The Password Life Cycle: User Behaviour in Managing Passwords

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

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

ABSTRACT

Users need to keep track of many accounts and passwords. We conducted a series of interviews to investigate how users cope with these demanding tasks, and used Grounded Theory to analyze the interview results. We found that most users cope by reusing passwords and writing them down, but with a rich variety of behaviour and diverse personalized strategies. These approaches seem to disregard security advice, but at a detailed level they involve perceptive behaviour and careful self-management of user resources. We identify a password life cycle that follows users' password behaviour and how it develops over time as users adapt to changing circumstances and demands. Users' strategies have their limitations, but we suggest they indicate a rational response to the requirements of password authentication. We suggest that instead of simply advising against such behaviour, new approaches could be designed that harness existing user behaviour while limiting negative consequences.

1. INTRODUCTION

Passwords present a difficult task for users. Users are told not to create weak passwords, not to reuse passwords on multiple accounts, and not to write their passwords down. Yet users have many passwords and are expected to create a password for every new service. Often, users are required to change their passwords at regular intervals. Taken as a whole, these requirements are difficult, if not impossible, for users to meet. In response, users develop strategies for coping as best they can. We wish to explore and understand these strategies, in the hope of identifying new ways to alleviate the difficulties.

We conducted interviews with users to find out about their coping strategies. We asked about how many accounts and passwords they have, how they create and reuse passwords, and how they handle password changes. We encouraged participants to discuss their experiences in detail, and share their motivations, fears, and password tricks.

Some findings were unsurprising. Users do write passwords down, and do reuse passwords. However, these are simplifications of their actual behaviour that do not tell the whole story. For example, users often write down passwords as a fallback strategy, and when they reuse passwords, they often adapt them for different accounts. We analyzed our interviews using the Grounded Theory methodology and identified some important patterns in user behaviour. We identified a "life cycle" of password use, where the user's central concern is rationing effort to best protect important accounts. Many of the specific practices are already known, and our contribution is the identification of a coherent model that highlights a consistent series of gaps between user behaviour and current tool support. We suggest that this model can inform better ways to support users in their behaviour, rather than providing unrealistic guidance.

In the following section, we outline related work. We then describe our methodology and the details of our interviews. Section 4 presents an overview of the results, and Section 5 documents the step-by-step process of our qualitative analysis. We then suggest some implications of our findings, and our conclusions.

2. BACKGROUND

Alternatives to passwords exist in the form of biometrics and security tokens, but these have issues with privacy, theft, and the huge infrastructural costs of deployment and maintenance.

Deployed solutions to the password problem consist mainly of password managers, which store and enter users' passwords, thus saving the user from remembering their passwords or which passwords are associated with which accounts. Browser-based password managers save passwords when they are typed into the appropriate fields, and then automatically input them when the page is visited again (often without authentication). Dedicated password managers (such as LastPass [14]) typically work in one of two ways [7]: they either generate a password at login by hashing the user's master password together with information from the website, or they store the user's passwords in a password "wallet" which is protected by a master password (which may be required at every login).

Existing research on password managers has shown that they can have usability problems that affect their ability to securely manage users' passwords. A study of two password managers found that both managers had significant usability issues [7]. Worse, participants had poor mental models for how the software worked, and these poor mental models led

Symposium on Usable Privacy and Security (SOUPS) 2014, July 9–11, 2014, Menlo Park, CA.

them to make dangerous and unrecoverable security errors.

Another solution to the password problem is single sign-on, where one party authenticates users for multiple websites. At login, the user presents their credentials to the authenticating party, who checks the credentials and relays the results to the website. Examples of single sign-on entities are Facebook, Google, and OpenID. A study of OpenID [20] found that adoption was hindered because it did not fit into users' existing password management techniques, and users were concerned about trusting a single entity to login to multiple sites.

A mismatch between security expectations and users' abilities has long been identified, and users develop coping strategies as a response. These disconnects can lead to the misuse or avoidance of security mechanisms [2].

One coping strategy for having multiple passwords is to reuse passwords across multiple accounts. This strategy is widely employed by users [10, 9, 11], but has security risks. If a reused password is discovered (e.g., through a leaked password set), an attacker may be able to gain access to several accounts. Das et al. [8] found that 43% of all passwords in their data set were reused across multiple accounts, and showed that password reuse can be leveraged for more efficient password attacks.

