Project Proposal

Password Manager in Python

Group 8

Ryan Baker	101072478
Mitansh Desai	101168117
Adam Prins	100879683

Introduction:

We plan to develop a password manager. I will be able to store and retrieve passwords, encrypted by a master password. Passwords should be able to be categorised and sorted. It will be able to generate possible new passwords, and determine the strength of stored passwords. The system should be readily accessible from a GUI.

The main challenges will be the encryption of the files, the secure handling in memory, and making sure the program is only using encryption algorithms when needed.

Background:

Users are often the weakest point in a secure system (Townsend, 2020). The use of user generated passwords therefore become a massive target to malicious users as they know that user generated passwords tend to be weak and reused. Furthermore, there will be different rules in place for each password you generate, such as the length and the allowed characters. However, these rules create different challenges such as failure by the user to remember complex passwords. Furthermore, a user may create insecure passwords that are prone to brute force dictionary attacks, regardless of the criteria put in place.

In a study done by Virginia Tech, more than fifty percent of people use the same password across multiple sites (Wang, K., Hu, Bossart, & Wang, 2018). The most common passwords reuse was seen on applications which contain sensitive information such as shopping websites and email services. Furthermore, they developed a new training-based password guessing algorithm. With this algorithm they were able to crack over 16 million of the 61.5 millions passwords in under 10 guesses or less. This goes to show how weak user created passwords are, as they can be easily guessed.

Password managers attempt to solve these problems. A password manager creates an easy solution for users to implement that directly solves all the problems stated above by generating their own complex passwords, and storing them for the user. This is all guarded by one master password, which if used correctly should be a memorable, but still complex password such as a string of random words with random symbols in between the words. This allows the user to only need to remember one secure and complex password as opposed to many.

System/tool/attack description:

We will implement end-to-end encryption using Advanced Encryption System(AES) because it has been established as the encryption standard by the National Institute of Standards and Technology (NIST) for almost 2 decades now (Chernev, 2021). It is currently one of the most used methods of encryption across multiple transfer protocols like HTTPS, FTPS, SFTP, AS2, and OFTP. Most of the modern-day VPNs like CyberGhost, NordVPN, and ExpressVPN use the highest level of AES encryption (AES-256) which is considered military-grade (G., 2021).

The manager tool will take plaintext passwords as input and process them through the cipher which implements AES and store the output in a text file. The AES will use a common key to encrypt and decrypt the data which will be the user's master password. Each password entry will be stored in the database with additional data, such as the website/service, the user's registered email/username for the website/service. The user will be able to use the tool through a GUI created using Tkinter or pysimplegui. Some additional features that will be implemented would include a password generator, password strength indicator, and a convenient way to copy stored passwords to the clipboard.

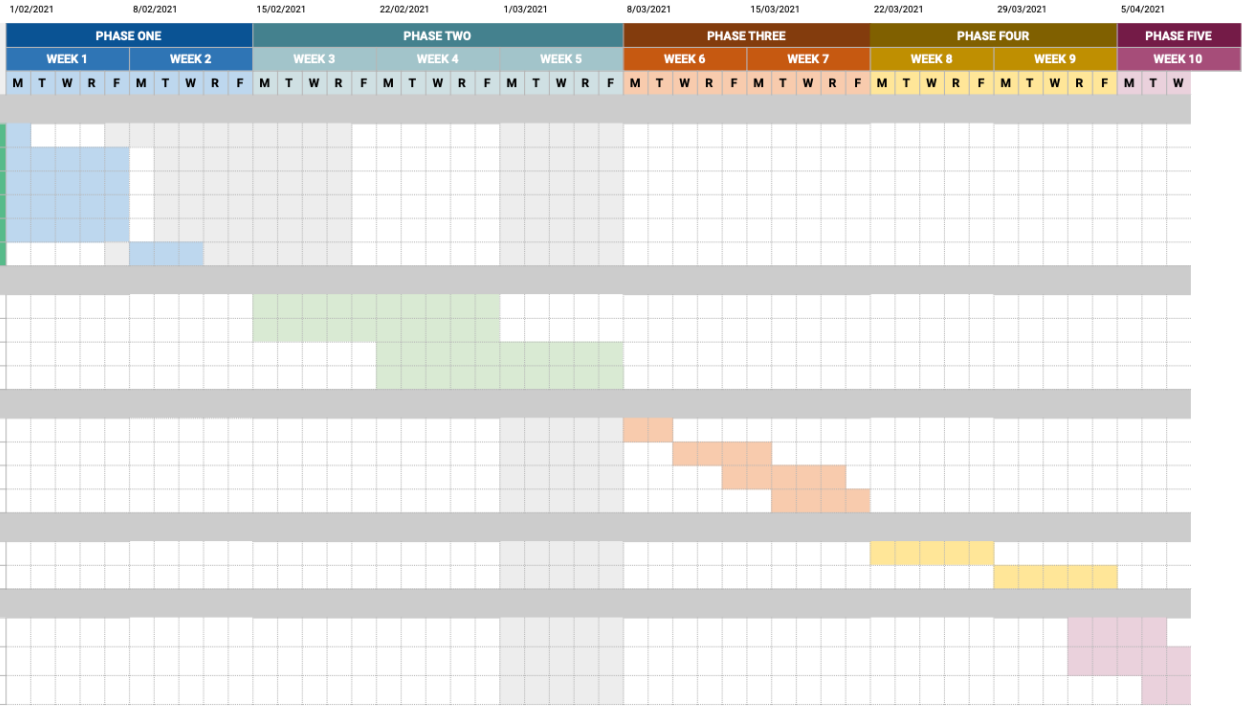
Some challenges we might face would include striking a balance between escalating security and usability, to navigate this efficiently we will need to make sure that we create a robust information architecture that presents data in an easy to understand format. We will also need to make sure that our encryption/decryption algorithm is efficient and makes use of minimal computation so we can have an economical and fast tool.

