Aleena

20BCE0200

Contents –

1. Abstract
2. Introduction
    - Background and Motivation
    - Objectives
3. Related Work
    - Literature Survey
    - Research Gap
    - Problem Statement
4. Design Approach
    a. System Architecture
    b. Class Diagram
    c. Use case Diagram
5. Methodology
6. Implementation
7. Results and Discussion
8. Conclusion
9. References

Objectives

The objective of this project is to develop a secure and user-friendly password manager that secures user credentials using encryption and multi-factor authentication. The application aims to provide users with the ability to safely store, retrieve, and manage their passwords and user IDs, while also offering robust recovery mechanisms in case of forgotten passwords or lost access. The system will include features for securely adding, updating, and deleting credentials, along with mechanisms to provide limited access through alternate login method that is used for emergencies. The project will prioritize user experience and data security, ensuring that users have reliable access to their credentials while minimizing the risk of unauthorized access.

Literature Survey

1. **Systematization of Password Manager Use Cases and Design Paradigms**

   Simmons, J., Diallo, O., Oesch, S., & Ruoti, S. (2021, December). Systematization of password manageruse cases and design paradigms. In Proceedings of the 37th Annual Computer Security Applications Conference (pp. 528-540).

   The paper aims to address the usability of password managers by identifying and categorizing their use cases and design paradigms. Through reviewing password management documentation and literature, the authors systematized seventeen use cases and seventy-seven design paradigms. They conducted cognitive walkthroughs on eight popular desktop managers to evaluate their usability across these use cases. The study revealed significant usability issues such as difficulties in entering credentials on secondary devices, fatiguing setup processes, and challenges with interface designs and credential linking. Key observations include the limited functionality and security of browser-based managers compared to extension-based managers. The study highlights the need for further research to improve password manager designs and usability. A major gap identified is the lack of comparative studies on design paradigms, preventing a comprehensive understanding of their strengths and weaknesses. The authors suggest a transition strategy from browser-based to extension-based managers to enhance security and functionality for users.

2. **"It Basically Started Using Me:" An Observational Study of Password Manager Usage**

   Oesch, S., Ruoti, S., Simmons, J., & Gautam, A. (2022, April). "It Basically Started Using Me:" An Observational Study of Password Manager Usage. In Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (pp. 1-23).

   This paper investigates the real-world usage and rationale behind password manager use through observational interviews with 32 users, employing grounded theory for data analysis. The research reveals that many users concurrently utilize both browser-based and third-party password managers, primarily as a backup strategy, and often without initial intention. Users avoid generated passwords due to difficulties in cross-device entry and memory challenges. Additionally, while credential audit tools are rarely used due to overwhelming and confusing outputs, users appreciate simpler and more direct warnings from Chrome's built-in manager. Mobile password manager usage is minimal due to inconsistent autofill functionality and syncing issues, with users preferring single sign-on (SSO) solutions. Adoption is driven by work requirements, ease of credential entry, and improved password quality, yet promotion of password manager usage is limited outside immediate family. The study highlights the need for improved usability in password generation, credential audits, and mobile managers. Limitations include a U.S.-centric, tech-savvy sample from MTurk, potentially introducing biases and not capturing the experiences of non-users or those who abandoned managers. Future research should explore diverse populations and employ quantitative methods to validate and expand these findings.

3. **That Was Then, This Is Now: A Security Evaluation of Password Generation, Storage, and Autofill in Browser-Based Password Managers**

   Oesch, S., & Ruoti, S. (2020, August). That was then, this is now: A security evaluation of password generation, storage, and autofill in browser-based password managers. In Proceedings of the 29th USENIX Conference on Security Symposium (pp. 2165-2182).

