REQUIREMENTS

#INTRODUCTION: A password manager is a computer program that allows users to store, generate, and manage their passwords for local applications and online services. A password manager assists in generating and retrieving complex passwords, storing such passwords in an encrypted database, or calculating them on demand.

#RESEARCH: Password managers, though commonly recommended by security experts, are still not used by many users. Understanding why some choose to use password managers while others do not is important towards generally understanding why some users do what they do and, by extension, designing motivational tools such as video tutorials to help motivate more to use password managers. To investigate differences between those who do and do not use a password manager, for this paper, we distributed an online survey to a total of 137 users and 111 non-users of the tool that asked about their opinions/experiences with password managers. Furthermore, since emotion has been identified by work in psychology and communications as influential in other risk-laden decision-making (e.g., safe-sex behavior such as condom use), we asked participants who use a password manager to rate how they feel for 45 different emotions, or, as the case for those who do not use a password manager, to rate how they imagine they would feel the 45 emotions if they did use the tool. Our results show that "users" of password managers noted convenience and usefulness as the main reasons behind using the tool, rather than security gains, underscoring the fact that even a large portion of users of the tool are not considering security as the primary benefit while making the decision. On the other hand, "non-users" noted security concerns as the main reason for not using a password manager, highlighting the prevalence of suspicion arising from lack of understanding of the technology itself. Finally, analysis of the differences in emotions between "users" and "non-users" reveals that participants who never use a password manager are more likely to feel suspicious compared to "users," which could be due to misunderstandings about the tool.

Source - *https://hcis-journal.springeropen.com/articles/10.1186/s13673-017-0093-6*

Defining System:

The password manager's data structure is focused around the 4 key features:

Login:

The user types the password to unlock the program and load the file into the data structure of the program. The login would also create a new user if required.

Inputs from User: Login take two datasets from the user: Username and main password.

Inputs from file: Login function loads the saved data file into the program.

We chose to use the

Main Menu:

Implements the functions of creating and retrieving the passwords. The main menu navigates the program and implements the features.

Inputs: User choice for navigating between the program features.

New Password:

Retrieve Password:

Program functions:

SWOT Analysis:

Strength: All computer systems store passwords in some encrypted form, think of the password as a key to a cryptographic system. Cryptographic systems provide more security as the key size grows, suggesting that passwords are more secure as they grow longer. There is some truth in this observation. However, a longer password is not as strong when compared to a

shorter password as one might think. This is due to the limitations imposed by some computer systems and the way in which people choose their passwords.

- **Weakness**: If random characters from the set of alphanumerics are used, an 11-character password would be necessary. Unfortunately, users are unlikely to memorize a randomly selected 11-character string.
- If pronounceable passwords are chosen, each character contributes about 4 bits to the key size, so a 16-character password would do. This, too, is a much longer password than people will memorize.
- If people are allowed to select their own password, conventional wisdom says that each character contributes only 2 bits, so passwords would have to be 32 characters in length. This is also too long.

Opportunities:

- With the increasing internet services penetration, improving communication infrastructure, and data speed improvements, the growing number of internet and mobile users is influencing various businesses, across the world, to adopt the internet to offer their services and products, driving the need for the creation of different profiles by the end-users. Along with this, enterprises are increasingly adopting security measures to increase accountability by adopting user accounts. Such developments are, in turn, augmenting the demand for password management software.

Threat:

The most obvious risk from using a password manager is that **it keeps all of your sensitive login information in one place**, so one breach could be catastrophic. That said, many password managers use numerous layers of security that greatly reduce the chance of your passwords being hacked and shared.

High Level Requirement :

Character Set	Password Length				
	4-octet	5-octet	6-octet	7-octet	8-octet
Lowercase letters (26)	$4.6x10^5$	$1.2x10^7$	$3.1x10^8$	$8.0x10^9$	$2.1x10^{11}$
Lowercase letters/digits (36)	$1.7x10^6$	$6.0x10^7$	$2.2x10^9$	$7.8x10^{10}$	$2.8x10^{12}$
All alphanumeric characters (62)	$1.5x10^7$	$9.2x10^8$	$5.7x10^{10}$	$3.5x10^{12}$	$2.2x10^{14}$
Printable characters (95)	$8.1x10^7$	$7.7x10^9$	$7.4x10^{11}$	$7.0x10^{13}$	$6.6x10^{15}$
7-bit ASCII characters (128)	$2.7x10^8$	$3.4x10^{10}$	$4.4x10^{12}$	$5.6x10^{14}$	$7.2x10^{16}$
8-bit ASCII characters (256)	$4.3x10^9$	$1.1x10^{12}$	$2.8x10^{14}$	$7.2x10^{16}$	$1.8x10^{19}$

Low Level Requirement :

Character Set	Password Length				
	4-octet	5-octet	6-octet	7-octet	8-octet
Lowercase letters (26)	0.5 sec.	12 sec.	5.2 min.	2.2 hours	2.4 days
Lowercase letters/digits (36)	1.7 sec.	1 min.	36.7 min.	21.7 hours	32.4 days
All alphanumeric characters (62)	15 sec.	15 min.	15.8 hours	40.5 days	7 years
Printable characters (95)	1.4 min.	2.1 hours	8.6 days	2.2 years	209 years
7-bit ASCII characters (128)	4.5 min.	9.4 hours	50.9 days	17.8 years	2283 years
8-bit ASCII characters (256)	1.2 hours	12.7 days	8.9 years	2283 years	570,776 years

- .