document contains four sections: General Information, System Summary, Getting Started, and Using The System. The template used to create this document can be acessed here (1).

The current section, General Information outlines the purpose of the software and the breakdown of the user manual. The System Summary gives an overview of the software and hardware configurationsfor the system as well as user access levels. The next two sections , Getting Started and Using the System explain how to install the software and how to access all of its functions, respectively.

2 System Summary

2.1 System Configurations

PasswordProtectionProgram can be used on desktop computers that use Windows, OSX and Linux OS. The application will be available for download as an executable file containing all necessary software dependencies, such as the Python libraries: cryptography, peewee, tkinter, pyperclip. After running the executable file, the product will be immediately ready for use.

2.2 User Access Levels

All users that download the application onto their computer and create a password protected account are able to use the application. However, only one master account can be created per downloaded system and thus only one individual can use the software per computer.

2.3 Contigencies

The system in completely offline so all dependent account details are saved into an offline database stored and accessed on the operating device. In the case of power outage or hardware failure, there is no backup created and all data could be lost.

3 Getting Started

3.1 Installation and Logging In

The PasswordProtectionProgram software is currently available to be downloaded at (URL HERE). When the .exe file is run, the application should open up to a one time only master password creation screen. The user is to create a password based on the security recommendations provided by the system and this password will be used for all future log ins to the system. As there is only one user per application download, a username is unnecessary.
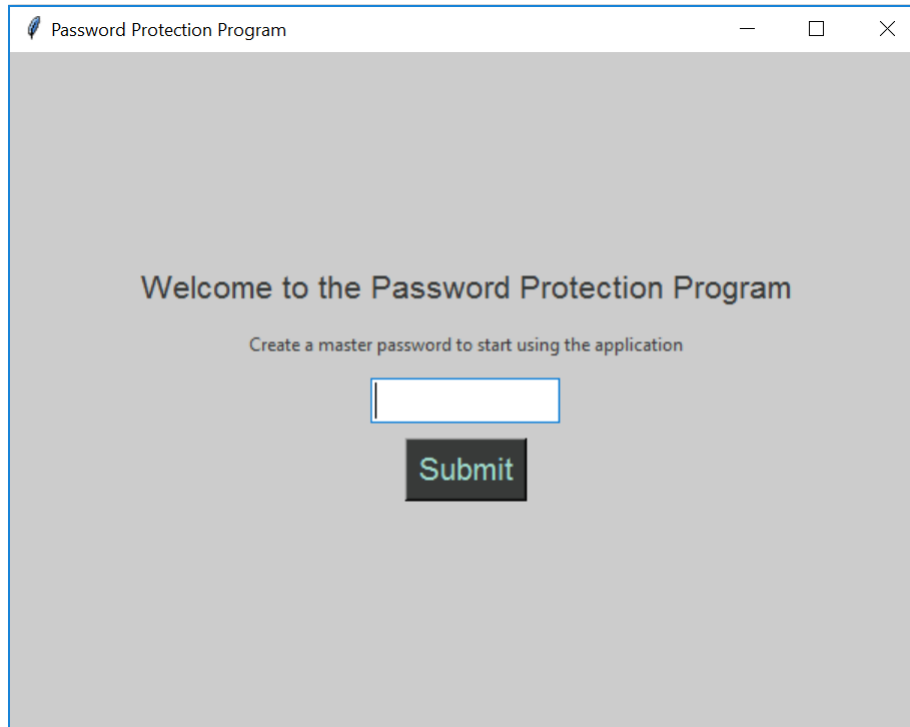

