TEAM ADL

Team Members

Avila, Minard Angelo

Dorado, Ethan John

Langres, Ivan James

Overview of the Problem

Password management remains a significant challenge in 2025, as many users struggle to create and remember strong, unique passwords for the numerous online accounts they maintain. This often leads to weak or reused passwords, which increases the risk of unauthorized access and account breaches. Despite the advances in authentication technologies, such as biometrics and passkeys, passwords remain the primary method of login due to their widespread adoption. Cybercriminals exploit poor password habits through attacks such as phishing, brute force, and credential stuffing, making effective password management critical for digital security.

To address this problem, password managers have become essential tools that help users generate, store, and auto-fill complex passwords securely across devices. These tools reduce the burden of memorization and encourage better password hygiene, significantly lowering the risk of breaches. However, password managers must be user-friendly, secure, and accessible to people with varying technical skills. Improving password management practices through such solutions is vital to protecting individuals and organizations from the growing threat of credential-based cyberattacks.

User Characteristics

The primary users of password managers are everyday internet users who manage multiple online accounts and seek a simple, secure way to store and generate strong passwords. The target audience includes professionals, older adults, and individuals with varying levels of technical expertise who want to improve their online security and reduce the risk of password-related breaches. Password managers are also commonly used in workplace environments to enhance credential security.

Task Analysis

Task Characteristics

Users will use the app to do the following:

- **Secure Password Storage** – Store generated or inserted passwords in secure and encrypted storage.
- **Generate Complex Passwords** – Generate strong, unique, and complex passwords for each account, helping users avoid weak or reused passwords.
- **Auto-fill Login Credentials** – The app will auto-fill stored usernames and passwords on websites and apps.
- **Alerts for Compromised Passwords** – The app will notify users when their password appears in data breaches
- **Manage and Update Passwords –** The app helps users quickly change or reset passwords, especially after security breaches.

Task Environment

The task environment encompasses the digital contexts in which users create, store, manage, and use passwords across multiple online accounts and services. It involves interaction with various websites, applications, and devices where authentication is required, as well as integration with browsers and operating systems. The environment includes the need to securely encrypt and store credentials, generate strong passwords, auto-fill login information, and synchronize data across devices while protecting against threats like phishing, brute force attacks, and data breaches.

Structured Task Analysis

1. **Setup Password Manager**
    - 1.1. Install the app or browser extension
    - 1.2. Create a master password for the application.
    - 1.3. Configure basic settings.
2. **Store Existing Passwords**
    - 2.1. Import passwords from browsers or other password managers.
    - 2.2. Manually input passwords for accounts not yet stored.

    2.3. Organize passwords into categories. (optional)

3. **Generate Strong Passwords**
    3.1. Use the built-in password generator to create new complex and unique passwords.
    3.2. Customize the password length and character type. (optional)
4. **Password Auto-fill**
    4.1. Enable auto-fill credentials on supported websites and applications.
    4.2. Select correct account credentials when multiple accounts are detected.
5. **Sync Passwords Across Devices**
    5.1. Connect the password manager to local or cloud sync services.
    5.2. Ensure passwords and updates are available on different devices.
    5.3. Manage device access.
6. **Backup and Recovery**
    6.1. Create a backup for encrypted passwords if needed.
    6.2. Setup recovery options in case of losing access to the master password.
    6.3. Restore passwords from backups if necessary.

Analysis of Existing System

Password managers have become important tools to help people securely store and manage their passwords in an increasingly digital world. They offer features like generating strong passwords, auto-filling login details, and syncing information across devices to improve security and convenience. However, despite their benefits, many users still face challenges that prevent password managers from being fully effective for everyone.

- **Limited User Adoption** – Many people are unaware of or hesitant to use password managers due to concerns about complexity or trust.
- **Usability Challenges** – Some systems are not intuitive, making it hard for less experienced users to navigate and use them properly.
- **Security Fears** – Users worry about the risk of having all their passwords stored in one place and the potential consequences if that data is compromised.
- **Compatibility Issues** – Password managers may not work smoothly across all devices, browsers, or applications, leading to inconsistent experiences.
- **Technical Limitations** – Problems with auto-fill accuracy, syncing delays, and adapting to new authentication methods can reduce overall effectiveness.

Addressing these issues is essential to making password management tools more accessible, reliable, and trusted worldwide.

Social and Technical Context

Password manager applications play a crucial role in helping individual users navigate the growing challenges of digital security in their daily lives. Socially, many people struggle with remembering multiple complex passwords and often resort to risky practices like reusing or writing down passwords, which increases their vulnerability to cyberattacks and identity theft. While awareness about good password habits is improving, many users still find it difficult to adopt secure and convenient solutions. Trust is also a key factor, as individuals worry about storing all their sensitive information in one place and the potential consequences if that data is compromised.

From a technical perspective, password managers provide users with encrypted storage, automatic password generation, auto-fill features, and synchronization across devices to simplify secure password management. However, challenges remain, such as ensuring ease of use for people with varying technical skills, maintaining compatibility across different devices and platforms, and protecting against security vulnerabilities related to cloud storage or master password breaches.

Usability Criteria

1. Efficiency – Users should be able to complete tasks such as adding, generating, and auto-filling passwords quickly and accurately with minimal effort.
2. Ease of Learning – The user interface should be straightforward and intuitive, allowing users of varying technical skills to learn how to use the password manager without confusion.
3. Error Tolerance – The application should prevent common user errors and provide clear guidance, ensuring users do not compromise security unintentionally.
4. Cross-Platform Compatibility – The application must work seamlessly across multiple platforms to provide consistent access and functionality whenever needed.

Implication of Design

- **Usability Challenges Hinder Adoption –** Despite their security benefits, many users find password managers difficult to use for basic tasks like safe login, which reduces widespread adoption and effective use.
- **Security Concerns Affect Trust** – Users worry about risks such as cloud breaches, local device vulnerabilities, and the security of the master password, which can undermine trust and discourage reliance on password managers.
- **Compatibility and Autofill Issues** – Password managers often face problems with auto-filling credentials incorrectly or not supporting certain websites' password policies, which frustrates users and disrupts workflow
- **Password Managers Provide Critical Protection** – Despite drawbacks, password managers significantly improve security by enabling strong, unique passwords, protecting against phishing, and reducing password reuse, making them essential tools in digital security