Final Report

Group 4

**Improving the Usability of Password Managers**

Submitted December 3, 2019

Caleidgh Bayer, B00672134

André Gagné, B00707964

Sunny Jagasia, B00813395

Sithara Jayachandran, B00824470

Ms Shehzeen, B00812551

Zachary Wilkins, B00725952

## Overview of Proposed Study

Password management is a persistent problem for Internet users in the present day. There is a wide consensus that it is important to choose secure passwords that are not reused on different websites. Unfortunately, many users disregard these advisories.

To address this issue, we want to investigate password managers as a potential solution to this problem. Based on our criteria sourced from the literature in phase 1, we have designed a wireframe prototype. In our proposed study, we will engage participants to discern their thoughts on our prototype, and inform a future, high-fidelity prototype of a browser-based password manager.

The study will be conducted as an anonymous questionnaire that is administered via Google Forms. Users will begin by answering questions about their experiences with password managers, before being walked through our wireframe prototype. After, they will be asked for feedback on particular user interface considerations, as well as their perception of the security requirements in the manager. Finally, they will have the opportunity to provide their overall impressions of the prototype, as well as suggestions for improvement. We will also include questions to collect basic demographic information.

We are not offering financial compensation to our participants, as the time commitment is negligible and the questionnaire can be completed at their convenience. In the process of piloting our study, we found that participants typically took less than 10 minutes to complete the questionnaire. That being said, we aim to develop a working prototype extension that would eventually be available to the public. In that sense, there could be a direct benefit to users who choose to share their time with us, in addition to the indirect benefit of contributing to the scientific process.

We hope that our final prototype can serve as both a useful tool to the Internet community, and a point of inspiration for other password managers who can incorporate our findings into their own work. In this way, we will have contributed to the enhanced security of many user accounts.

## Desired Study Learning Experiences

We have identified two research objectives in our REB application:

1. Understand the rationale and preferences of users who employ password managers
2. Ascertain the usability of our wireframe prototype by comparing responses to UI designs which use opt in/opt out password generation

The first point is rooted in a desire to design a password manager that is optimal for the broadest spectrum of users, ranging in ability from technological novice to computer scientist. In particular, we want to know why users choose to (or choose not to) employ a password manager, the nature of the manager (3rd party vs. built-in, browser vs. operating system keychain, etc.), and what features they expect of their password manager. Another important point is the use of a master password, and what is an acceptable tradeoff between user convenience and account security.

The second point furthers the first by exploring the most effective way to deliver those desired features. This includes user interface considerations such as the various ways of updating previously stored passwords. In particular, we believe that randomly generated passwords are an easy way for users to secure their accounts, and so wish to explore how best to motivate users to employ them. Our hypothesis is that an opt-out system, whereby users need to actively refuse the generator, will be more convincing than an opt-in system.

## Learning Experiences from the Pilot

In phase 2, we piloted our study with peers during lab times. We recruited 24 participants to complete our web-based questionnaire in Google Forms. After conducting our pilot, we were pleased to see broad acceptance of our proposed password manager. Nearly 80% of our participants understood the intended use and functionality of our extension, and 58% indicated that they would consider using it for their daily activities.

Our overall takeaways from the pilot were very positive, and show that users are sympathetic to the realities of managing their own passwords. Specifically, we believe that users will accept a more challenging scheme for their master password in the interest of protecting their other passwords.

In addition, users need to ensure their individual account passwords are effective, and our pilot showed us that two factors may encourage them to do so. The first is to show real-time feedback for users as they enter a password. We theorize that this is because if they are explicitly told they are choosing a bad password, they may reconsider. The second is to prominently place a secure, random, password generator as close to the password field as possible. In our pilot, we found that placing the generator on top of the field was the most effective, and did not hinder user understanding that they could choose their own password. By making password generation an opt-out feature, rather than opt-in, users said they were more inclined to generate a password. In this way, we can discourage them from reusing an old password, or making up an insecure one.

The previous points notwithstanding, we still have areas to improve based on the feedback we received from our participants and our TAs. Accordingly, we have made the following changes to our study design:

* Update opinion-based questions from a 1-3 Likert-type scale (negative, neutral, positive) to a 1-5 scale (very negative, mildly negative, neutral, mildly positive, very positive). This will provide more granularity in the answers we receive from our participants.
* Update the recruitment study population section (2.3.1) of the REB application. In this, we address concerns of sourcing global participants by reducing our geographical requirements, and leveraging the international student population in Halifax.
* Change the master password creation screen to show an example of the password scheme. As well, change the password requirements to be coloured based on whether they have been met (red for unfulfilled, green for fulfilled). We also added a checkmark/cross, to account for users with colour vision deficiency.

Also need:

* DONE Updated REB application (just one page to reprint: recruitment section (p.5 & 6, double-sided)
* DONE Final pilot study prototype (need to update scale to 1-5), consent form, recruitment notice
* DONE Meeting minutes from Nov 29 (presentation day)