Several studies have investigated the number of passwords and accounts that users possess. Gaw & Felten [10] found that undergraduates had an average of about 12 accounts, but they had fewer unique passwords and password reuse was rampant. The study also found that most participants cited easier memorability as their reason for password reuse, and that participants classified their accounts by the desired level of privacy and security. Florencio & Herley [9] conducted a large scale study of password use through the six-month deployment of a Microsoft toolbar. They collected data from more than 250,000 users, and found that the average user had 6.5 passwords, each of which was shared across 3.9 websites. They found that the average user accessed 25 accounts over the six month period, and logged into eight accounts per day. A 2011 diary study of password use by Hayashi & Hong [11] collected detailed records of password entries over a two-week period. They found that users accessed a mean of 8.6 accounts over two weeks, and estimated that most participants had about 11 accounts in total. Although they did not study password reuse directly, all of their participants reported reusing passwords across multiple accounts. A more recent diary study [18] conducted in an organizational setting found that users authenticated 23 times a day on average, and were frustrated by the frequent disruptions to their primary tasks.

Password-composition policies also influence how users choose and manage passwords. A study of a change in password policy at Carnegie Mellon University found that the shift to a more complex policy annoyed and frustrated users, causing them to rely on new coping strategies, but also made them believe that they were more secure [17]. Another study showed that password policies do influence how users choose passwords [13]. However, users are likely to retain fragments of existing habits and passwords across changes in policy, leading to long-term reuse [21].

While several studies have investigated *what* users do to cope with passwords, there exists less investigation into *why* users behave the way they do. Wash [22] identified folk models of security threats (viruses and malware) that users use to justify ignoring security advice. A follow-up study [15] investigated how users find information about security, and found that most users depend on informal shared security stories from friends and family.

Figure 1: Participants were provided with cards showing website screenshots, to help them understand and immerse themselves in the task.

Another problem in the deployment of useful security advice is the divide between those who make security policies, those who enforce security policies, and those who follow security policies. Studies of information security in organizations have revealed a "digital divide" between policy makers, who typically do not bear the cost of security vs. users, who handle the downsides of security including lost productivity and opportunities [3]. Beautement, Sasse & Wonham [5] suggest that organizations must factor in and budget for the cost of employee compliance with security policies. They suggest that organizations need to consider costs and benefits to the organization when setting security policy.

3. STUDY

To investigate how users manage and keep track of their passwords, we conducted a series of interviews about password habits. The interviews were facilitated by the researcher, who asked the questions, recorded answers, and encouraged participants to discuss or give fuller answers. The interview was audio-recorded to allow further note-taking and analysis. We also conducted a brief self-administered demographics questionnaire that collected basic information including age, gender and occupation, and was mostly intended to give a better understanding of the interview sample. This study was approved by our ethics board.

We developed our interview questionnaire around the idea of exploring users' password management techniques. We asked a set of general questions about password habits and usage, including questions about how many passwords and accounts participants had, whether they reused passwords, whether they used password managers, and how they kept track of their passwords. The next series of questions asked about how they would behave when creating new accounts, and when changing or resetting the password on an existing account. We did not ask participants what their passwords were, and we specifically told participants that they should never reveal their passwords to us. Each interview took approximately 30 minutes, and the interviews were conducted at our university.

We chose our methodology to encourage participants to discuss thoughtfully the ways in which they approach the task of password management. We used a guided interview to focus the discussion around topics of interest to us, but we asked additional questions to probe responses and follow up on emerging topics of interest. We broke questions into a number of parts to give participants an opportunity to fully explain how and why they make their decisions, and to avoid having participants rush through their answers. We provided users with props in the form of cards with website screenshots (Figure 1) to situate themselves in the password creation and reset tasks, and to encourage them to consider their real life behaviour.

