CS301.1 Investigative Studio

Written by Conor Cook

Working with Nicki Choo

Supervisor, Rouwa Yalda

Contents

[Abstract: 3](#_Toc160803133)

[Introduction: 3](#_Toc160803134)

[Literature Review 4](#_Toc160803135)

[Article 1: A Study for an Ideal Password Manager 4](#_Toc160803136)

[Article 2: Balancing Password Security and User Convenience: Exploring the Potential of Prompt Models for Password Generation 4](#_Toc160803137)

[Article 3: A comparative study on Modern Password Management 4](#_Toc160803138)

[Article 4: A Dynamic Method and Program for Multiple Password Generation and Management 5](#_Toc160803139)

[Article 5: 5](#_Toc160803140)

[Research Question(s) or Problem Definition: 6](#_Toc160803141)

[Changes to be Made and Tools: 6](#_Toc160803142)

[New Features: 6](#_Toc160803143)

[Improvements: 6](#_Toc160803144)

[Schedule for Implementation/Timeline: 6](#_Toc160803145)

[Conclusion: 7](#_Toc160803146)

[Notes (For personal use) 8](#_Toc160803147)

[Structure 8](#_Toc160803148)

# Abstract:

In the modern age of the internet, passwords have become an essential. With how often a password is needed online, it gets challenging to remember all of them. Therefore, people have developed a product called a password manager. A password manager stores a user’s login details and keeps them secure. Several hundred password managers exist online, some even built into a browser, but the issue related to these tools are related to either being secure but not user friendly, or not secure but very user friendly. In 2023 a password manager, called MasterVault, has been deployed with the aim to balance user-friendly design with enhanced security. It had an excellent design, but it fell short of the original intentions and was not able to deliver all it had promised to do. This project aims to enhance MasterVault, making it an ideal password manager that perfectly balances security with user-friendly design.

# Introduction:

Password managers need to be secure, as they store incredibly important user information. However, a lot of easily accessed password managers have next to no security. Browser-based password managers are an excellent example. There have been several studies stating that browser-based password managers are not secure and have been a part of several private data leaks. But they are by far the easiest password managers for users as they are built into the browser. Meanwhile a well know password manager called ‘Dashlane’ (*Dashlane password manager* 2024), which is widely considered one of the best password managers on the market, is not very user-friendly. This imbalance causes users who are not experienced with password managers to primarily use browser-based password managers, which as stated before, are not secure. This leaves a large number of users online vulnerable to their private information being stolen. MasterVault aimed to fill this gap in the password manager market. By implementing several security features like 256-AES encryption, master passwords and account locking all while having a user-friendly interface. However, when the product was released, it wasn’t able to deliver all it promised to be.

The aim of this CS301.2 project it to enhance MasterVault. Adding new features to make it more secure and user-friendly. But also improving what was already developed. By the end of this project, MasterVault will be the ideal password manager for users of all backgrounds and experiences.

# Literature Review

## Article 1: A Study for an Ideal Password Manager

This article discussed the requirements for a password manager to be secure and usable. Users usually opt for weaker passwords due to the cognitive load of recalling complex passwords. In terms of password generation, password managers that are designed for simplicity typically have a limited symbol set used in generation. The authors found that KeePass has one of the most comprehensive symbol sets. The article states that a secure password manager should use 256-AES encryption, however there are various methods used for meta data encryption among password managers. The authors then discussed the importance of user engagement to prevent unauthorised access through functions like autofill. In addition, valuable insights for creating an ideal password manager that emphasises the significance of password strength and encryption standards.

## Article 2: Balancing Password Security and User Convenience: Exploring the Potential of Prompt Models for Password Generation

This article highlights the important of strong passwords in the face of cyber-attacks and data breaches. Modern password generation can create incredibly secure and complex passwords, it often results in password that are far too hard to remember, causing users to reuse or write the password down. However, prompt models such as ChatGPT are presented as solutions to generate strong and memorable password generators, tailored to the users.

The author of this article used Pass fault to evaluate the strength of passwords generated by ChatGPT, while applying rules to modify the passwords. Some of the rules used in the study include changing vowels with characters, replace the most common vowel, remove all vowels and more. The results indicate that the modify passwords had improved strength, particularly when the vowels of a password were changed. While passwords generated by prompt models posed security concerns. The article concludes by emphasizing the need for reasonable password standards and considering prompt models as tools to balance security and user convenience.

## Article 3: A comparative study on Modern Password Management

This article discusses the importance of password managers in the digital age, highlighting the increasing threats from attackers and hackers. The articles emphasise the need for a secure password manager. The article suggests that most password managers are considered safe, there are various risks when storing sensitive information. The research suggests the idea of using passphrases as a secure alternative to regular passwords. The author states that passphrases are easier to understand, remember and harder to hack. The article explores strengthening passwords through paraphrases and discusses their application in protecting SSH and private keys used in email encryption tools.