Implementation plan:

GANTT CHART

PROJECT TITLE	Password Manager	**Group:**	Group 8
Due Date	7/04/2021	**DATE**	1/02/2021

WBS NUMBER	TASK TITLE	TASK OWNER	START DATE	DUE DATE	DURATION	PCT OF TASK COMPLETE
1	**Project Proposal**					
1.1	Template	Adam	1/02/2021	1/02/2021	1	100%
1.2	Introduction	Adam	1/02/2021	7/02/2021	7	100%
1.3	Background	Ryan	1/02/2021	7/02/2021	7	100%
1.4	System Description	Mitansh	1/02/2021	7/02/2021	7	100%
1.5	Implementation plan	Adam	1/02/2021	7/02/2021	7	100%
1.6	Review	Adam	8/02/2021	10/02/2021	3	100%
2	**Encryption and Decryption**					
2.1	Encryption of Strings	Mitansh	15/02/2021	26/02/2021	12	0%
2.2	Decryption of Strings	Mitansh	15/02/2021	26/02/2021	12	0%
2.3	Salt Generation	Ryan	22/02/2021	5/03/2021	14	0%
2.4	Test cases	Ryan	22/02/2021	5/03/2021	14	0%
3	**Password Storage**					
3.1	Reading/Writing Files	Ryan	8/03/2021	9/03/2021	2	0%
3.2	Password Organization	Mitansh	10/03/2021	13/03/2021	4	0%
3.3	Password Generation	Adam	12/03/2021	16/03/2021	5	0%
3.4	Password Strength (Entropy)	Adam	14/03/2021	17/03/2021	4	0%
4	**Password Manager GUI**					
4.1	GUI Framework		22/03/2021	26/03/2021	5	0%
4.2	GUI Navigation		29/03/2021	3/04/2021	5	0%
5	**Project Wrap-Up**					
5.1	Final Testing		3/04/2021	6/04/2021	4	0%
5.2	Project Documentation	Mitansh	3/04/2021	7/04/2021	5	0%
5.3	Project Video Demonstraition		6/04/2021	7/04/2021	2	0%



References

Townsend, K. (2020, November 26). Weakest Link In Security. Retrieved February 01, 2021, from https://blog.avast.com/weakest-link-in-security-avast

Wang, C., K., S. T., Hu, H., Bossart, D., & Wang, G. (2018, March). The Next Domino To Fall: Empirical Analysis of User Passwords across Online Services. Retrieved February 01, 2021, from https://people.cs.vt.edu/gangwang/pass

Chernev, B. (2021). What Is AES - The World's Most Popular Encryption Method. TechJury. Retrieved 1 February 2021, from https://techjury.net/blog/what-is-aes/

G., D. (2021). The Ultimate List of Best VPN Services for 2021 [Honest Reviews]. TechJury. Retrieved 1 February 2021, from https://techjury.net/best/vpn-services/