Expert Password Management

Elizabeth Stobert[1] and Robert Biddle[2]

[1] ETH Zürich
Zürich, Switzerland
elizabeth.stobert@inf.ethz.ch
[2] Carleton University
Ottawa, Canada
robert.biddle@carleton.ca

Abstract. Experts are often asked for advice about password management, but how do they manage their own passwords? We conducted interviews with researchers and practitioners in computer security, asking them about their password management behaviour. We conducted a thematic analysis of our data, and found that experts described a dichotomy of behaviour where they employed more secure behaviour on important accounts, but had similar practices to non-expert users on remaining accounts. Experts' greater situation awareness allowed them to more easily make informed decisions about security, and expert practices can suggest ways for non-experts to better manage passwords.

1 Introduction

Security experts are often turned to for advice about password management, but what do experts themselves do to manage their passwords? How are the practices of those who are knowledgeable about computer security different from or similar to those of non-experts?

Little work exists on the password habits of experts, who must be affected by the same problems that affect all users: difficulties choosing random passwords, difficulties remembering passwords, and multitudinous accounts. If remembering large numbers of random passwords is difficult or near-impossible for non-expert users, it should be similarly difficult for experts.

We conducted a series of interviews with researchers and practitioners 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? What differentiates experts from non-experts? We hoped to find insight from the practices and coping strategies of experts to help us form recommendations for non-experts.

In the following sections, we describe our study methodology and present our results. Our interviews yielded a set of descriptive quantitative data as well as a richer qualitative data set. We first present an overview of our interview results, before conducting a thematic analysis of experts' descriptions of their password management techniques. We identify four themes, and use these to better understand the ways in which experts differ from non-experts, as well as to form recommendations for non-expert users. We also identify areas of difficulty: password management problems that even expert knowledge cannot solve.

2 Background

Passwords pose a considerable usability challenge for end users, who are asked to create secure, unique passwords for every account, remember each of those passwords for a long time, and remember which password goes with which account for multiple accounts. These security requirements place demands beyond human capability on users' memory, time, and attention [15], and lead users to create passwords which are memorable, but easily guessed by attackers. This is known as the password problem [31]: passwords that are easy to remember are also easy to guess.

The password problem has existed for most of the history of computing. Morris and Thompson [22] describe the problem in a 1979 article about passwords in the UNIX operating system. However, with the introduction of personal computing and the web, the problem has scaled enormously. Current research continues to find users creating weak passwords [4], and instances of leaked or stolen passwords leading to major losses are increasingly common [8]. The password problem results from a mismatch between security expectations and users' abilities [31], and these disconnects can lead to the misuse or avoidance of security mechanisms [1]. Users may avoid password expectations by writing passwords down, or by reusing the same passwords across multiple accounts [27].

Conventional wisdom concludes that users are lazy and unwilling to comply with security advice. Correspondingly, the conventional suggestion is that users should be motivated to try harder to follow security advice, and be better educated about the dangers of poor security practices. However, the quantity of information that users are expected to remember is arguably impossible for users to memorize [15]. Users often end up ignoring security advice, and Herley [19] argues that these decisions are rational. Not only are password expectations impossible for users to meet, but a cost-benefit analysis of following security advice suggests that users should not even try [19].

2.1 Coping Strategies

Reusing Passwords One technique for coping with the demands of multiple passwords and accounts is to reuse passwords across multiple accounts. Reusing passwords carries security risks because an attacker may be able to uncover a

password for one website and then use that password to attack a user's other accounts (e.g., through the leak of a password database). In spite of these risks, almost all studies of password use have uncovered password reuse [14, 16, 18, 24, 25, 32]. Notoatmodjo [24] found that reuse increased with the number of users' accounts, and that most users cited increased memorability as the reason for reusing passwords. Reuse is a simple and intuitive coping technique that scales well to handling password meters [9], and coping with password policies [25].

Empirically tracing the extent of password reuse can be difficult. Das et al. [7] examined leaked datasets from 10 websites, and found that 43% of all passwords in their data set were reused across multiple accounts. They showed that knowledge of password reuse (via cross-referenced usernames) can be leveraged for more efficient password attacks.

Even when users do not completely reuse passwords, they often reuse pieces of passwords, or make minor modifications when using a password on another website. Most transformations take place at the beginning or end of a password, and the most common transformations are to add a number, symbol, or capitalization to comply with a new password policy [7, 30]. Users often retain fragments of existing habits and passwords across the creation of new accounts and changes in policy, leading to long-term reuse [28].