## Article 4: A Dynamic Method and Program for Multiple Password Generation and Management

This article discusses the challenges associated with the increasing number of passwords users need for various online services and the potential security risks involved. It introduces different approaches to password management, such as password managers, password generators, and specific methods like Site-Specific Passwords and Password Multiplier. The article then delves into the Chinese Remainder Theorem and proposes a dynamic method and program for multiple password generation and management based on the Forward Direction Method. This method involves determining a strong unique password and generating divisors to obtain individual passwords. The article highlights the security advantages of this approach, where only divisors are stored, making it difficult to retrieve the unique password even with knowledge of the divisors. The results and discussion section provides sample individual passwords generated using this method and emphasizes the numerical size difference between the unique password and divisors, enhancing security.

## Article 5: Revisiting Security Vulnerabilities in Commercial Password Managers

This article explores recently found problems as well as vulnerabilities that have been made in popular password managers. The vulnerabilities that have been found include two-factor authentication seed, element inspection, registration discovery, HTTP(S) autofill and ignoring subdomains. The study reveals that most password managers are susceptible to, HTTP(S) autofill, and ignoring subdomains vulnerabilities.

The article also identifies new vulnerabilities, including a potential brute force vulnerability via extension in Keeper, Dashlane, and 1Password, a phishing attack on LastPass and 1Password Android applications, a clipboard vulnerability in various password managers, and a PIN brute force vulnerability in Dashlane and RoboForm Android applications.

The article "Revisiting Security Vulnerabilities in Commercial Password Managers" discusses both previously disclosed vulnerabilities and newly discovered issues in popular password managers. The identified vulnerabilities include two-factor authentication seed vulnerability, element inspection vulnerability, registration discovery vulnerability, URL mismatch vulnerability, HTTP(S) autofill vulnerability, and ignoring subdomains vulnerability. The study reveals that most tested password managers are susceptible to URL mismatch, HTTP(S) autofill, and ignoring subdomains vulnerabilities. Additionally, the article highlights new vulnerabilities, such as a phishing attack on LastPass and 1Password Android applications, a clipboard vulnerability in various password managers, PIN brute force vulnerability in Dashlane and RoboForm Android applications, and a potential brute force vulnerability via extension in Keeper, Dashlane, and 1Password. The authors emphasize responsible disclosure efforts, detailing interactions with vendors and their responses to the reported vulnerabilities, while acknowledging both positive and negative aspects of vendor responsiveness to the disclosed issues. The article concludes with a suggestion for developing rigorous security models and canonical security tests for password managers to enhance overall security.

# Research Question:

After reviewing the previous articles, we came up with the following research question:

“How can password managers evolve and adapt to security threats and user preferences while maintaining user-friendliness?”

# Changes to be Made:

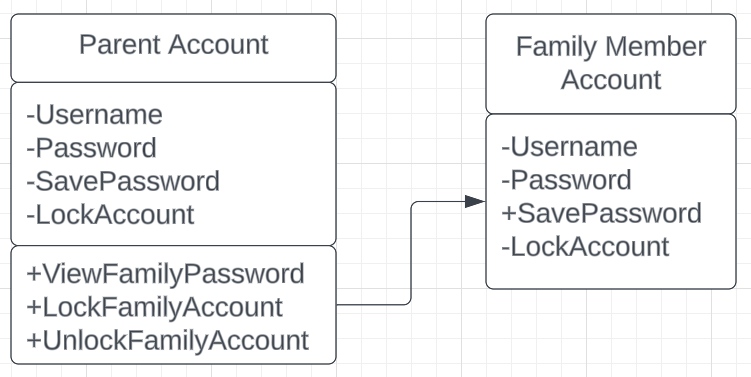
## New Features:

