Risks mitigated or created by password managers

Sarthak Siddhant Bharadwaj
Department of Computer Science,
Colorado State University,
1113 west plum street,
Fort Collins, Colorado, India
email:sarthak7@colostate.edu

Quick research on the topic , we found that there are several risks involved with usage of password managers. The effectiveness of password managers are questionable with recent data breaches in big firms like LAST PASS. Further detailed study is required in this field for conclusion.

Keywords: Risk, Password

1 Introduction

Password managers help internet users create , save , manage and use passwords across different online services. Almost all online service require a username and password to create and gain access. Over time, users face a recurring choice: create unique passwords for each site or use a single password over all the sites. Using single password over all site would mean easy data breach and high risk if the password is compromised at any place. This is where the role of password managers comes to the fore, the password managers help remember all the passwords for the user,

Password managers[1] are an attempt to improve password usability, enabling users to create unique, complex passwords for every online account without needing to remember them. All information is securely stored in a password vault and accessible via the password manager. The password manager also helps create highly random and unique passwords if the user visit's a site for the first time.The username and password are then securely stored in the password manager. The next time the user visits the same site, the password manager opens a prompt window, usually the user input is required, asking if the user wants to input the previously saved information. On the other hand, when the user already has a username and password but visits a site for the first time with a password manager installed, it prompts the user to save account information for future visits.

1.1 pros.

1.1 pros. Password managers provide the convenience to the user, they auto fill, minimise the reuse of passwords , help provide stronger passwords , provide increased security , give password mobility like synchronisation of password across devices such as laptop and mobiles.

1.2 cons. Although the password managers have a lot of pros but they also come with several risks[2].In a password manager, users essentially create a single point of failure. If the password manager is hacked, all of a user's passwords could be at risk.Basically the master password is the only key stopping the hackers from the users data.Sometimes it may not adhere to 2 factor authentication and multi-factor authentication.

2 Recent Developments

2.1 Zero Knowledge Architecture. Zero-knowledge encryption security model uses encryption and data segregation to make data breaches irrelevant. When a software platform is zero-knowledge, the user's data is encrypted and decrypted at the device level not on the company's servers or in the cloud. The keys to decrypt and encrypt data are derived from the user's master password and secret keys stored on the user's device.

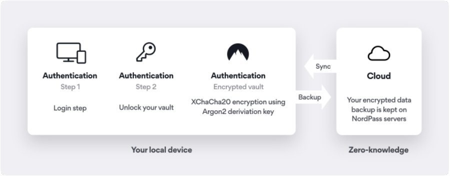

Fig. 1 Zero knowledge architecture.

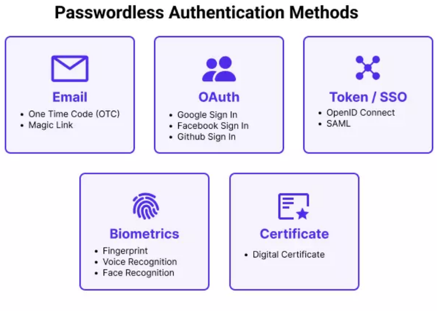

Fig. 2 Passwordless Architecture.

2.2 Passwordless architecture. Passwordless authentication verifies user's identity without any request for a password. This technology replaces passwords with Possession factors like one-time passwords, authentication app codes or a hardware token. Bio metrics including fingerprints, face recognition, retina scans or heartbeats or a "magic" link is used that grants access to the user via email.

Passkeys technology is still far from reality Users need to open an additional email application to access online accounts. Email is an easy medium for hackers to compromise through phishing , which means hackers could intercept codes or passkeys. If the passwordless technology uses SMS or push notifications instead of email, it's a hindrance for people to use another device every time they log in

2.3 Hardware Based Password Managers. Naing Oo (2022) argued that there is a significant research gap between software-based password managers and hardware-based password managers and there is no hardware-based password management solution in the market that is portable, cost-effective, backward compatible and which also gives full access and control over the credentials stored in their hardware wallet. For a hardware wallet to function properly as a password vault, it should interact with the user's web browser through client-side software which can facilitate two-way communication channels via USB, Bluetooth,

Version 1, ¿

3 Products and Technologies in Industries

Password managers benefit organisations by providing complete visibility into employee password practices, they enforce password policies more efficiently and implement Role based Access control.

3.1 NordPass. NordPass is user-friendly and offers all the features an average user could need. You can generate passwords and evaluate their strength, use auto fill auto save, and share login credentials. There a real-time Data Breach Scanner that scans leaked databases for your passwords and credit card details. If any of your information is found online, you are immediately alerted via an in-app notification or an email . The OCR feature – automatically scans text information from credit cards, documents, and photos. They also support offline mode access unlike a lot of other softwares / apps present.

3.2 Keeper. Keeper is a feature-rich service. It offers KeeperChat – an exclusive feature available only on Keeper. It's a secure messaging system with self-destructing messages and a media gallery for private photo sessions and saxophone-heavy music videos. Security Audit – checks all our passwords, evaluates their strength, and suggests changing the weak ones.

3.3 1Password. 1Password has a few unique features such as Watchtower – It scans dark web and also checks if a website supports 2FA. Travel Mode – hides sensitive information on your phone while you're away. If you lose the phone or someone steals it, you can be sure that all personal information is safe. This feature works on all devices and when enabled.

References

[1] Fernando, D. L. K., Dissanayake, 2023, "Challenges and Opportunities inPassword Management: A Review ofCurrent Solutions," Sri Lanka Journal of Social Sciences and Humanities, **3**(2), pp. 9–20.

[2] Pearman, S., Zhang, S. A., Bauer, L., Christin, N., and Cranor, L. F., 2019, "Why people (don't) use password managers effectively," *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, USENIX Association, Santa Clara, CA, pp. 319–338, https://www.usenix.org/conference/soups2019/presentation/pearman

List of Figures

List of Tables

,