   This study evaluates the current security of 13 popular browser-based password managers, examining all three stages of the password manager lifecycle: password generation, storage, and autofill. The purpose is to determine if these tools have addressed known vulnerabilities from past research conducted five years ago. The researchers generated 147 million passwords to analyze their strength and randomness using various statistical tests, examined local password storage for encryption practices, and tested autofill functionalities against known web attacks. They found improvements in security features such as better encryption and safer autofill processes, but also identified persistent issues like unencrypted metadata, unsafe defaults, and susceptibility to clickjacking attacks. Notably, some generated passwords were still vulnerable to online and offline attacks, and certain managers auto-filled passwords without user interaction, posing security risks. The study highlights the need for users to carefully select and configure password managers, recommends enhancements like filtering weak passwords and improving master password policies, and suggests areas for future research such as mobile password managers and browser-supported password generation. Despite advancements, the study emphasizes that significant gaps remain, requiring ongoing evaluation and improvement to ensure password manager security and usability.

4. Why people (don't) use password managers effectively

Pearman, S., Zhang, S. A., Bauer, L., Christin, N., & Cranor, L. F. (2019). Why people (don't) use password managers effectively. In Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019) (pp. 319-338).

The study investigates the adoption and effective use of password managers among users of built-in (browser-based or OS-based) and separately installed password managers through 30 semi-structured interviews. It aims to understand user mindsets, motivations, and barriers related to password management practices. Findings reveal that users of built-in managers prioritize convenience, often resulting in weaker password practices like reuse, while users of separately installed managers prioritize security with stronger, unique passwords. The study identifies barriers such as security concerns, lack of awareness, and usability issues. However, it acknowledges gaps in addressing specific user frustrations and suggests the need for more tailored designs and improved usability testing to enhance adoption among diverse user groups, particularly those less inclined towards security-centric behaviours. Future research should focus on bridging these gaps to effectively promote secure password management practices universally.

5. Why Older Adults (Don't) Use Password Managers

Ray, H., Wolf, F., Kuber, R., & Aviv, A. J. (2021). Why older adults (Don't) use password managers. In 30th USENIX Security Symposium (USENIX Security 21) (pp. 73-90).

This study explores the adoption of password managers (PMs) among older adults (>60 years), and compares motivations and barriers with younger cohorts. Through semi-structured interviews with n = 26 participants, it identifies key differences: older adults exhibit higher mistrust of cloud storage and cross-device synchronization but show favourability towards PMs when recommended by family. Findings highlight barriers like perceived complexity and lack of urgency, suggesting advocacy and education as strategies for promoting PM adoption. However, the study acknowledges limitations in sample size and generalizability, particularly in technological literacy among older adults. This points to a need for further research to comprehensively explore these factors across diverse older adult populations and to address potential gaps in understanding how best to encourage PM adoption among this demographic.

6. **Challenges and Opportunities in Password Management: A Review of Current Solutions**

   Fernando, W. P. K., Dissanayake, D. A. N. P., Dushmantha, S. G. V. D., Liyanage, D. L. C. P., & Karunatilake, C. (2023). Challenges and Opportunities in Password Management: A Review of Current Solutions.

   This review paper explores the enduring challenges of password management in computer systems, emphasizing the prevalence of passwords despite numerous security vulnerabilities and malpractices. It evaluates various solutions including traditional, biometric, and PIN-based authentication, concluding that none have supplanted passwords due to their simplicity and universal applicability. The paper extensively discusses password managers (PMs) as a promising solution, categorizing them into software and hardware-based types, each with distinct advantages and limitations. Software PMs offer convenience but face security risks, while hardware PMs enhance security but suffer from usability concerns and potential data loss risks. The review identifies a research gap in the need for fully automating the password management process to address these issues comprehensively, emphasizing the importance of usability, security enhancements, backup mechanisms, and resistance to attacks as crucial areas for future research and development efforts.

7. **Android Password Managers and Vault Applications: Data Storage Security Issues Identification**

   Petrov, M. (2022). Android password managers and vault applications: data storage security issues identification. Journal of Information Security and Applications, 67, 103152.