* Saving different login details

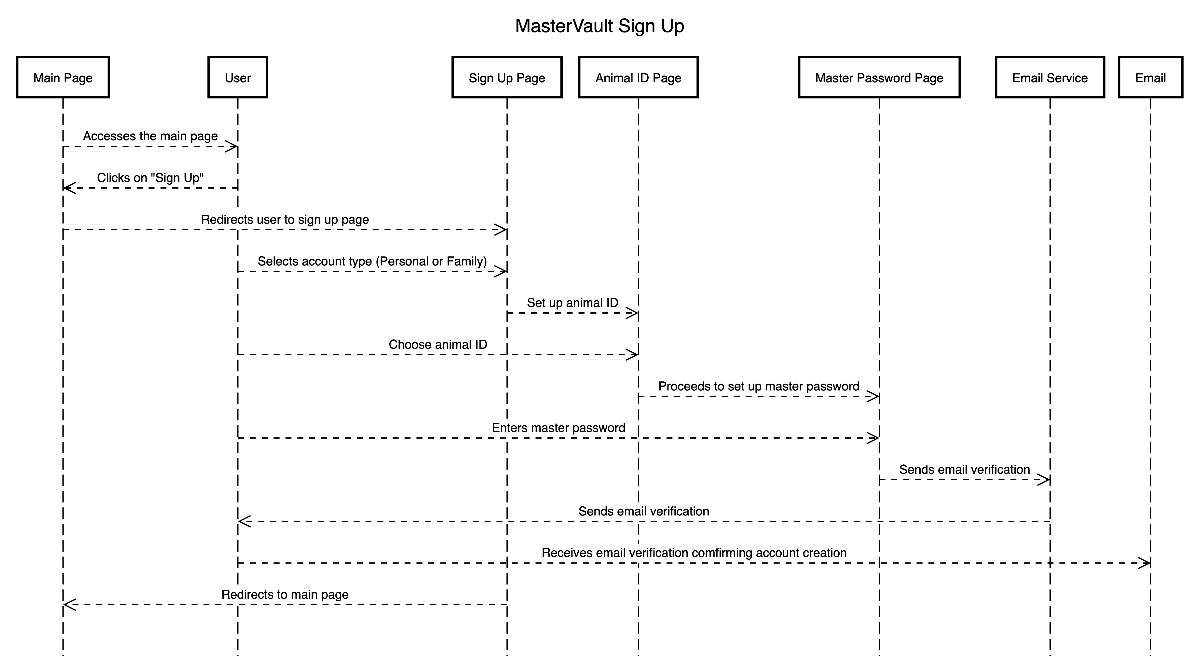
Currently with MasterVault, you can only save three details at one. Those details being website, email/username, and password. However, some websites require more details for login. We aim to add new login details that users can save when saving a password with the password manager. These new login details will be Date, Number and Other. Other will be a text input which can be used for anything that does not fit into the other fields.

* Adding types of account options

Modern password managers only have one account option, a personal account.

* + Personal
  + Family
* Search & Filter
* Secure/lock passwords

## Improvements:

* 256-AES Encryption
* Securer login
  + Animal ID
* Move to online (deployable for website)
* Improving our data framework
* Paraphrase Generator

# Schedule for Implementation/Timeline:

# Tools:

# Conclusion:

# References

* *Dashlane password manager*. Dashlane. (2024, March 7). <https://www.dashlane.com/>

# Notes (For personal use)

* Articles
  + [A Study for an idea password manager](https://d1wqtxts1xzle7.cloudfront.net/79233614/A_Study_for_an_Ideal_Password_Management_System-libre.pdf?1642755729=&response-content-disposition=inline%3B+filename%3DA_Study_for_an_Ideal_Password_Management.pdf&Expires=1709253904&Signature=ZQsdPZ~TA9ZZeFBht803D0F9jDQeHFgWVW7-lvlEtiqn9UrNCe3Sp643G2Xsc2GtDcYzwi9eu1Aqo-RCohdiMHWlSm7Dpq84~5bbkvprazLUp2lZ84xyEvSx03VD6Py0qCH87hH5oSPvRoIdHrLactFs1uwxBGPwYB-wPQjKtBpvs5YHT5fLdBG7cce-0c1lGnX~Ea7mVAD8gfkDdjIJyVPdK5OBmcXsxjT51OVFD7oWy3FIuFn3HS7zbHT8EnhcTN8rXiyGqWPnKCNm2Gz2N0fkn2FJGjc3myxsIFWJnOlsI0~H93WKUbvwJ5u1lBTw~N81YXe4aLYCVruwyA8R2Q__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA)
  + [Balancing Password Security and User Convenience: Exploring the Potential of Prompt Models for Password Generation](https://www.mdpi.com/2079-9292/12/10/2159)
  + [A Comparative Study on Modern Password Management](https://annalsofrscb.ro/index.php/journal/article/view/9761)
  + [A Dynamic Method and Program for Multiple Password Generation and Management](https://dergipark.org.tr/en/pub/ject/issue/64442/1031900)

## Structure

* Abstract (150-250 words):
  + Briefly summarize the project.
  + Cover background, current issues, motivation, proposed solution, and expected outcomes.
* Introduction:
  + Provide comprehensive background and motivation.
  + Discuss challenges in the chosen research area.
  + Briefly outline the proposed solution and contributions to knowledge.
* Literature Review
  + 1.
  + 2.
  + 3.
  + 4.
  + 5.
* Research Question(s) or Problem Definition:
  + Clearly state research gaps or questions based on the literature analysis.
  + Connect these questions to the proposed solution.
* Changes to be Made and Tools:
  + List features.
  + Components, tools, and programming language.
* Schedule for Implementation/Timeline:
  + Outline milestones and ~~timelines.~~
* Conclusion (90-220 words):
  + Summarize main points.
  + Restate the significance of findings.

Remember to number sections and use sub-sections for better organization. This simplified structure should make the proposal more digestible and easier to navigate.