Writing Passwords Down Another coping strategy that users adopt for remembering passwords is to write passwords down. Writing passwords down can allow users to select and remember more complex passwords, as well as a higher number of passwords, but can have security risks if an attacker were to discover the list of recorded passwords.

Many users write down some or all of their passwords. Zviran and Haga [32] asked users about their password recording practices, and found that 35% of their participants wrote down their passwords, and the most common storage locations for recorded passwords were wallets, notebooks, and calendars. No relationship was found between password characteristics (length, composition) and likelihood of password recording, but participants were significantly more likely to write down passwords that were difficult to remember, or used infrequently. Grawemeyer and Johnson [17] found that writing passwords down was a coping strategy used to complement password reuse. They found that users were almost 18 times more likely to record unique passwords than reused passwords.

An important issue for recorded passwords is how they are stored: if securely stored, writing passwords down can be a perfectly acceptable technique for aiding users with passwords. Shay et al. [25] asked users how they protected their recorded passwords and found that about 30% of people did not protect them at all. Of the remaining 70%, strategies were varied, but included hiding the list of passwords, or storing it on another computer or device with a password.

2.2 Security Practices of Experts and Non-Experts

Quite a lot of work has focused explicitly on non-expert users. Wash [29] investigated non-experts' mental models of security, and found that users have often

inaccurate folk models of viruses and hackers that affect how users perceive and react to threats. Wash theorized that botnets behave in ways unanticipated by users' mental models, allowing botnets to propagate unnoticed. Stobert and Biddle [27] interviewed non-expert users about how they create, keep track of, and remember passwords. They found that users' passwords move through a life cycle where they are created, reused, and adapted into subsequent passwords.

Work comparing experts with non-experts has generally found that experts focus on different parts of the problem than non-experts. Asgharpour, Liu and Camp [3] had experts and non-experts participate in a card-sorting experiment to elicit mental models of security. They found that expert users' mental models of security differed from those of non-experts, and that a physical security metaphor was likely to be useful for framing computer security messages. Kang et al. [21] investigated users' mental models of the internet and examined perceptions of security and privacy online. They distinguished lay participants from technical participants and found that technical participants actually took fewer steps to protect themselves online. Their results showed that both lay and technical participants suffered from high levels of uncertainty around how information is collected and shared online. Although technical participants had different concerns than the lay participants, all were somewhat affected by not knowing how to handle the problems.

Ion, Reeder, and Consolvo [20] examined the security practices of expert users in a survey-based study. They examined exclusive practices of experts vs. non-experts and found that experts were more likely than non-experts to install system updates, use two-factor authentication, and use a password manager to stay safe online. Experts were likely to mention "unique" passwords and the use of password managers, while non-experts discussed "strong" passwords and password change policies. Non-experts were also more likely to say that they visited only known websites, changed passwords regularly, and used antivirus programs to stay protected from security threats.

Norman [23] reports anecdotal evidence that experts reuse and record passwords to handle the difficulty of remembering secure passwords. He reported that many security professionals told him that they reused two passwords: a strong password and a weak password. For accounts with unusual password requirements, they reported writing passwords down.

3 Study

To investigate how computer security experts manage their passwords, we conducted a series of semi-structured interviews. We interviewed participants about a variety of subjects relating to password management, including creating, reusing, remembering, changing, and forgetting passwords. The interviews were conducted by the researcher, who asked questions and recorded responses. The interviews were also audio-recorded to facilitate further note-taking. We chose our methodology so that participants could reflect on and discuss not only what they do, but why they do it. We encouraged participants to elaborate on incomplete

answers and to pursue alternative discussion paths that revealed the details and complexity of their password management strategies. To allow comparison with earlier research on coping strategies and the password life cycle, we used the same interview script and elicitation techniques as in [27]. Participants were not given the interview questions in advance.

The interview had two parts: a short self-administered demographics questionnaire, and the password interview. The study was approved by the ethics committees at Carleton University and at ETH Zürich. We emphasized to participants that they should not share their passwords with us, and that all interview questions were optional. The interviews took approximately 30 minutes. Participants were not paid, but were happy to participate because of their interest in the topic.

