CS301 Investigative Studio

MasterVault Password Manager Enhancements

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:

For our CS205.2 project, me and Nicki choose to develop a password manager, called MasterVault, which was designed to balance security with user-friendly design. We were able to create a minimum viable product based on our proposal. But after creating our app, we realised we could refine the product and add more improvements to it. Our minimum viable product is currently limited to local system use and is not very secure. We plan to move the product online so it can be used from anywhere and make the product more secure. We plan on encryption the user’s data via 256-AES encryption and making the login more secure. We also plan on making new additions to the password manager, like saving different details to a saved password and adding new account types for users. With all these additions and improvements, we believe we can turn our minimum viable product into an industry standard password manager designed to balance security with user-friendly design.

# Introduction:

In 2023, me and Nicki had the idea for our CS205.2 project to develop a password manager that balanced security and user-friendly design. At the time we believed that password manager leaned either too heavily on security and lacked user-friendly design or prioritised user-friendly designed and lacked security. We believed that we could make a password manager that could do both. We envisioned a browser-based password manager that anyone with any skill level could use easily. We planned on implementing keyword-based password generation, 256-AES encryption, along with other security measures like a master password, account locking and more. We were able to develop the password manager and were able to make a minimum viable product, but we were unable to deliver on all that we promised to implement. We were unable to add 256-AES encryption and password manager is limited to local system usage.

For CS302 we plan on improving MasterVault to make it a marketable product. To do this we plan on implementing 256-AES encryption, improving the data structure, and transitioning the product online. We also plan to add the ability to store more details with passwords (such as birthdays or pins), a new security measure for login, new account type options and more.

*(I’m not sure what else to write about)*

# 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:

# Research Question(s) or Problem Definition:

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

# Changes to be Made and Tools:

*(Will be expanded/elaborated. For now, this is just notes)*

## New Features:

* Saving different login details (birthday, pins/numbers, personal question)
* Adding types of account options
  + Personal
  + Family
  + Business
  + Password sharing
* 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:

# Conclusion:

# 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.