   In their study titled "Android Password Managers and Vault Applications: Data Storage Security Issues Identification," the authors conduct a comprehensive analysis aimed at evaluating the security of Bitwarden and Keeper, two highly rated Android password manager/vault applications. Their primary objective is to assess the efficacy of these applications in securely storing user-entered data over the long term. The methodology involves advanced reverse engineering techniques, including runtime analysis and debugging, to uncover implementation details beyond what is publicly documented. By scrutinizing artifacts such as application data in persistent storage, crash dumps, and installer files, they aim to identify potential vulnerabilities and security gaps. Through their investigation, the authors successfully uncover several vulnerabilities and demonstrate proof-of-concept attacks that exploit these weaknesses. However, the study is limited in scope to the core protections implemented by the applications themselves, excluding external libraries and network-related security aspects. Despite revealing significant security risks and design flaws, the study provides valuable insights for improving data storage security in password managers and vault applications, suggesting avenues for future research on antipatterns and alternative security approaches.

8. Enhanced Password Manager using Hybrid Approach

Pandare, P., Uniyal, S., Vani, R., Mali, S., & Rumao, P. (2023, April). Enhanced Password Manager using Hybrid Approach. In 2023 International Conference on Inventive Computation Technologies (ICICT) (pp. 1793-1798). IEEE.

This paper introduces an enhanced password manager extension for web browsers, aiming to provide secure and user-friendly password storage. Using a hybrid approach of SHA-256 and AES encryption, the system ensures robust data security. The methodology involves leveraging Trongate as a development platform with PHP, HTML, CSS, and JavaScript for frontend and backend implementation. Data is stored securely in a phpMyAdmin database hosted on a localhost server, optimizing speed and cost-effectiveness. The system encrypts passwords upon saving, ensuring privacy and protection against unauthorized access. However, while the approach integrates strong cryptographic methods and emphasizes user privacy, potential drawbacks include scalability concerns with local hosting and the dependency on a single database system, which may limit deployment flexibility in larger-scale environments or cloud-based deployments. Future work could focus on enhancing scalability and exploring cloud-based storage options to address these limitations and broaden applicability across different deployment scenarios.

9. Password Manager with Multi-Factor Authentication

Dhanalakshmi, R., Vijayaraghavan, N., Narasimhan, S., & Basha, S. (2023, April). Password Manager with Multi-Factor Authentication. In 2023 International Conference on Networking and Communications (ICNWC) (pp. 1-5). IEEE.

This paper introduces a password manager enhanced with multi-factor authentication (MFA) to bolster security against data breaches and unauthorized access. The primary goal is to securely store and encrypt passwords using AES-256 encryption and PBKDF2 hashing for the master password. The system offers users the choice between local storage (offline) and cloud-based storage for passwords, each providing distinct advantages in terms of accessibility and security. MFA is implemented using biometric factors like fingerprints and graphical passwords, enhancing authentication security. The architecture involves modules for master password management, vault key generation, MFA, and interaction with a web server or cloud database. Implementation includes a user-friendly interface for managing various credentials securely. However, potential drawbacks include the risk of security bugs due to the complexity of MFA integration and the possibility of compromising the master password hash in cloud-based scenarios. Future work could focus on rigorous security testing, additional hashing techniques, and improving user education on MFA usage to mitigate these risks effectively and enhance overall system resilience.

10. MonoPass: A Password Manager without Master Password Authentication

Jeong, H., & Jung, H. (2021, April). MonoPass: a password manager without master password authentication. In 26th international conference on intelligent user interfaces-companion (pp. 52-54).

MonoPass is a novel password manager designed to eliminate the use of a master password for authentication, aiming to enhance security against password breaches while maintaining usability. The system employs a password generator that derives unique passwords from a master password using PBKDF2 hashing and HMAC-SHA256/512 encryption, ensuring consistency across devices without storing passwords centrally. Password metadata, including username and policy requirements, is hashed to generate passwords locally on each device, avoiding transmission over the network. The central server facilitates synchronization of metadata between devices via user-generated identification codes. While MonoPass addresses security concerns by decentralizing password storage and eliminating the risk of exposing all passwords through a master password breach, it relies on a central server for metadata synchronization, limiting functionality without an internet connection. Additionally, usability aspects such as manual metadata entry and potential inconvenience in real-world scenarios require further evaluation. Future work includes exploring alternative synchronization methods and conducting comprehensive security and usability assessments to validate MonoPass's effectiveness in real-world usage scenarios.