We interviewed 15 expert users, recruited from the community of industry security practitioners and from among the information security research groups at ETH Zürich. Reflecting the gender distribution of the security community, the majority of our participants were male (13 participants). Participants ranged in age from 24 to 35, with a median age of 29. All participants except two had a graduate degree in computer security and all were employed as researchers, graduate students, or practitioners in information security.

Our interviews resulted in two datasets: a quantitative dataset of participants' specific responses to yes/no and quantitative questions, and a qualitative dataset of participants' explanations and detailed responses. During the interviews, we took detailed notes about each participant's responses. Later, we returned to the audio recordings to add detail to the notes taken during the interviews and to transcribe quotes. We summarize the results of our interviews in Section 4.

We conducted a thematic analysis of our qualitative data (Section 5), using methodology described by Braun and Clarke [5]. We chose thematic analysis for its flexibility and because it allowed us to explore the depth of our data and better understand the commonalities of participants' discussion and responses. We familiarized ourselves with our data by listening to the audio-recordings while reviewing and adding to the notes made during the interviews. We then began the process of open coding, where we identified ideas present in the data and assigned each idea a code. Next, we identified themes resulting from the coding process. We copied our codes onto post-it notes, and manipulated them on a whiteboard, where we could draw around them and use mind-map techniques to identify and refine themes. Finally, we considered our themes in relation to each other, and how they fit into the overall story of the data.

4 Results Overview

The expert participants in this study had a median of 64 accounts, and reported using a median of ten accounts in an average week. They reported wide ranging numbers of unique passwords, from 4 to 200, with a median of 58.

We were very clear that participants should not share their passwords with us, and experts were understandably private about their exact password creation strategies. Several participants mentioned algorithmic password creation strategies that integrated different pieces of information into passwords. All but one of these participants mentioned using this technique alongside reused passwords, and the remaining participant relied exclusively on this kind of algorithmic scheme. This participant had an elaborate password-generation algorithm that included a component related to the website, a random seed, and a personal evaluation of the required security level of the website.

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 capital letters in their passwords.

> All the passwords have capital letters usually... it's more sometimes they say "okay, you have two strange characters", like unsupported special characters and you have to delete this, and it's a bit annoying. – E08

Although password reuse is a technique often criticized by security experts, the majority of our participants (12 out of 15) said that they reused passwords on at least some of their accounts. Of those participants who reported reusing passwords, all said they reuse multiple passwords. The median number of reused passwords was 3.5. Most participants 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.

> [Do you reuse multiple passwords?] Yep. [How many?] Four. Four different ones that have different behaviour in terms of complying to bullshit regulations like numbers, or punctuation, or ... – E03

Conversely, participants also described restricting password reuse for 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 bootstrap password" – E14). Multiple participants referenced having had their password since they began using computers and one mentioned having had their password since high school.

We asked participants about how they stored passwords, and most (12 out of 15) reported storing their passwords in a computer program. Of these, six participants reported using a dedicated password manager, and the rest reported

storing their passwords in a web browser. Nine participants told us that they wrote their passwords down. Eight of these specified that writing their passwords down was something they did rarely, and only when unavoidable (e.g., in the case of an assigned password that they could not remember); the remaining participant treated his list as a kind of password manager, but also said one of the purposes of his list was to give to family members in case of emergency.

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 (in spite of using a password manager to save passwords). Some participants described only generating random passwords for certain accounts, and most often said that they used this functionality for high-importance accounts.

Participants reported that they enter their passwords on a variety of device types, including smartphones, tablets, laptops and desktops, but most said that when creating passwords, they did not consider the entry device. Two participants mentioned shortening their passwords, or avoiding special characters when they knew they would be entering the password on a smartphone. One participant said that when using a regular keyboard, they tried to create their passwords so that all characters requiring the use of the "shift" key were next to each other.

Slightly less than half of the participants (7 out of 15) reported that they will enter their passwords on computers belonging to friends or family members, but most qualified the statement by mentioning that they would only log into certain accounts on other people's computers. Those who said that they would not enter their passwords on systems not managed by them said that this was a deliberate and strict policy for them.

5 Thematic Analysis

We began our thematic analysis with the process of open coding. We traversed the notes from our interviews, assigning codes to the data. To gain greater familiarity with the data, we relistened to the audio recordings of the interviews and took additional notes, which we then coded. We identified a total of 30 codes, and a list of all the codes used is included in Table 1.

Following the process of open coding, we began the process of identifying themes and relationships in the data. We identified four broad themes in our data, each of which answers some aspect of our research question: how do experts manage passwords?