Figure 1: Create Master Password Screen

For all subsequent use of the product, the initial entry screen will only require entry of the aster password as shown in the following image.
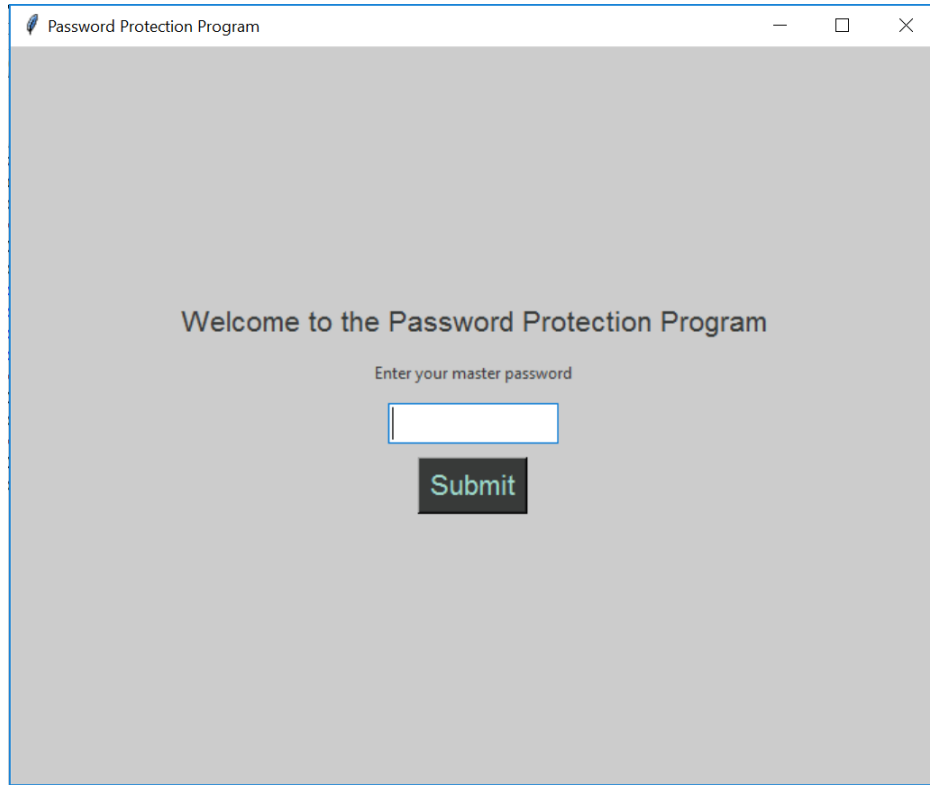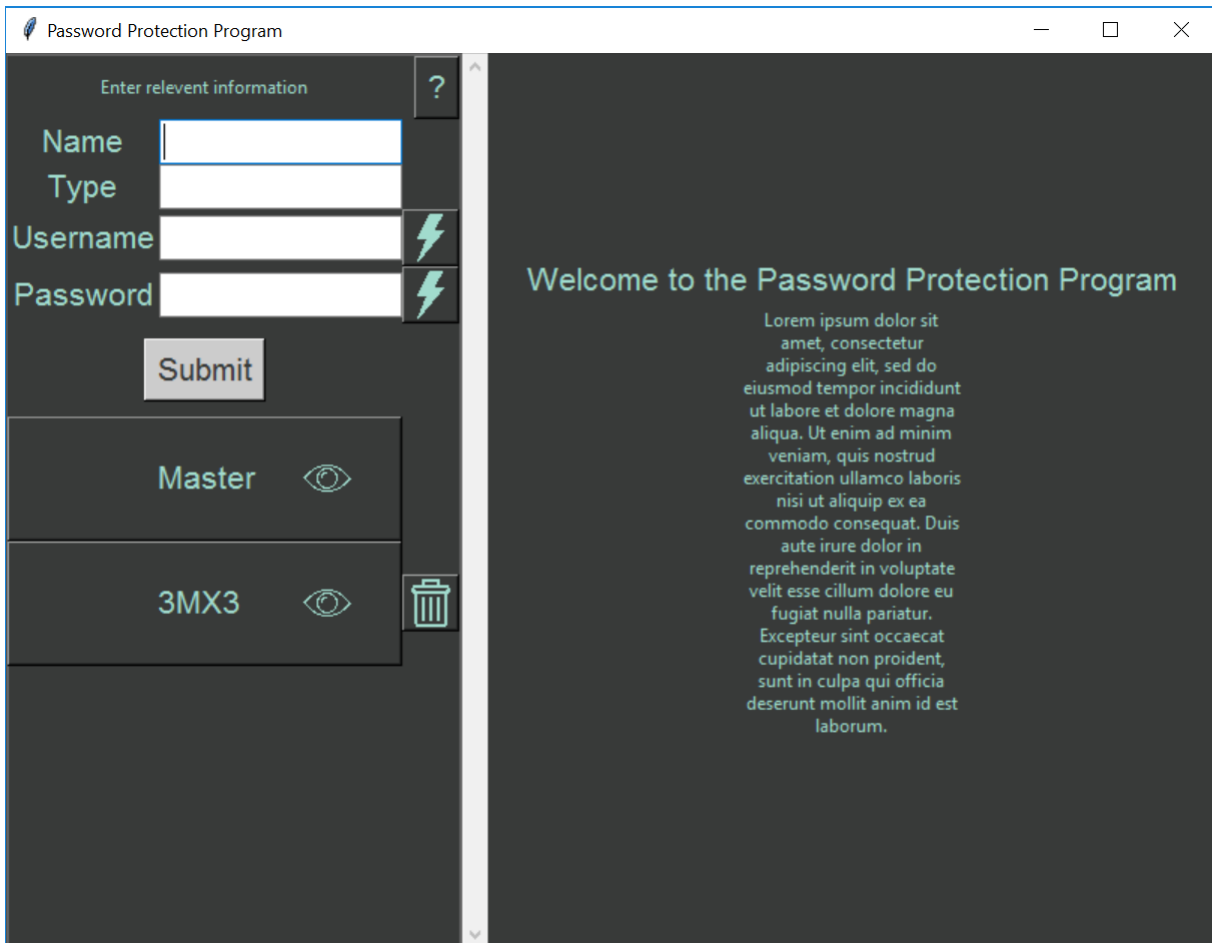

