# Investigating the Usability of Password Managers


Dr. Peter Story
pestory@clarku.edu

Adryana Hutchinson
ahutchinson@clarku.edu

Jeffrey Tang
JeTang@clarku.edu


Presenter: Adryana Hutchinson '23, Fall Fest 2022 | Sponsor: Dr. Peter Story

## Introduction

Passwords are one of the most popular forms of authentication [1, 2]. Users often engage in unsafe password behavior, such as creating and reusing guessable passwords. This behavior is not unreasonable, as creating secure passwords places a heavy burden on users [3, 4]. Password managers (PWMs) are able to shoulder this burden by generating and saving secure passwords. Little research has been done on how password requirements can hinder the usability of PWMs on websites, especially on less-visited websites.

- RQ1: How often do websites' password policies disallow passwords generated by PWMs?
- RQ2: Which password policies could websites adopt to maximize their compatibility with PWMs?
- RQ3: Which password generation approaches could PWMs adopt to maximize their compatibility with websites?
- RQ4: What other usability issues do we encounter when signing up for and logging in to websites?

Many different PWMs are available. We decided to test a set of 4 PWMs: Safari's built-in PWM, Chrome's built-in PWM, Bitwarden's Chrome plugin, and Keeper's Chrome plugin.

## Merits & Impacts

- Passwords are often used to safeguard valuable information, such as bank account and social security information.
  - If the passwords are insecure, malicious actors can access private information. This can be detrimental if the same password is used across multiple websites.
- If PWMs are not able to meet user demands, adoption levels will remain meager, leaving users with the task of creating and remembering complex passwords.

## Methods

We chose our 4 PWMs based on the following critera: generation patterns, consistent generation over multiple operating systems, popularity, and open-source status.

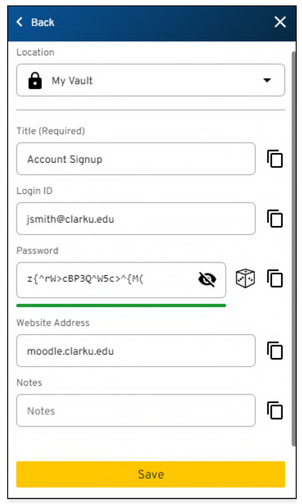


Fig 1: Keeper's PWM interface.

- A diverse set of generation patterns ensure that we are able to catch unique password generation policies.
- Consistent generation patterns ensure our data can be replicated.
- It is crucial to measure the usability of PWMs that users are most likely to use or know about.
- The open-source status of a PWM may play a role in its usability.

**Bitwarden**

| Autogenerated Password | Uppercase | Lowercase | Numbers | Symbols |
|---|---|---|---|---|
| bmypYuCJouE5zL | 5 | 8 | 1 | 0 |
| FinVYkLhWYFkj6 | 7 | 6 | 1 | 0 |
| y9RQB8nDDnksc9 | 5 | 6 | 3 | 0 |

Fig 2: Examples of passwords generated by Bitwarden.

**Chrome**

| Autogenerated Password | Uppercase | Lowercase | Numbers | Symbols |
|---|---|---|---|---|
| rb3EWy7BLUAfoM | 7 | 5 | 2 | 0 |
| NMJmKtBkmoXq5B | 7 | 6 | 1 | 0 |
| AxEq4gh*6f+*hqm | 2 | 8 | 2 | 3 |

Fig 3: Examples of passwords generated by Chrome.

**Keeper**

| Autogenerated Password | Uppercase | Lowercase | Numbers | Symbols |
|---|---|---|---|---|
| 4Ao{S!yiV?uG[,crGr7^ | 5 | 7 | 2 | 6 |
| NqtUTVO,E5t9xw.ww()f | 6 | 8 | 2 | 4 |
| ,YnB4KKFjeEyC9W0$?X{ | 9 | 4 | 3 | 4 |

Fig 4: Examples of passwords generated by Keeper.

**Safari**

| Autogenerated Password | Uppercase | Lowercase | Numbers | Symbols |
|---|---|---|---|---|
| ziPdyx-vevqok-waxju7 | 1 | 16 | 1 | 2 |
| cyMge7-xutwob-viqnin | 1 | 16 | 1 | 2 |
| caksiMdytri1gibsyq | 1 | 16 | 1 | 0 |

Fig 5: Examples of passwords generated by Safari.

We tested our 4 PWMs on 100 unique websites. Usability issues were catergorized into 3 categories:

- Issues due to the website's homepage (e.g., the website being offline).
- Issues on account registration (e.g., a PWM not generating a password, or a website rejecting a password).
- Issues on login (e.g., a PWM not storing the correct username/password).

## Future Work

In order to address RQ1, RQ2, and RQ3:

- Data collection is nearly complete.
- Data analysis is still in progress.

Using both SBO [5] and Tranco [6] data, we want to see if site popularity is associated with how well PWMs work. SBO data contains a log of website domain names that users have logged into. Tranco rank estimates the popularity of a website, with 1 being the most popular.

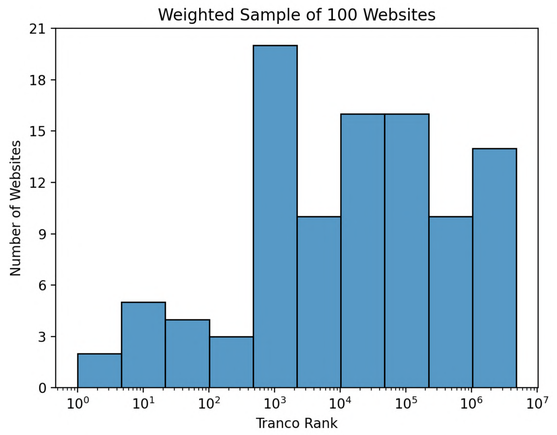


Fig 6: A random weighted sampling of 100 websites and the distribution of their Tranco rank. It is weighted by the number of users that have logged into (have accounts) on that domain. This is how we selected our sampling pool to test both popular and less popular domains.


[1] Cormac Herley and Paul Van Oorschot. *A research agenda acknowledging the persistence of passwords.*
[2] Sunyoung Seiler-Hwang, et al. *"i don't see why i would ever want to use it": Analyzing the usability of popular smartphone password managers*
[3] P. Arias-Cabarcos, et al. *Comparing password management software: Toward usable and secure enterprise authentication.*
[4] Philip G. Inglesant and M. Angela Sasse. *The true cost of unusable password policies: Password use in the wild.*
[5] https://cups.cs.cmu.edu/sbo
[6] https://tranco-list.eu/