5.1 Expert Awareness

During the interviews, it was clear that a key strategy for expert participants was to have consistent and pre-planned strategies. Experts were able to speak knowledgeably and fluently about their password management and security strategies. They were familiar with what they do to address security and often anticipated subsequent questions in the interview. While this familiarity is no doubt due to

Table 1. Complete list of all the open codes used in the analysis, organized by theme.

Code name	Description
Expert Awareness	
Consistency	Showed evidence of consistent habits (between accounts, or over time).
Algorithmic/deterministic	Generates passwords according to deterministic strategy or algorithm.
Exceptions to the rule	Discussed situations where consistency is damaged because of other factors.
Threat awareness	Shows awareness of specific security risks.
Family/friend trust	Describes special trust for friends or family.
Resets as coping strategy	Uses the password reset mechanism instead of remembering passwords.
Combining Strategies	
Variations on a theme	Describes creating passwords that are slight variations on each other.
Go-to password	Describes a particular password that is often reused.
Combination of strategies	Describes combining strategies.
Password manager as coping strategy	Uses password manager to cope with some difficulty of passwords.
Writes as backup	Writes passwords down as an insurance strategy (rather than to use often).
Records on paper	Writes passwords down on paper.
Records electronically	Writes passwords down in an electronic document (e.g., email, word document).
Personal Assessment of Risk	
Personal categorization	Organizes accounts by some "personal" strategy.
Security categorization	Organizes accounts by security.
Service-based categorization	Organizes accounts based on the website service.
Financial categorization	Organizes accounts based on money-based considerations.
Frequency-based categorization	Organizes accounts based on frequency of use (both frequent or infrequent).
Hidden category	Has accounts that belong to a category based on their non-dominant categorization.
Personal assessment of risk	Indicated that their assessment of risk was specifically applicable to themselves.
Usability Problems	
Usability problems	Describes usability problems.
Privacy	Describes privacy concerns.
Lack of control	Describes situation where control is lost.
Memory problems	Describes problems remembering information.
Password manager usability	Describes usability problems with password managers.
Username problems	Describes problems with usernames.
Limited online presence	Describes minimizing their online presence to avoid coping with security problems.
Broad online presence	Describes having many accounts.
Change of behaviour	Describes a situation where they changed their practices.
Self-dictionary attack	Guesses at own passwords.

the fact that these participants spend large amounts of their lives considering security, it also seemed to highlight the *a priori* nature of the expert approach. These participants referenced specific policies, and as in the following quote, were emphatic about avoiding certain situations.

> [Do you ever enter your passwords on computers that don't belong to you?] No. This is something I really try to avoid. – E08

Experts were specific about how they create and adapt passwords, and when asked the same question in different contexts, they often showed confusion about why the question was being asked again. Our interview asked about password creation when creating a new account vs. resetting a forgotten password, and at the second question, many participants gave us answers such as:

> [If you do have to reset a password because you don't remember it, how do you pick the new password?] Uh, I mean [it] is the same technique as I used before. – E02

Experts also showed awareness of specific threats in the interviews. 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 [6].

> 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, that this might be a time to change passwords.– E07

The experts in our study sometimes mentioned planning for failure. Many participants reported using the password reset feature on a regular basis, and participants often planned to rely on this mechanism rather than going to the trouble of keeping track of an unusual password (e.g., one that deviated from their predictable password algorithms.) In these situations, participants were effectively planning on forgetting their password, relying on other existing mechanisms to save them. For accounts used infrequently, the trade-off of login time against convenience appeared to be worthwhile.

Planning for security can be made difficult by the myriad other pressures and unexpected situations that can arise, and experts did mention these situations that forced them to deviate from their preferred strategies. Among the situations described in the interviews were the pressures of friends and family, as well as unforeseen circumstances where information needed to be retrieved. The social and contextual pressures that affect everyone also affect computer security experts.

> I can be as paranoid as I want, but you know, in the real world I have a family and stuff, so sometimes you have to make compromises. – E15

5.2 Combining Strategies to Remember Passwords

Participants described a number of strategies for managing their passwords and accounts, and unexpectedly, many participants described using more than one technique, depending on the account.

Almost 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 (e.g., a letter with a PIN sent by the bank). 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

Some participants described writing down other pieces of information as a backup strategy. One participant who had an algorithmic password generation strategy said that he sometimes wrote down the year that he had created the password for a specific account. Together with his memorized algorithm, this small piece of information was sufficient for him to regenerate the passwords.