Figure 2: Enter Master Password Screen

3.2 System Menu

After creating a master password or logging into the system, the user is lead to a screen that in the center displays a brief description of the application. In the top left corner, the user is able to add new account usernames and passwords to the password manager by specifying the account name, type, username and password. Below this, starting with the master password, all the accounts for which the user has already saved a username and password are listed.

Figure 3: In Application Screen

3.3 Changing Master Password

If the master password that was initially set for the software needs to be changed, this can be done so by choosing the master password box on the left side of the in-application screen.
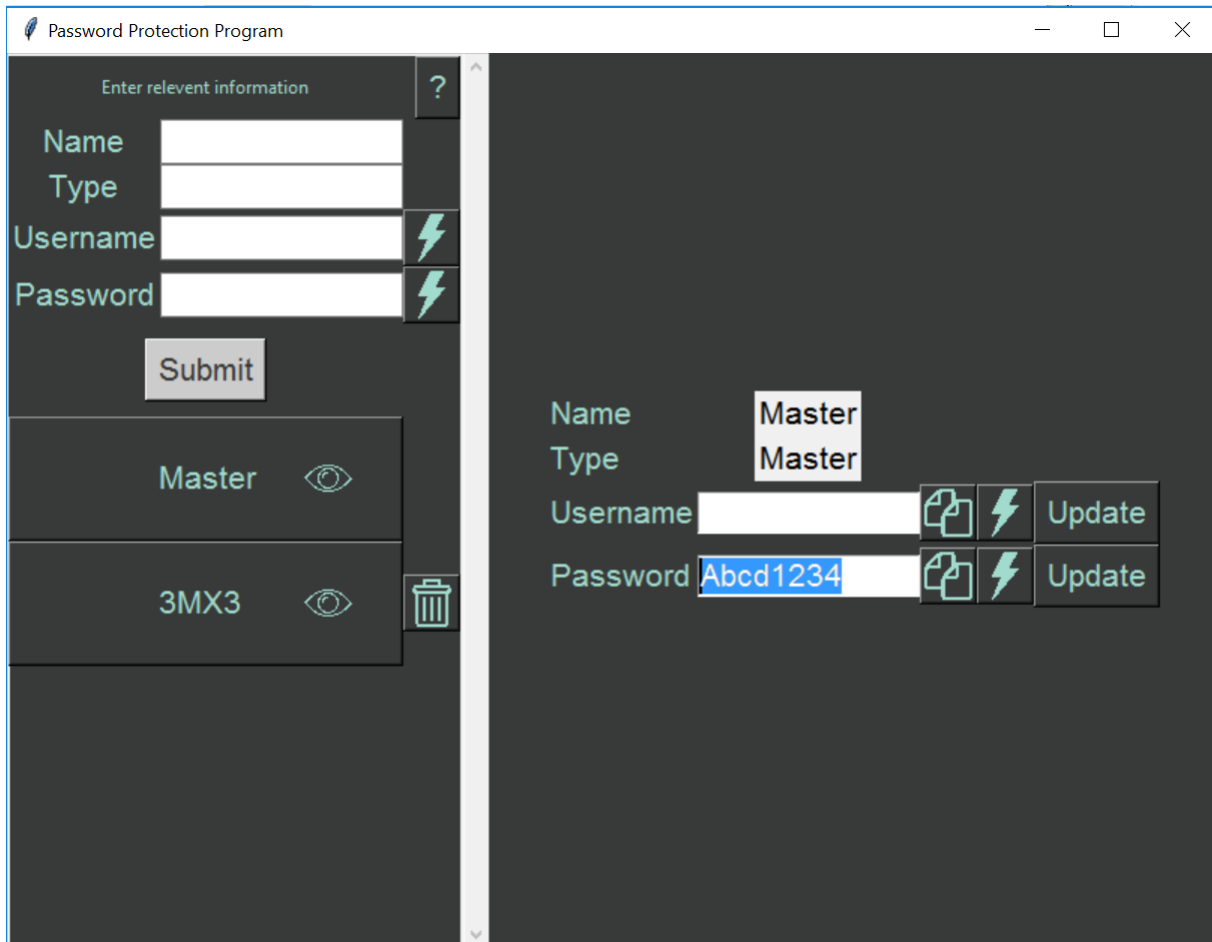

Figure 4: Changing Master Password

3.4 Exit System

The system can be exited by simply closing the application window as this automatically logs the user out as well. The application will also close after TIME AMOUNT of inactivity in order to preserve the security of the data.