We used Grounded Theory [19] to analyze the interview data and conduct qualitative analysis of participants' responses and discussion. Grounded Theory is an analytical framework that seeks to develop an explanatory theory from a set of data. It builds a theory grounded in evidence, rather than validating an outside theory or testing generalizability. Grounded Theory defines a theory as:

> ". . . a set of well-developed categories (e.g., themes, concepts) that are systematically interrelated through statements of relationship to form a theoretical framework that explains some relevant social, psychological, educational, nursing, or other phenomenon." (p.22 [19])

4. RESULTS OVERVIEW

There were 27 participants interviewed for the study, and all were recruited from the university community via posters, mailing lists, and word-of-mouth. In conducting the interview, we used the constant comparative approach, where we refined the focus of the interview discussion throughout the study. At 27 participants, we reached saturation, where we were hearing little new from additional participants.

Two-thirds of participants were female. Participants' age ranged between 17 and 67, with a median age of 22. Most participants were either full- or part-time students, and came from a range of programs including the humanities, sciences, and social sciences. None of the participants were studying computer science or computer security. The other participants worked in the university community, in roles such as administrative assistants, librarians, and security guards.

In addition to the discussion and deeper responses, the interview questions also yielded a set of quantitative data about how many passwords and accounts users have, how many passwords they reuse, and the extent to which they use password managers and other tools. We present below descriptive statistics of the responses to these questions. We present these data before the Grounded Theory analysis to give context to participants' responses.

The first part of the interview investigated how many accounts and passwords users have. We wanted participants to closely reflect on their answers to these questions, so we divided questions into multiple parts. For example, in a question about number of accounts, we identified 14 account categories where participants might have accounts, and asked about each category individually. We hoped this technique would help users remember infrequently used accounts.

Participants reported their total number of accounts as being between 9 and 51 accounts, with a median of 27 accounts. The bulk of most participants' accounts consisted of email addresses, school or work accounts, and social networking accounts. They reported using a median of 11 accounts in an average week, with a range of 3 to 14 accounts.

Participants reported having between 2 and 20 unique passwords, with a median of 5 passwords. All but one of the participants in the study (26 participants, 96%) reported reusing passwords between accounts. Of the participants who reported reusing passwords, most (23 participants, 88%) reported reusing more than one password, and 19 (73%) reported reusing passwords either "always" or "frequently". Participants described different strategies for reusing passwords. Some described using the same password for all accounts, and others described linking passwords with usernames. Participants also reported using different passwords for different online contexts, such as at work or school. Several participants mentioned that they were careful not to reuse passwords on "financial" or "important" accounts (though many did not clarify what was important). Conversely, many participants also mentioned having a specific password that they reused widely on accounts of low interest, low importance, or infrequent use.

We were interested in whether participants considered context of use in their password management strategies. Participants reported entering their passwords on a range of devices including desktop computers, laptop computers, tablets, e-readers, and smartphones, but the most commonly reported context was a computer (laptop or desktop) and a smartphone. Most participants (18, 66%) said that they did not consider device constraints when choosing passwords. Participants who considered device constraints mentioned that they checked the availability of apps (to reduce the difficulty of password entry), the different security requirements of different devices, and awareness of the usability of different keyboards. All participants reported that they enter their passwords on computers that do not belong to them. Several participants mentioned that they were more careful about logging out on these computers, and about not saving passwords in the browser. One participant mentioned that they sometimes changed their passwords after entering them on computers belonging to other people.

The next set of questions addressed the coping strategies that users develop to keep track of passwords and accounts. We asked participants if they used any kind of password manager (including the browser-based managers), and 22 respondents (81%) said that they saved their passwords in some kind of password manager. All of these went on to clarify that they saved passwords in their browser or in the Apple Keychain. No one reported currently using dedicated password management software, although one participant said that he had previously used one. We also asked if participants ever clicked the "remember me" button to stay logged in to websites using cookies, and 22 participants (81%) reported clicking these boxes. Interestingly, although the same percentage of participants said they used cookies as password managers, these sets did not completely overlap.

Twenty-one participants (78%) reported writing down at least some of their passwords. Of these participants, most referred to the recorded passwords as a backup for memory, and not a resource used at every login. Participants reported different recording strategies – some recorded only part of the password, or a hint to the password, while others were more methodical about recording all of every password. Participants reported using both physical and digital media to store passwords, but specified that the recorded passwords were easily accessible from their regular computing context.

