SecurePass - A Web Extension for Password Authentication

Introduction

Users can protect their online accounts by using two-factor authentication. Users can now log on using both a password and a code instead of just a password, which is transmitted to their mobile devices. To authenticate, they must enter that code. Because an attacker would require both their password and mobile device, this safeguards their accounts. However, this also creates usability issues, such as the requirement for a mobile device and the necessity to enter another item. The effects of two-factor authentication on usability will be investigated in this research. Does it increase users' sense of security? Are users irritated by it? Why do consumers choose to utilize this technology or not?

SecurePass is a web extension that provides an additional layer of security for users who store their passwords on their web browsers. With SecurePass, users must authenticate themselves whenever they want to access their saved passwords, ensuring that only authorized users can access their accounts.

Literature Review

According to research, two-factor authentication is more secure than single-factor authentication methods and can significantly reduce the risk of password-related attacks **(Yu et al., 2016).**

In addition to increased security, two-factor authentication can also improve user experience. By making the process of accessing saved passwords more secure and convenient, users are more likely to engage in secure password practices. This, in turn, can help to reduce the risk of password-related security breaches **(Nash, 2018).**

While there are various approaches to implementing two-factor authentication for saved passwords, research has shown that the most effective approach is to use a separate application or device for authentication **(Dell'Amico et al., 2017).** This approach provides an additional layer of security by separating the authentication process from the password storage process.

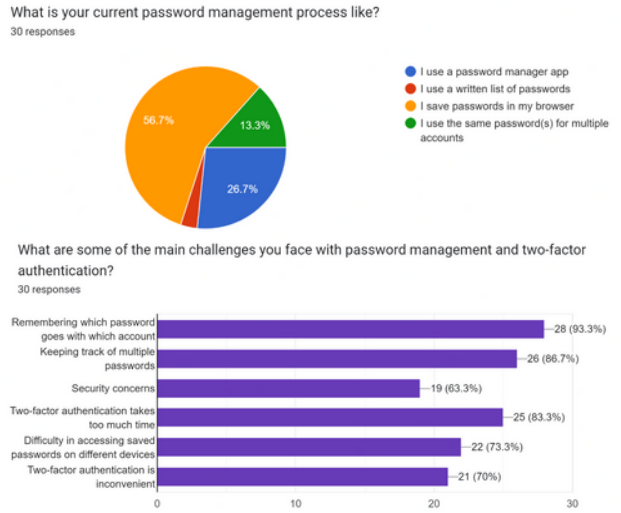
Competitive Analysis

1Password Lastpass Keeper Dashlane

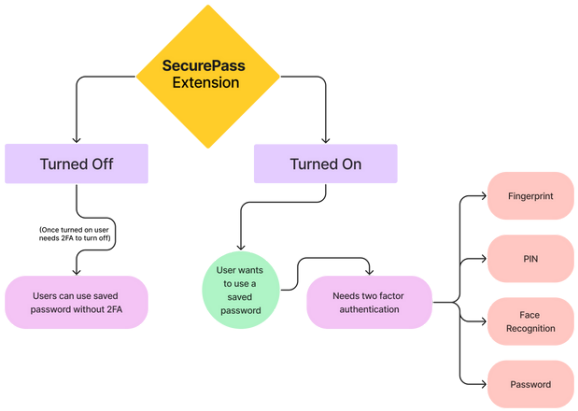
All web extensions offer users two-factor authentication and password management solutions.

Regarding two-factor authentication options, LastPass and Keeper offer the widest variety of authentication methods, including biometric authentication on mobile devices. Dashlane offers a more limited range of options, while 1Password only offers Google Authenticator.

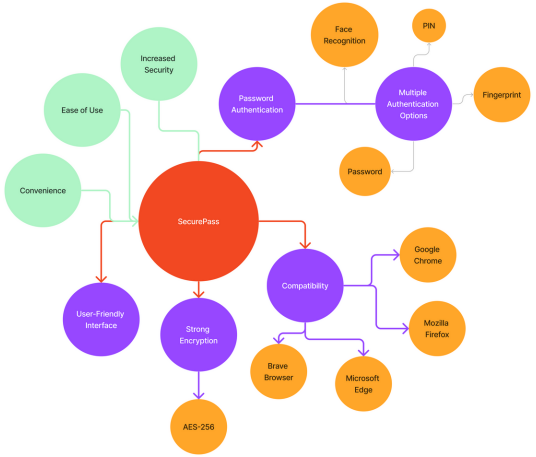
Research



Taskflow



Insights



Lakavath Vasanth Kumar
2020386

Devi Sri Charan
2020412

INDRAPRASTHA INSTITUTE of INFORMATION TECHNOLOGY DELHI