How Do Experts Manage Their Passwords?

[Poster Abstract]

Elizabeth Stobert
Carleton University
Ottawa, Canada
elizabeth.stobert@carleton.ca

Robert Biddle
Carleton University
Ottawa, Canada
robert.biddle@carleton.ca

1. INTRODUCTION

Passwords pose a variety of problems for users: random passwords are difficult to create and hard to remember, and keeping track of passwords can be difficult for users who have many accounts. These problems can lead users to adopt sometimes insecure coping strategies [1] such as reusing passwords [2]. Little work exists on the security habits of experts, who must be affected by the same problems that affect all users. If remembering large numbers of random passwords is difficult or near-impossible for non-expert users, it should be similarly difficult for experts. How do expert users cope with their passwords?

Following on our earlier investigation of end users' password management techniques and coping strategies [3], we became interested in the behaviour of expert and power users. How are the practices of those who are knowledgeable about computer security different from or similar to those of non-experts? We conducted a series of interviews with graduate students and researchers in computer security, asking them about their password management behaviour. We found that these knowledgeable users described a dichotomy of behaviour where they employed more secure behaviour on important accounts that they deemed more worthy, but employed similar practices to non-expert users on their remaining accounts.

The goal of our interviews was to better understand the practices of expert users, and to see how they address the demands of creating and managing large numbers of passwords. Do experts rely on similar coping strategies as non-experts? What kind of tools and techniques do they use? We hoped to find insight from the practices and coping strategies of experts that will help us form recommendations for non-experts.

2. STUDY

We interviewed participants about a variety of subjects relating to password management, including creating, reusing, remembering, changing, and forgetting passwords. We took detailed notes and also audio-recorded the interviews. Each interview took about 30 minutes, and had two parts: a short self-administered demographics questionnaire, and the password interview. The study was approved by the Carleton University Research Ethics Board.

We interviewed 11 expert users, primarily recruited from among the information security research groups in the Computer Science Department at ETH Zürich. The majority of our participants were male (9 participants), and participants ranged in age from 24 to 35. All participants except one had a graduate degree in computer security and all were employed either as graduate students or researchers in some aspect of information security.

We analyzed our data by going through open coding, and synthesizing those findings into five themes. Because of space limitations, we present the categorized findings here.

3. RESULTS

The expert users were able to speak knowledgeably and fluently about their password management and security strategies. Participants referenced specific policies, and emphasized the *a priori* nature of their approach.

3.1 Password Selection

Expert participants were not forthcoming about their precise password creation strategies, but they did mention a variety of techniques. One participant used an elaborate password-generation algorithm to create his passwords. His technique included a component related to the website, a random seed, and a personal evaluation of the required security level of the website. Several participants said that they relied on their password manager to generate passwords for accounts, but others said that they did not use this functionality for all accounts. Although participants did not discuss the exact components of their passwords, most participants said that their passwords were rarely rejected for failing to comply with password policies, indicating that these experts were including special characters, digits, and mixed cases in their passwords.

3.2 Password Reuse

Although password reuse is a technique often criticized by security experts, all but one of our participants said that they reused passwords on at least some of their accounts. However, most people described a careful strategy for reuse. Participants often mentioned they did not reuse all of their passwords, but that they had one or two passwords that they consistently reused for "throwaway" accounts. Participants mentioned reusing specific passwords for specific purposes, such as single-use websites, or seldom-visited websites. Participants also described restricting password reuse for other accounts.

> What I perceive as important, which is typically the four or five accounts that I use on a very regular basis, I use unique passwords for all of them. And I believe that these passwords are strong. But on the other hand, I use a common

> password for ... a lot of services that badger you to create an account at times. – E10

When discussing the kind of password that they reused, participants were clear that they had "their" password, often naming it (*e.g.* "my easy-to-steal password" – E09). Multiple participants referenced having had their password since they began using computers.