The final part of the interview asked participants about password changes and resets of forgotten passwords. Forty percent of participants reported having ever changed passwords of their own volition, and these participants remarked that they changed passwords rarely, and only under special circumstances. Most participants evidently did not consider situations where they changed forgotten passwords, because all participants reported having done this. Most participants reported resetting forgotten passwords once per month or less, and most people said that their strategy in those cases was to change the password to something similar to existing passwords (often reusing or adapting an existing password).

5. QUALITATIVE ANALYSIS

We chose not to fully transcribe our data. Instead, we made detailed notes about responses to the interview questions. These notes included quantitative question responses, but also included additional details from participants' discussion of the topic. In places where our notes were not sufficiently detailed, we returned to the audio-recorded data for additional information. We referred to the audio-recordings to transcribe exact quotes for use in this paper.

For the qualitative analysis, we followed the grounded theory methodology of Strauss & Corbin [19]. This method involves several steps in the analysis process. First, recorded data is analyzed point-by-point and assigned descriptive codes, in the process of *open coding.* Next, these codes are compiled, and the process of *axial coding* looks for relationships among the codes. In the process of axial coding, the researcher asks questions such as *why*, *where*, *how*, and *when* in an effort to uncover structure in the data. Finally, *selective coding* integrates the results of the open and axial coding, and refines them into a theory.

5.1 Open Coding

We began the process of Grounded Theory by developing a set of descriptive open codes. We generated the open codes by examining the noted responses from the interview data. We traversed the answers to each question, looking for recurring patterns and themes in the data. Each of these themes was denoted by a code. We had a total of 66 codes.

Some of the codes emerged in relation to the question being asked in the interview. For example, we asked participants about whether they wrote their passwords down, and how they stored and referred to recorded passwords. Several codes about password recording emerged from responses to that question. However, other codes emerged over the sequence of the discussion. Participants gradually revealed more about their password creation, organization and categorization techniques as we explored how they would handle password creation, how they would choose passwords for new accounts, and how they would keep track of new accounts.

One of our password recording codes was *records passwords as backup strategy*, and we used this code when a participant indicated that although they wrote at least some of their passwords down, they did not refer to these recorded passwords on a regular basis, and instead appeared to use the recorded passwords as a backup.

In the following quote, the participant describes how she used to write her passwords down as a fallback for memory when going on vacation.

> "Not any more. I used to. [Why did you stop?] Because the only reason to write them down was if I was going on vacation for two weeks and I'd come back to work and I wouldn't remember my password [laughs]. So that was [garbled] but now I very rarely take vacation more than one week at a time and I can remember one week [laughs]." – P15

This participant describes writing her work passwords down so that she would be able to remember them after a long delay. However, she does not need this technique in everyday use. She also explains how a change in her circumstances (shorter vacations), has affected her password coping strategies (coded as *change of habit*).

Another code was *single sign-on* which we used when a participant brought up the subject of single sign-on services, such as through Facebook or Google.

> "Or you could just connect through Facebook. [It's true. Would you/do you do that?] I actually don't do that very often, no. [Why not?] Uhh, I just find there's so much junk on Facebook sometimes that I really just don't want to add to it. On Facebook, I try to only add, umm, things that are more important to me I guess." – P27

This participant shows a misunderstanding of single sign-on when she explains that she avoids signing in through Facebook because she thinks her activities will be posted to her Facebook feed. Interestingly, she does not express concerns about privacy, but rather about the relevance of information that she posts to her personal page.

5.2 Axial Coding

Following open coding, we began the process of axial coding. In axial coding, we took the codes assigned in open coding and looked for patterns, connections, and relationships between those codes. Our eventual goal was to form a model or theory that described our data. To examine the codes, we tagged each code with a post-it note, and arranged them on a table to look for connections (Figure 2).

A list of codes used in open coding is presented in Table 1, along with a brief explanation of each code. The groupings in the table are the result of the first round of axial coding where we collected codes with a similar focus. Following this, we identified an ordering, and then assembled our groupings into larger categories following this order. These categories are described in the subsequent sections.

5.2.1 Choose Your Password

At some point, every user must create their passwords and how they do this is up to them. In our interviews, participants discussed a number of strategies that they employed when choosing passwords. Some participants included personal information in their passwords. Participants mentioned including the birthdays of loved ones, phone numbers, and personal information such as hobbies in their passwords.

