301 Investigative Studio

MasterVault Password Manager Enhancements

Written by Conor Cook

Working with Nicki Choo

Supervisor, Rouwa Yalda

Contents

[Abstract (150-250 words): 3](#_Toc160439910)

[Introduction: 3](#_Toc160439911)

[Literature Review 4](#_Toc160439912)

[Article 1: A Study for an Ideal Password Manager 4](#_Toc160439913)

[Article 2: Balancing Password Security and User Convenience: Exploring the Potential of Prompt Models for Password Generation 4](#_Toc160439914)

[Article 3: A comparative study on Modern Password Management 4](#_Toc160439915)

[Article 4: 5](#_Toc160439916)

[Article 5: 5](#_Toc160439917)

[Research Question(s) or Problem Definition: 5](#_Toc160439918)

[Changes to be Made and Tools: 5](#_Toc160439919)

[Schedule for Implementation/Timeline: 5](#_Toc160439920)

[Conclusion (90-220 words): 5](#_Toc160439921)

# 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 MVP is currently limited to local system use and is not very secure.

* + Briefly summarize the project.
  + Cover ~~background~~, ~~current issues~~, ~~motivation~~, proposed solution, and expected outcomes.

# Introduction:

# 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-

while there is variation in metadata encryption. (TBC)

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 Passfault 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. (Conclusion TBC)

## Article 4:

## 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:

# Schedule for Implementation/Timeline:

# Conclusion:

Notes

* 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)

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
* 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.