3.3 Password Recording

About half of the participants said that they wrote some passwords down, and all of these described it as a kind of backup strategy. One participant said he wrote down passwords that were difficult or impossible to change. Another said that when he was issued assigned passwords, he often kept the piece of paper that came with the password. One participant said that he wrote down most of his passwords, but was explicit about how his strategy was intended as a backup strategy for infrequently-used accounts.

> I just keep them written down just in case, and there are those more throwaway accounts that I use once every ... a few times a year, but I need then to check. – E04

All but one participant described using some kind of password manager. Four participants told us they used standalone password managers, and ten participants reported using browser-based managers. Most participants mentioned using more than one tool, and even users of dedicated password managers reported using them alongside the browser-based managers.

Several participants described using a combination of strategies. In particular, multiple participants mentioned using password reuse in combination with password managers. One participant said that he used a password manager to randomly generate and remember passwords for important accounts, but that he opted to reuse passwords instead of storing them in the password manager for insignificant accounts.

> I don't store everything in a password manager. [Why not?] Because I, I dunno, because that's kind of incon-[breaks off] -it's just another layer of inconvenience to use a password manager, and I, for me personally, it's not worth the investment to store it there. And it also kind of clogs my database, I guess, if I would store it in there, the password manager. – E01

3.4 Password Recovery

In the interviews, the expert users demonstrated awareness of specific security threats. When we asked about password changes, several experts referenced having changed their passwords in response to Heartbleed, a security bug in the OpenSSL library that necessitated widespread password changes.

> Well, there's, there's been a couple of incidents like, uhh, my laptop got stolen at one point, or... Or maybe you hear, like, a serious vulnerability like Heartbleed, and that's when you think that, this might be a time to change passwords.– E07

In this quote, the expert participant describes two situations where he changed his passwords. One was a situation specific to him: his laptop was stolen and he was concerned that the thief might have gained access to his accounts. The second was a worldwide security bug that affected millions of users.

4. DISCUSSION & CONCLUSION

The purpose of the expert interviews was to better understand how experts are managing passwords, but also to see what can be learned from the practices of experts and adapted to help non-expert users manage their passwords.

Our interviews suggest that both experts and non-experts tailor their password coping strategies to the specific account requirements, but that experts' consistency gives them an advantage in managing passwords. The experts in our study used password managers in combination with password reuse and other less secure coping strategies. They acknowledged the additional effort of using the password manager, but had selected the accounts where this effort was worthwhile. By using the password manager only on those accounts, they were effectively budgeting their time and effort to protect their most valuable accounts.

Based on these results, we suggest that end users should be able to apply these consistent strategies to strongly protect the accounts they care about most, while not wasting effort on other accounts. The process of setting up a password manager can be daunting to end users, but by selecting a small set of accounts for initial set-up, the task is made significantly smaller. For example, users could select three important accounts, install a password manager, and add those accounts to the manager. Instead of attempting to solve their whole password problem, users should focus on the accounts that matter most to them. This incremental approach is scaleable, and it is possible that once the password manager is set up and in use, the user may want to use it for other accounts.

The experts in our interviews were largely taking advantage of existing tools (open source and commercially available password managers) that are easily available online. We cannot expect that every user will be able to create a robust password generation algorithm, but most of the expert tools are available for use by anyone. This means that the expert approach really is accessible to non-experts.

Of course, expert knowledge does not solve all usability issues with passwords. Problem areas for password management include the usability of password managers and the ease of password changes. Although the expert approach cannot remedy all password management problems, it can suggest practical advice and strategies to help end users manage passwords in their daily life.

5. REFERENCES

[1] A. Adams and M. A. Sasse. Users Are Not The Enemy. *Communications of the ACM*, 42(12):40–46, Dec. 1999.

[2] D. Florencio and C. Herley. A Large-Scale Study of Web Password Habits. In *International World Wide Web Conference*, 2007.

[3] E. Stobert and R. Biddle. The Password Life Cycle: User Behaviour in Managing Passwords. In *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, 2014.