> "I'll try to usually think of some kind of hobby of mine, uhh, whether it would be something like hockey or a video game and a video game character, and I'll try to link it to that. Something that I usually think about quite a bit." – P24

Table 1: A selection of the 66 codes used in the open coding process. The codes are organized into related groups based on the initial step of the axial coding process.

Code Name	Description
Contextual Behaviour	
Banking as important account	Banking was a frequently distinguished important account.
Contextual behaviour for different websites	Different password behaviour on different websites.
Contextual behaviour for different environments	Different password behaviour in different places (e.g., work vs. home).
Password Categories	
Categorizes by security	Categorizes password reuse by the level of security.
Categorizes by password rules	Categorizes password reuse by the password rules on the website.
Categorizes by frequency	Categorizes password reuse by the frequency of website use.
Categorizes by semantics	Categorizes accounts by content similarity.
Passwords linked to password rules	Creates passwords to use with different password policies.
Affective passwords	Picks passwords that have emotional significance.
Personal information in passwords	Incorporates personal information into passwords.
Creating Passwords	
Algorithmic passwords	Uses some kind of algorithm to generate passwords.
Variations on a theme	Unique passwords consist of variations on a single password.
Passwords linked to usernames	Associates passwords with unique usernames
Passwords linked to times	Associates passwords to the time period in which they were created (e.g., during undergrad).
Passwords linked to website content	Links passwords to content found on the website, or reason for visiting the website.
Affective passwords	Creates passwords with emotional significance.
Personal information in passwords	Creates passwords with personal information (i.e. phone numbers, birthdays).
Named Passwords	Has a specific nickname for their most frequently used password.
Preferred Characters	When fitting password to password policies, has a set of habitually used numbers and symbols that they add.
Password Recording	
Digital Recording	Records passwords in digital media (e.g., in email, or in an excel file).
Physical Recording	Records passwords in physical media (e.g., on post-it notes, in a journal).
Records as backup strategy	Records passwords, but does not refer to them consistently.
Always records	Systematically records all of their passwords.
Records when special policies	Records passwords when the website policy prohibits resets or disables cookies.
Records clues to password	Records hints or clues about the password.
Tools	
Uses tools only in some contexts	Uses cookies or browser password managers only on some devices.
Combination of coping strategies	Uses a combination of coping strategies to remember passwords (e.g., password manager, writes passwords down, and password resets).
Unable to take advantage of coping strategies	For some reason, cannot use a certain tool or technique to remember their passwords.
Personal Validation Questions	Relies on the personal validation questions to reset forgotten passwords.
Single Sign-On	Sometimes uses single sign-on to log into different websites.
Password Rules	Creates passwords by consulting the available password policy.
Attacks on Self	
Guessing attack on self	At login, attempts to guess own passwords.
Dictionary attack on self	At login, guesses all of own reused passwords.
Password Difficulties	
Password reuse not working well	Reuses passwords, but still has problems managing or remembering.
Password reuse for memorability	Reuses passwords because unable to remember more passwords.
Security Concerns	
Privacy	Explicitly considers privacy when creating accounts.
Difficulty	Expresses the difficulty of managing and remembering passwords.
Behaviour Change	
Change of habit	Has had a major change of behaviour in how they create, manage, or remember passwords.
Hacked	Described an incident where they found the security of an account had been breached.

Figure 2: Re-arranging the codes to look for patterns in the axial coding process.

These strategies were often combined with affective strategies that included personally meaningful information in passwords. One participant told us that she had changed her passwords to a personal goal, so that the password would be easy to recall, but also so that she would be continually reminded of the goal.

> "I read an article this, this, uhh, month, that said 'whatever your goal is, make that your password' [okay] and you can still follow their rules . . . but because you're going to be entering in your password so many times a day, make it your goal, and it can be anything, you know." – P15

Another participant said that she included religious phrases such as "God is good" in her passwords, as a reminder of her beliefs and priorities.

Another strategy described was temporal. One participant told us that she changed email addresses depending on the point in her life (it appeared that she habitually switched all of her email into the address associated with her current educational institution). She had a password associated with each of her email addresses (when used as usernames). At login, she considered the time period in which she created the account, and entered the password linked with that email address and time of life.

A number of participants told us that they linked passwords closely to website content. As an example, one participant told us that if he was creating an account on an online store, he might incorporate the item he was purchasing into his password.