Twelve participants described using some kind of password manager to save passwords. Six participants told us they used dedicated password managers, and eleven participants reported saving passwords in the web browser or in applications. 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... 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

In this quote, the participant describes the inconvenience of the password manager. Although he uses the manager, he weighs the inconvenience of the password manager against the significance of the account before deciding if he will use the manager for that account. Another participant described the same technique, but said that he made his decision on whether the website collected financial information. Yet another participant described a kind of thresholding process for determining which accounts got added to his password manager:

> If [password resets] happens more often than, I don't know, a bunch of times, then I will just use 1Password to remember that password. – E09

5.3 A Personal Assessment of Risk

Experts often explicitly mentioned the personal assessment of risk that played a role in their password management and creation strategies. One of the problems of computer security is that it can be difficult to know how well an account is protected, and to what level an account needs protection. Even with the additional experience and knowledge that accompanies expertise, it is hard to know exactly how specific decisions and choices will affect the protection of an account. In the following quote, the participant corrects himself to clarify that his classification of his two passwords as secure is based on his own judgment:

> I have two passwords that are, um, that I *consider* to be more secure, and that I use for only few things, but yeah, I consider more valuable. – E04

This idea of personal assessments of security came up repeatedly in the interviews, often in the discussion of a categorization strategy for accounts. Participants remarked on a number of categorization factors, including money/financial information, service-based categorization, or simply "importance".

> The first ingredient is the security level of the service, that I personally think it falls into this category. So for Amazon I would identify the security level I think Amazon should have in my world and then this is the first ingredient of the password. – E05

These strategies were often vaguely defined, and experts sometimes acknowledged their own inconsistency.

> I actually buy train tickets with this [password], but, yeah, I am contradicting myself because buying a train ticket involves money but I don't really care! – E11

Experts were clear in the interviews that objective assessments of security are difficult to make, and almost every description of a password management strategy mentioned this in some way. Experts did not express hesitation or concern about these decisions, but they were quick to clarify that many of their security assessments were particular to them. Having the awareness and ability to make these decisions quickly and relatively accurately is a hallmark of expert password management.

5.4 Usability Problems

Even though passwords are presumably a subject of interest for people employed as security experts, our participants still described difficulty and frustration with password management. One participant described assigned random passwords as "ridiculous string[s] of horror"(E03). Participants described a number of ways

in which they anticipated and experienced usability problems with passwords. Several participants said that they did not expect to remember passwords that were modified to comply with unusual password policies, and one participant described problems remembering the usernames associated with passwords.

One participant gave a long description of usability problems resulting from an unusual password policy and his reliance on the password reset mechanism.

> If all of them reject the password policy, then I would take the simplest one and do minimum compliance to make it fit their policy, and then any time I ever want to use it again, I wouldn't remember it, because of this, and if they told me this was their policy I would remember but as it is I wouldn't have any clue and I would get angry and frustrated and say "remind me my password" and they would send it to me and I'd be like "oh right, I forgot about this silliness." Or actually, no, what would happen is they would say "ok, reset your password" and then I would click the reset password and I would try to enter the simple password, it would reject it and explain the policy, and then I would remember what it was, the old one, but it was already too late because I had said reset the password and need to enter a new one. Yeah.– E03

This quote describes not only anger and frustration, but the additional time and effort that result from invisible password policies. In this description, the user enters multiple known passwords, creates a new password, revisits the website, logs into his email, clicks a reset link, and chooses another new password. This is a lot of work to log into an account!

Only a few expert participants described changes of behaviour related to security, but when they did, changes related to usability problems rather than to security concerns. One participant said they started using a password manager when they could not remember all of their passwords, but another participant said that they had stopped using a password manager because the built-in browser password manager filled their needs.

> [Do you use any kind of dedicated password manager?] Not at the moment, no. [Have you in the past?] I have tried. [What didn't work out?] Ummm. I guess I would say that in the situation as now, my browser remembers my passwords and that's somehow sufficient for me. My mobile remembers my passwords, so I, at the moment, I don't really feel the need for a separate password manager. – E07

A few participants described making efforts to minimize their online presence to avoid dealing with security and passwords. One participant told us how he avoided creating and managing passwords by relying on his spouse:

> I try to shove off all my passwords to let [my partner] manage it. – E10

The usability problems of passwords also lead experts to make mistakes: experts mentioned a number of practices with obvious security vulnerabilities. Since experts are presumably aware of these weaknesses, it is telling that they

have chosen to trade off security for usability in certain situations. Two participants said that they sometimes created passwords using dictionary words from their non-English mother tongue. Dictionary words in any language are easy for an attacker to guess.