4 Using the System

4.1 System Functions

4.1.1 Add Entry

An account entry can be added to this password manager by filling out the required entry fields specified in the top left corner of the in-application screen. The name of the entry will be used as a unique identifier for this entry account's information, the type is used for organization purposes and the username and password are those that the user has already associated with the specific account.
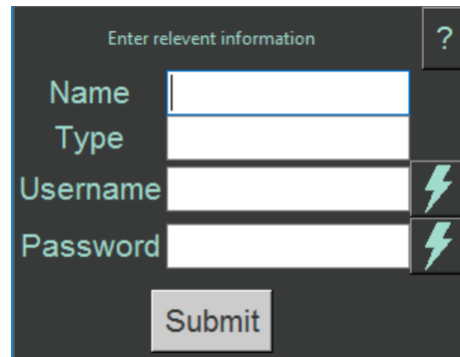

Figure 5: Adding an Entry

4.1.2 View Entry

Once an entry has been added, it will be listed for viewing as a button in the menu on the left of the in-application screen. The entries are ordered from least recent to most recent entry, starting with the master password. The entry name is displayed on the button along with an eye sympbol to indicate the account that it is associated with.
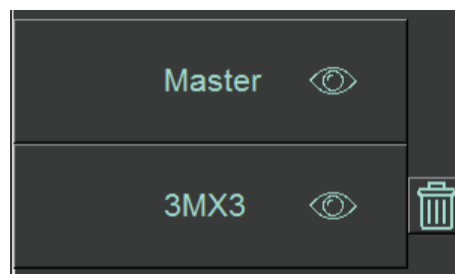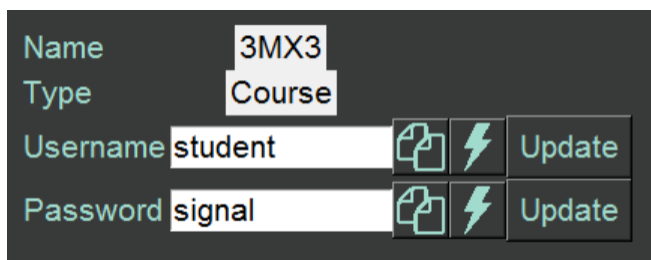

Figure 6: Button to View an Entry

After the button is clicked, all of the account information will be displayed in the center panel of the screen along with buttons for additional functions such as Copy, Generate and Update.

Figure 7: Viewing an Entry

4.1.3   Delete Entry

An entry can be deleted at any time using the delete button located beside each account lising in the menu on the left of the screen. Obviously, the master password can not be deleted.

Figure 8: Deleting an Entry

4.1.4   Update Entry

An entry can be modified after it is selected in the menu and the information is displayed on the screen. Only the username and password for the selected account can be modified, if the user wishes to change the name and type of the account, the account must be deleted and recreated. After the desired fields are altered, to save these changes, the user must press the Update button located beside each field.
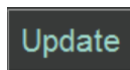

Figure 9: Updating an Entry

4.1.5   Copy Field

The copy button located beside the username and password fields is used to facilitate entering authentication information into the service the user wishes to use. The decrypted passoword or username is copied directly to keyboard when the corresponding copy button is pressed.

Figure 10: Copying a Field

4.1.6 Generate Field

The generate button, denoted by a lightning bolt, provides the user with a random, cryptographicaly sage 8 charater string consisting of upper and lower case alphabets and numbers. The user can use this generated value for their account if they wish.

Figure 11: Generating a Username or Password

4.1.7 User Manual

If at any time the user is unsure of the function of a button, a user manual will be linked to the question mark button located on the top left corner of the in-application screen beside the add a new entry section.

Figure 12: Accessing the User Manual

4.2 Inactivity Timeout

As PasswordProtectionProgram is a password manager, the primary concern of the application is the security of the user information. Therefore, the system is equipped with an automatic logout function when 2 minutes of inactivity is detected. In this way, the application is not left open when the user is not present and this prevents individuals other than the user from accessing the information.

4.3 Special Instructions for Error Correction

TENTATIVE: In the case that the master password is forgotten, the system has a "forgot master password" button that when pressed will reset the application to the state it was when first downloaded. Thus, all saved data will be lost and a new master password will have to be created.

References

[1] "User's manual," 2002.