A few participants mentioned an algorithmic strategy for creating passwords. They systematically combined pieces of information to create passwords with a consistent format. Participants described different pieces of information that were included in their passwords. One participant said she included a piece of information associated with the website, as well as a piece of personal information in each password. Participants also had a few standard symbols, numbers, or words that they recombined for variation in their passwords.

External factors are also taken into account when choosing passwords. Several participants told us that they liked having the password policy rules displayed at create time, because they can factor them into their passwords, rather than having to create a password and modify it when it does not satisfy the policy.

5.2.2 *Reuse Your Password*

Password creation always happens with a new account, but users almost always have other accounts as well. Most of our participants reused passwords across accounts. We were interested in how they chose to reuse passwords across accounts, and how they matched passwords with accounts.

The participants in our study who reused passwords all built a personal model of reuse. Often, participants described categorizing their accounts and assigning passwords to categories. Participants described a number of different categorization strategies. Security was a common consideration that many people mentioned.

> "Like I said, it depends on what the website actually is. If it requires a weak password according to me or a strong one, I'll chose it on that basis and probably alter a letter or two." – P25

Participants assessed the security needs of the websites, and they referenced matters such as privacy, and confidentiality without clarifying those terms. Many participants explained that they treat accounts differently if they store credit card information. We were unclear on how well they assessed the security needs for non-financial personal information (such as on social networking websites).

Several participants described reuse strategies that hinged on password policies. One participant told us that he maintained a set of five passwords that fit increasingly complex password rules. If the password rules were easily viewed, he chose the appropriate password. If the password policy was not displayed, he began by trying the simplest password and only trying more complex passwords if the site rejected the simpler password.

Many participants described a semantic or thematic approach to their password reuse. They attempted to reuse passwords on accounts with similar purposes or contents. Examples included using the same password for social media websites, or across online shopping accounts. Participants also described strategies that organized passwords into less obvious semantic categories. These included using the same password on all professional accounts, or on all accounts that had low personal value.

Unexpectedly, many participants discussed frequency of use when describing password reuse. Participants mentioned having trouble remembering passwords for infrequently used accounts, but surprisingly, they often seemed to feel that infrequent use indicated a lack of need for security. Correspondingly, these same participants saw frequently used accounts as needing more protection. One way of bolstering the frequency of infrequently-used passwords was to have a single password for infrequently-used accounts, but it was unclear whether the purpose of this was to group accounts.

It was clear in the interviews that although many people had several reused passwords, there was a primary password that was reused on most accounts. Participants referenced this password in a variety of ways, but the language used indicated the importance of this password. One participant called it her "go-to password" and told us that she relied on it because she trusted the person who had chosen it for her. Several participants referred to a certain password as being "familiar" or "easy". Many participants remarked that they had many passwords that were variations on a single password, and it appeared that these were often variations on this most used password.

> "[How many unique passwords do you have?] Eight? But it's always, like, you know, adding a one at the end when I forget. [So some of them are slight variations?] Yeah, yeah." – P9

A few participants were unable to describe any particular strategy to their reuse, although they definitely did reuse passwords. One participant told us that they "randomly" choose one of their reused passwords, and another participant said that they cycle through their reused passwords in order when creating accounts. None of these participants mentioned any reasoning for their habits.

5.2.3 Commit Your Password

After assigning a password to an account, the user must be able to keep track of this password. In our study, participants described a variety of coping strategies that they used to remember (in the active sense – store) their passwords.

Writing Passwords Down: The majority of participants told us that they wrote at least some of their passwords down. Some participants described strategies where they recorded all of their passwords, and others told us that it was a strategy that they used only in special cases. Most participants said that they wrote their passwords down to prevent forgetting them, but others wrote their passwords down as part of a larger strategy. One participant told us that she records her passwords in a spreadsheet for her husband to access in case of emergency. She later implied that she sometimes consults the spreadsheet for herself, but this is not the primary reason for keeping it.

> "[Do you ever write your passwords down?] Only maybe a couple of banking ones, they're the only ones, my banking, so if I die my husband can find them." – P5

Most participants appeared to view their password recording as a backup strategy rather than a constant resource. Interestingly too, writing passwords down can support not needing to rely on such techniques forever. One participant told us that she wrote passwords down only until she had memorized them. She also used a rehearsal strategy to help her memorize her passwords.