> I sometimes do pick words from my native language because they almost look like a garbled set of characters in English, and then it's highly unlikely that somebody gets it. – E10

Another insecure practice mentioned by experts was guessing at their passwords. If an attacker is collecting password entries, guessing multiple passwords can quickly leak many passwords to an attacker. More than one participant referenced this technique, though most did clarify that they would only turn to it for low-value accounts.

> Since those belong mostly to throwaway accounts, I will just try another variation or try another one of my standard set of passwords. – E01

6 Discussion

Experts make use of many of the same coping strategies that are well-documented for non-experts. They reuse passwords, write passwords down, and create new passwords by making slight variations of older passwords. However, they combine these possibly insecure strategies with more careful habits for accounts where they are strongly concerned about security. One way they accomplish this is by using a password manager to generate and store passwords for high-value accounts, while reusing old passwords across other, lower-value, accounts.

The segmentation of strategies and clear division between important and unimportant accounts is what distinguishes expert behaviour from non-expert behaviour. Experts carefully plan to treat certain accounts more carefully than others. However, other studies [27, 20] have shown that non-experts try to use similar strategies. What allows experts to be more successful than non-experts?

Defining expertise is problematic, but it is usually agreed that an expert is someone with high knowledge in a certain domain and who is successful in that domain [12]. For example, an expert in chess is someone who is deeply familiar with the rules and strategy of the game, and is able to use this knowledge win many of their games. However the notion of success is less clear in personal practice with passwords. How exactly can it be shown that someone is more successful at managing their passwords than another person? How can we know that a lack of security breaches is due to good management and not due to luck?

In "ill-structured problems" [26] such as computer security, Endsley [11] argues that expertise comes from skilled decision making, which is enabled by *situation awareness*. Situation awareness is "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future."– [10, p.97]. Along with specialized skills and high knowledge in a domain, strong situation awareness contributes to expertise.

Experts with high situation awareness have learned knowledge and skills, schemas for prototypical situations, mental models of the domain, and automatic processes in the domain [11]. In our interviews, experts demonstrated all of these characteristics. They had high knowledge of the security domain and awareness of specific threats. They recognized the kind of password-related scenarios they had encountered in the past, and remembered their behaviour in those situations. They had mental models of threats and defences for those threats, as well as for which accounts were susceptible to which threats. Finally, the experts in our study had clear and automatic processes for how to create, remember, and reuse passwords in prototypical situations.

Although someone may have good situation awareness and expertise in one area of their domain, they may not maintain that awareness and expertise when handling novel situations [11]. Most of the password management scenarios discussed in our interviews were fairly routine, but participants repeatedly mentioned the frustration of situations where (for example) an unusual password policy forced them to change their password creation algorithm. In these situations, experts are no longer experts because they have lost some of their situation awareness.

6.1 What Do Experts Do Right?

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.

Together with other studies [27, 20], our interviews suggest that both experts and non-experts treat accounts with different requirements differently, but that the 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 a 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. Experts' additional situation awareness of security allowed them to make effective decisions about where to place their time and energy, and how to prioritize good security practices for important accounts.

Many of the habits and behaviours described by experts are accessible to anyone. Experts mostly mentioned using 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 many of the expert behaviours were similar to the practices of non-experts, and the additional software they used was available to anyone. But how we can help non-experts develop situation awareness to help them make informed decisions about security?

One way in which we can increase situation awareness for end users is to make security policies as transparent as possible. The potential presence of an attacker complicates this, but often-seen strategies such as obscuring the password policy

do little to discourage attackers, while complicating the situation for end users. Presenting information such as password rules and policies at password creation, and making log information about the time and location of logins available to users could potentially help them better manage their accounts.

Helping users develop schemas and good mental models for security is more difficult. Security is a secondary task and users are typically uninterested in the topic. Security and password management tasks are also distributed across many websites and accounts, with no central place through which to monitor them. Password managers create a central place through which passwords are created, saved, and monitored, and this could potentially help end users' situation awareness of their own passwords. Password managers provide users with a list of all their passwords, so users can see where they are reusing passwords, and in the case of a known vulnerability, make it easier for users to change affected passwords. Password managers could also help users by bringing vulnerabilities and compromises to users' attention. Some commercial password managers already do this: 1Password provides a service called Watchtower that allows users to identify services that are vulnerable to Heartbleed [2], and LastPass has a "Security Audit" feature that identifies passwords that occur in leaked datasets [13].

