LAB 11 : Authentication and Account Management

1. Download and Install a Password Management Program

The drawback to using strong passwords is that they can be very difficult to remember, particularly when a unique password is used for each account that a user has. As an option, password management applications allow the user to store account information such as a username and password. These applications are themselves then protected by a single strong password. One example of a password storage application is KeePass Password Safe, which is an open source product. In this project, you download and install KeePass.

Instructions:

1. Use your Web browser to go to keepass.info and then click Downloads
2. Under Downloads, locate the most recent portable version of KeePass and click it to download the application. Save this file in a location such as your desktop, a folder designated by your instructor, or your portable USB flash drive. When the file finishes downloading, install the program. Accept the installation defaults.
3. Launch KeePass to display the opening screen.
4. Click File and New to start a password database. Enter a strong master password for the database to protect all of the passwords in it. When prompted, enter the password again to confirm it.
5. Click Edit and Add Entry. You will enter information about an online account that has a password that you already use.
6. Under Group, select an appropriate group for this account.
7. Enter a title for this account under Title.
8. Under Username, enter the username that you use to login to this account.
9. Erase the entries under Password and Repeat and enter the password that you use for this account and confirm it.

10. Enter the URL for this account under URL.
11. Click OK.
12. Click File and Save. Enter your last name as the filename and then click Save.
13. Exit KeePass.
14. If necessary, navigate to the location of KeePass and double-click the file KeePass.exe to launch the application.
15. Enter your master password to open your password file.
16. If necessary, click the group to locate the account you just entered; it will be displayed in the right pane.
17. Double-click under URL to go to that Web site.
18. Click KeePass in the taskbar so that the window is now on top of your browser window.
19. Drag and drop your username from KeePass into the login username box for this account in your Web browser.
20. Drag and drop your password from KeePass for this account.
21. Click the button on your browser to log in to this account.
22. Because you can drag and drop your account information from KeePass, you do not have to memorize any account passwords and can instead create strong passwords for each account.
23. Close all window.

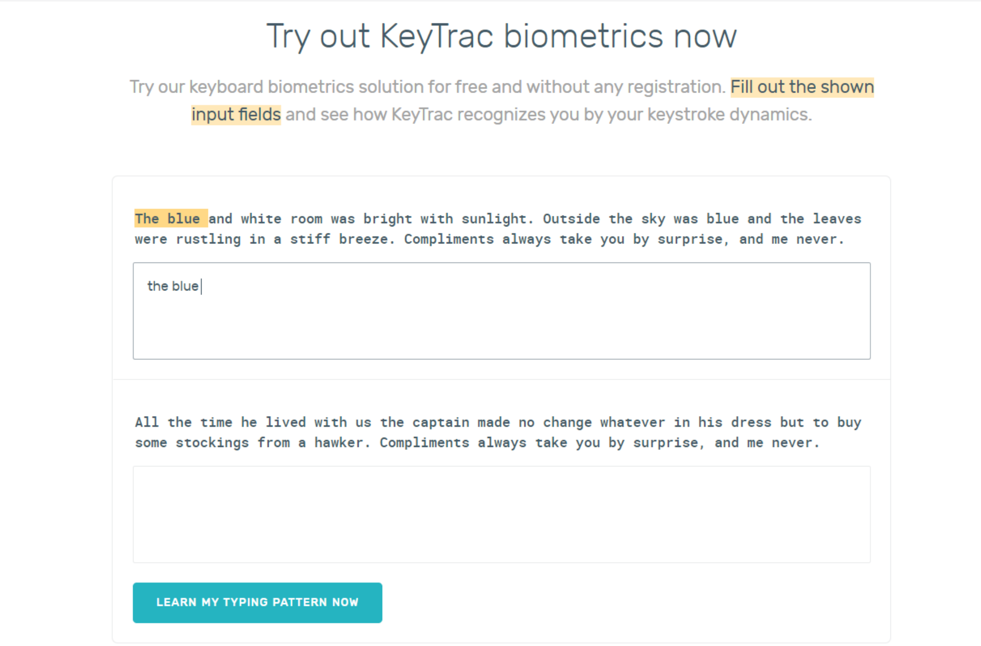
1.1 In your opinion, is this application can help users create and use strong passwords?
1.2 What are the strengths of these password programs?
1.3 What are the weaknesses?
1.4 Would you use KeePass? Why?

2. Keystroke dynamics

One type of behavioral biometrics is keystroke dynamics, which attempts to recognize a user's unique typing rhythm. In this project, you will use Keytrac to detect users based on their keystroke dynamics.