> "If it's new, I'll write it down for the first couple of times, but if it's new, I'll try to remember it, try to memorize it. I'll log in a bunch of times until I've memorized it." – P11

A number of participants described special cases where they would write passwords down. These special cases included assigned passwords, websites without any backup mechanisms (such as online password resets), and websites where the use of cookies is disabled. Other participants told us that they recorded hints or clues to their passwords. A few participants told us that they recorded usernames, either with or without the corresponding password. Another strategy was to write down only part of the password or some other form of password hint.

> "I email them to myself, and I have a folder with all my passwords in it [This is an email folder?], (nods) and instead of putting the actual password in there, I put something to remind me what the password was." – P13

An important consideration in the safety of recording passwords is how they are stored. Participants in our study described a variety of storage strategies for recorded passwords. Some participants wrote down their passwords on physical media, such as post-it notes, or journals. Often, they chose places near their computers to keep these passwords. One participant told us she pins a list of passwords to her bulletin board, while another described writing her passwords on a box kept on her desk. Some participants went to lengths to hide these passwords, by keeping the post-its underneath keyboards or by carrying the list of passwords with them, but others seemed unconcerned. Participants also shared a variety of strategies for storing their passwords digitally. These strategies included dedicated password documents (Excel spreadsheets, or Word documents), passwords emailed to themselves, passwords kept in online notebooks (such as Evernote), and passwords stored in desktop widgets.

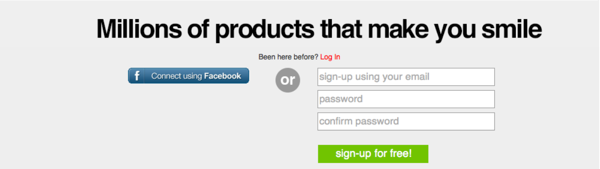
The accessibility of recorded passwords was a key issue. For participants who chose to store their passwords digitally, they often mentioned concerns about having the password list when it was needed. A few participants mentioned using services like Dropbox to keep their password lists in the cloud, and participants who emailed passwords to themselves appeared to have chosen this technique for accessibility. One participant emphasized the need for accessibility when he described using services that synced across devices to store passwords.

> "[Do you ever write your passwords down?] On my phone, sometimes. . . . Usually you would either keep it in, like, Google Keep, or iCloud, or messenger, or Evernote. In my case, Evernote. I use a lot of Evernote, so. . . . Anything that is really sync-able to multiple devices that way it is easier for me to store info." – P16

Password Managers: Almost all of our participants reported using the password managers built into web browsers. A few participants told us that they only used these tools in specific contexts: two participants told us that they saved their passwords in the browser at work, but not at home, and many participants clarified that they only saved passwords on their own computers. A number of participants also clarified that they only saved passwords for certain accounts in the password manager. Most commonly, participants said that they did not save the passwords for banking websites, but a few people specified that they did not save passwords on any websites that required credit card details.

One participant in our study told us that he used to use a dedicated password manager, but had stopped using it. He was vague on the details of the password manager, and could not remember its name, but was able to tell us that he had stopped using it because it was inconvenient to have to copy passwords out of the password manager.

> "I've used, umm, I can't recall the name, but I've used one before in the past. [What made you start or stop using it?] It was just inconvenient



Millions of products that make you smile

Been here before? Log In

Figure 3: A detail of one of the websites used as a prop in our interviews.

> because it encrypted it every time and I'd have to decrypt it. [Oh, okay] It was the same issue, it's like encrypting and decrypting constantly. It's just more convenient to have it. [And was that kind of like the time that it took to. . .] Yeah, but you had to basically sorta copy it, paste it into a search box. It wasn't the time issue, it was just the hassle if I wanted to do it with multiple passwords." – P25

This participant refers to the time and hassle of encryption and decryption, but we speculate that he is referring to the process of hashing a master password.

Many websites offer the user the opportunity to remain logged into a page via a cookie saved in the browser. This choice is often presented at login, via a checkbox that says "Remember me", "Stay signed in", or something similar. Although this mechanism is not one that saves passwords, it accomplishes the same result by removing the need for the user to enter a password. In our interviews, we asked about cookies directly after asking about browser-based password managers, and it was clear that a number of participants did not understand the difference between the mechanisms.