We suggest that end users should be able to develop 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, but by selecting a small set of accounts for initial setup, 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.

6.2 What Do Experts Do Wrong?

Though the habits and knowledge of experts can help address some of the issues with passwords, other problems still remain. Here, we highlight a few issues that were identified as problems during the interviews.

Password changes were a source of tension for most users. Experts were more likely to say that they changed their passwords than non-experts [27], but most experts said they changed their passwords only rarely and commented on the difficulty of the process. Participants commented on how the password change process can look different for every website, and finding the correct page and going through the password change process can be time-consuming. Password changes also affect the usability of password managers. To take advantage of the random password generation functions in most managers, passwords for existing accounts must be changed. This process can discourage all kinds of users from adopting password managers. Making password changes simpler could both encourage the adoption of password managers and improve security for users who want to change their passwords.

A lurking theme in our interviews was the usability of password managers. Although none of the experts in our study complained about the usability of their password managers, their unwillingness to make them their default password management strategy seems to point to some kind of issue with their usability or usefulness. Since their usefulness is evident, the issue is likely usability. Since there were no specific complaints about particular managers, the issue might simply be that password managers require an additional effort and a few extra clicks when logging into websites. Another possible issue here might be trust. A few participants did mention trust, and those that did had a personal rationale for why they did or did not choose to trust password managers. Interestingly, these personal rationales were not particularly similar to each other, and experts clearly put value on different parts of the security ecosystem.

7 Conclusion

Password management can be a struggle for everyone, even experts in computer security. Our interviews with experts about their password management habits showed that they use a combination of password management strategies to carefully allot appropriate security to individual accounts. Several experts relied on password reuse and other less secure coping strategies for lower-value accounts, but used a password manager to generate and remember random passwords for high-security accounts. Experts' increased situation awareness allowed them to more easily make informed decisions about their password management tasks.

The expert approach suggests that all users could improve their password management strategies by increasing their situation awareness of security. One way to do this might be to use a password manager for their most valued accounts. Explicitly identifying a small number of high-priority accounts is a natural extension of end users' existing strategies, and the comparatively small effort to better protect those accounts could significantly improve users' security. Additionally, this incremental approach could scale to protect more than just the most valuable accounts and could foster better password habits for all accounts.

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.

Motivations are complex, and it is difficult to know how individual biases and perspectives may affect our results. A limitation of interview studies is that we do not examine users' actual behaviour in the real world, and it can be difficult to know how factors such as reputation affect participants' responses. However, by probing responses and encouraging participants to thoughtfully examine and explain their comments, we hope that we have provided an initial perspective on the area, and that these results can be used to help inform security solutions for both end users and experts.

8 Acknowledgements

We would especially like to thank all of the computer security experts who lent their time, experience, and insight to our interviews. We also acknowledge support from the Natural Sciences and Engineering Research Council of Canada: Discovery Grant RGPIN 311982-2010.

