File Protection System using Multifactor Authentication

Introduction

There has been quite a number of challenges by PC users to restrict file access on their PC to certain users based on the privileged information that should be accessible. Often time, irrespective of how well the files are being masked in subfolders, unauthorized users still find their way to open these documents. Consequently, a file protection system is developed to address this concern

Project Objectives

1. Restrict access of important files to privileged users
2. Implement a 2FA system to open sensitive documents on a user’s PC
3. To use an OTP and password system to validate a user’s access to a file

Project Scope

1. Filesystems on Windows Operating System
2. Filesystems on Linux OS (Ubuntu, Fedora, Red hat, CentOS)
3. The use of python 2.7 /python 3.6
4. Google SMTP server in TLS mode

Project Procedures

1. A modular approach was adopted in the planning, design, development and testing of the project before deploying.
2. A user registration and storage system were developed to register new users by saving the username, email and hashed password in a file (Adhoc storage repo)
3. The user login module was also built after the completion of the user registration system. This system performs a check of the stored username and password in order to conduct a first level authentication of a user
4. An OTP generation function is enmeshed in the user login module which computes a 6 digits One Time Password (OTP) if the password condition of the user is being met
5. Subsequently, the OTP system triggers a mail server to deliver the OTP to the user’s email address which is linked to the identity of the user while creating the account
6. The OTP is received by the user in less than 15 seconds also factoring the internet connection of the PC where the program Is being tested.
7. A second level authentication is executed when the user enters the received OTP value which is compared by the system to what was generated within that session
8. Once the above is true, the protected file is opened

9. There are several conditions that have been integrated into the system which returns an error message for the user trying to access a file as detailed below:
   - If a user decides not to login
   - If a new user uses an already taken username
   - If a user enters a username not found in the authentication file (server)
   - If a user trying to login uses an incorrect password
   - If a user enters an incorrect OTP
   - If a user fails to adhere to the instruction of using character “Y” or “N” to determine their intention to proceed or not

Results & Discussion

After extensive work on all the respective modules and finally integration, the file protection system using 2FA was finally completed. A user can successfully create an account, login and receive a 6 digits code in order to access a privileged file. The time taken to execute the program is less than a minute and approximately 15 seconds to obtain receipt of the 6 digits OTP.

Summary & Conclusion

In accordance to the stipulated project section above which follows a defined sequence pattern, it is evident that this contributed to the timely delivery of the project. It is important to mention that the preliminary plan was to use a biometric sensor as a first level authentication but we experienced some challenges with the device which was anticipated based on the high margin of error and was specifically mentioned in the project proposal before commencement. For future work of the project, I recommend students to work on session timeout of the OTP where after certain seconds of unused OTP, it expires and also mitigate against replay attack where previously generated and used OTP cannot be reused. Another future work which is also a variant is expanding the application of the program to a network drive where multiple users over a network with different administrative rights and privileges are constrained to undergo such authentication before accessing highly confidential files.

Moreover, on a much larger scale the use of a structured database created with SQL could be applied in lieu of using a text file as a make shift authentication server for user validation.