Instructions:

1. Use your web browser to go to https://keytrac.net
2. Go to "Try Out" tab. Fill out the shown input fields.



Try out KeyTrac biometrics now

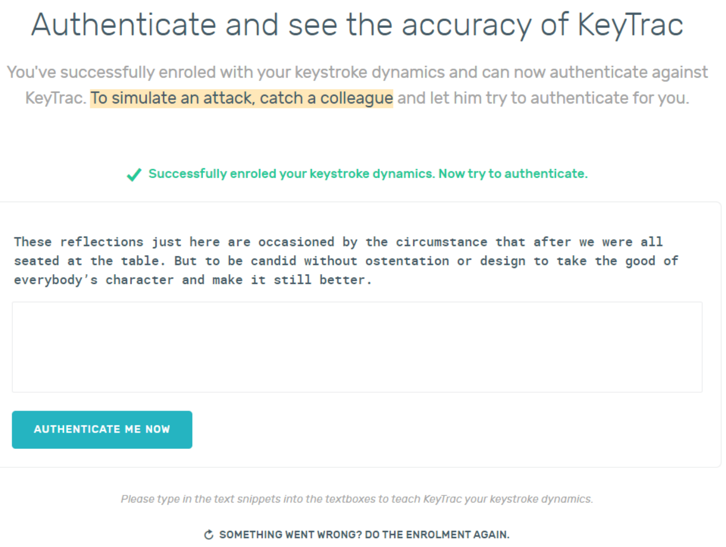
Try our keyboard biometrics solution for free and without any registration. Fill out the shown input fields and see how KeyTrac recognizes you by your keystroke dynamics.

```
The blue and white room was bright with sunlight. Outside the sky was blue and the leaves
were rustling in a stiff breeze. Compliments always take you by surprise, and me never.
```

the blue

```
All the time he lived with us the captain made no change whatever in his dress but to buy
some stockings from a hawker. Compliments always take you by surprise, and me never.
```

3. Click “Learn My Typing Pattern Now”.
4. Authenticate your keystroke by fill out the input fields.



Authenticate and see the accuracy of KeyTrac

You've successfully enroled with your keystroke dynamics and can now authenticate against KeyTrac. To simulate an attack, catch a colleague and let him try to authenticate for you.

✓ Successfully enroled your keystroke dynamics. Now try to authenticate.

```
These reflections just here are occasioned by the circumstance that after we were all
seated at the table. But to be candid without ostentation or design to take the good of
everybody's character and make it still better.
```

Please type in the text snippets into the textboxes to teach KeyTrac your keystroke dynamics.

5. Click “Aunthenticate Me Now”
6. Your score will be displayed.
7. Try again by letting other person authenticate for you.

2.1 What do you understand after using KeyTrac?
2.2 What does it mean if the score is 100%?
2.3 What does it mean if the score is 50%?

3. Use Cognitive Biometrics

Cognitive biometrics holds great promise for adding two-factor authentication without placing a tremendous burden on the user. In this project, you will participate in a demonstration of Passfaces.

Instructions:

1. Use your web browser to go to www.passfaces.com/demo.
2. Under First Time Users, enter the requested information and then click START THE DEMO.
3. Click Start the Demo.
4. Accept demo as the name and then click OK.
5. When asked, click NEXT to enroll now.
6. When the Enroll in Passfaces dialog box displays, click NEXT.
7. Look closely at the three faces you are presented with. After you feel familiar with the faces, click NEXT.
8. You will then be asked to think of associations with the first face (who it looks like or who it reminds you of). Follow each step with the faces and then click NEXT after each face.
9. When the STEP 2 Practice Using Passfaces dialog box displays, click NEXT.
10. You will then select your faces from three separate screens, each of which has nine total faces. Click on the face (which is also moving as a hint).
11. You can practice one more time. Click NEXT.
12. When the STEP 3 Try Logging On with Passfaces dialog box displays, click NEXT. Identify your faces, and click NEXT.
13. Click DONE and click OK.
14. Click Try Passfaces and then click Logon.
15. Click OK under the username and identify your faces.
16. Close all windows.

3.1. Is this type of cognitive biometrics effective? If you came back to this site tomorrow, would you remember the three faces?

4. Create an OpenID Account

Instructions:

1. By conducting online research, explore any OpenID Account.

4.1. What is an OpenID Account? List the example of OpenID Account.

4.2 What is the advantages of OpenID Account?

4.3 What is the advantages of OpenID Account?