References

1. A. Adams and M. A. Sasse. Users Are Not The Enemy. *Communications of the ACM*, 42(12):40–46, Dec. 1999.
2. AgileBits. 1Password Watchtower, 2015. `https://watchtower.agilebits.com`.
3. F. Asgharpour, D. Liu, and L. J. Camp. Mental Models of Security Risks. In *Financial Cryptography (FC)*, pages 367–377. Springer, 2007.
4. J. Bonneau. The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. In *Proceedings of the 33rd IEEE Symposium on Security and Privacy*, pages 538–552. IEEE, 2012.
5. V. Braun and V. Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, Jan. 2006.
6. Codenomicon. The Heartbleed Bug, Apr. 2014. `http://heartbleed.com`.
7. A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. Wang. The Tangled Web of Password Reuse. In *Network and Distributed System Security Symposium (NDSS)*. Internet Society, Feb. 2014.
8. eBay. eBay Inc. To Ask eBay Users To Change Passwords, May 2014. `http://www.ebayinc.com/in_the_news/story/ebay-inc-ask-ebay-users-change-passwords`.
9. S. Egelman, A. Sotirakopoulos, I. Muslukhov, K. Beznosov, and C. Herley. Does My Password Go Up to Eleven?: The Impact of Password Meters on Password Selection. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*, pages 2379–2388. ACM, 2013.
10. M. R. Endsley. Design and Evaluation for Situation Awareness Enhancement. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, pages 97–101, 1988.
11. M. R. Endsley. Expertise and Situational Awareness. In K. A. Ericsson, N. Charness, P. J. Feltovich, and R. R. Hoffman, editors, *The Cambridge Handbook of Expertise and Expert Performance*. Cambridge University Press, Cambridge, 2006.
12. K. A. Ericsson. An Introduction to the Cambridge Handbook of Expertise and Expert Performance. In *The Cambridge Handbook of Expertise and Expert Performance*, pages 3–20. Cambridge University Press, Cambridge, 2006.
13. J. Fitzpatrick. How to Run a Last Pass Security Audit (and Why It Can't Wait), Dec. 2013. `http://www.howtogeek.com/176038/how-to-run-a-last-pass-security-audit-and-why-it-cant-wait/`.
14. D. Florencio and C. Herley. A Large-Scale Study of Web Password Habits. In *International World Wide Web Conference (WWW)*. ACM, May 2007.
15. D. Florencio, C. Herley, and P. C. van Oorschot. Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts. In *Proceedings of the 23rd USENIX Security Symposium*. USENIX, Aug. 2014.
16. S. Gaw and E. W. Felten. Password Management Strategies for Online Accounts. In *Proceedings of the 2nd Symposium on Usable Privacy and Security (SOUPS)*. ACM, July 2006.

17. B. Grawemeyer and H. Johnson. Using and Managing Multiple Passwords: a Week to a View. *Interacting with Computers*, 23(3):256–267, May 2011.
18. E. Hayashi and J. Hong. A diary study of password usage in daily life. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI)*. ACM, May 2011.
19. C. Herley. So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In *Proceedings of the 2009 Workshop on New Security Paradigms (NSPW)*. ACM, Sept. 2009.
20. I. Ion, R. W. Reeder, and S. Consolvo. "...no one can hack my mind": Comparing Expert and Non-Expert Security Practices. In *Proceedings of the 11th Symposium on Usable Privacy and Security (SOUPS)*. USENIX, July 2015.
21. R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Proceedings of the 11th Symposium on Usable Privacy and Security (SOUPS)*. USENIX, July 2015.
22. R. Morris and K. Thompson. Password Security: a Case History. *Communications of the ACM*, 22(11):594–597, Nov. 1979.
23. D. A. Norman. When Security Gets in the Way. *ACM SIGCSE Bulletin*, 16(6):60, Nov. 2009.
24. G. Notoatmodjo. Exploring the 'Weakest Link': A Study of Personal Password Security. Master's thesis, The University of Auckland, New Zealand, Nov. 2007.
25. R. Shay, S. Komanduri, P. G. Kelley, P. G. Leon, M. M. Mazurek, L. Bauer, N. Christin, and L. F. Cranor. Encountering Stronger Password Requirements: User Attitudes and Behaviors. In *Proceedings of the 6th Symposium on Usable Privacy and Security*. ACM, June 2010.
26. H. A. Simon. The Structure of Ill-Structured Problems. In *Models of Discovery*, pages 304–325. D. Reidel Publishing, Dordrecht, 1977.
27. E. Stobert and R. Biddle. The Password Life Cycle: User Behaviour in Managing Passwords. In *Proceedings of the 10th Symposium on Usable Privacy and Security (SOUPS)*. USENIX, July 2014.
28. E. von Zezschwitz, A. De Luca, and H. Hussmann. Survival of the Shortest: A Retrospective Analysis of Influencing Factors on Password Composition. In *Proceedings of the 14th International Conference on Human-Computer Interaction (INTERACT)*. Springer, July 2013.
29. R. Wash. Folk Models of Home Computer Security. In *Proceedings of the 6th Symposium on Usable Privacy and Security (SOUPS)*. ACM, July 2010.
30. M. Weir, S. Aggarwal, M. Collins, and H. Stern. Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords. In *Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS)*. ACM, Oct. 2010.
31. S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon. PassPoints: Design and Longitudinal Evaluation of a Graphical Password System. *International Journal of Human-Computer Studies*, 63(1-2):102–127, July 2005.
32. M. Zviran and W. J. Haga. Password Security: An Empirical Study. *Journal of Management Information Systems*, 15(4):161–185, 1999.