> "[You know how sometimes you'll go to log in, and there will be a box for your username, a box for your password, and then there'll be a little box to tick that says "Remember me"? Do you ever tick that box?] Yeah. Because that's the same as saying 'save your password', right?"
> – P16

Some participants appeared to treat the mechanisms identically (typically, relying on both), but others told us that they used one or the other without giving much justification for their habits.

Other Tools: Over the course of the interviews, participants mentioned a few other tools and techniques that they used to keep track of passwords. These tools included a Smartwallet app, and single sign-on. Although a single sign-on option ("Connect via Facebook" – see Figure 3) was prominently displayed on the password creation prop card, only two participants commented on it. One participant told us she would use the option when it was available because she had a hard time remembering even her reused passwords. However, another participant (quoted in Section 5.1) said she would not use it, because she did not want any extra information cluttering her Facebook page. It is difficult to know why other participants did not mention any kind of single sign-on, since the cue was equally visible to all participants. Our interview script did not prompt them to specifically look at the Facebook button, but they were told to imagine they were on that page. Possibly, this indicates that most users do not understand how single sign-on services can be used as an alternative to reusing passwords.

In summary, it was clear that most participants used a variety of tools and strategies to help them cope with their passwords. Participants saved passwords in browser-based password managers to handle the case when they were using their own computers, but needed backup mechanisms for times when using other computers.

5.2.4 *Forget Your Password*

After a user has memorized their password, there is always the chance they may forget it. Users have many passwords, and it is clear that handling forgotten passwords is a large part of the password management task.

Several participants described situations where they could not remember their passwords at login, and told us their first action would be to try and guess their password. Some participants described a kind of targeted dictionary attack on themselves, where they would guess all of their reused passwords.

> "Sometimes, I do forget, but I try everything else [all of the passwords]" – P17

Other participants described guessing strategies where they attempted to recreate their motivation for being on the site (for example, the item they were buying when they created a shopping account), or the password they would have been likely to pick in the time period they created the account. Still others said they would try to recreate algorithms for password creation, or look at the password policy to make a better guess at their own password.

The other fallback strategy that participants described was the password reset mechanism. In this, we include both personal verification questions and email resets. Almost all participants told us that they have reset forgotten passwords, and it appears that many users do this on a regular basis. Some users seem fine with this as a strategy, but others raised objections. One participant told us that she had begun writing her passwords down when she realized she was resetting her passwords too often. Another participant remarked that she had not considered how often she reset her passwords until the interview, but that it was a major part of her password coping strategy:

> "It's funny, I never really thought about it, but I guess I do that a fair amount." – P19

5.2.5 *Live with Your Passwords*

Passwords and accounts can last a long time: once passwords have been created and linked to accounts, all users must begin the long process of living with and coping with their passwords.

A number of participants in our study commented on the difficulty of managing and remembering passwords. Participants displayed different attitudes toward this difficulty. One participant referred to passwords as agonizing.

> "Then what do I do? Ohhh, my gawd. Then I agonize for a few minutes." –P13

Another participant seemed resigned to reusing passwords.

> "[Do you ever reuse passwords?] Oh yeah! (laughs)"
> – P9

Participants also referred to fears of doing the wrong thing, and uncertainty about the outcomes of password decisions. Some participants explicitly referred to privacy, but only a few referred to private information that was not financial.

As time progresses, a user may change their behaviour in some way. In our study, a number of participants described changes in behaviour that had occurred for a variety of reasons. Some users described stopping or starting using tools. One participant told us that she no longer saved passwords in the browser because she had heard that this behaviour could be dangerous.

> "I used to and then I took one of these studies and they helped me with understanding why that was not a good idea. [Did you at that point go and erase the ones that were already in there?] Yes." – P13

Another participant told us that he used to use a password manager, but had stopped using it because of the time it took to copy and paste passwords when using the password manager. He describes the hassle of using the password manager in a quote in Section 5.2.3.

One reason to change an existing password is in the case of a security breach. A number of participants in our study described situations where they had changed account passwords after suspecting that an account was not secure. Examples of breached accounts included email and PayPal accounts. As participants described their security breaches, it emerged that they were often unsure about whether they had been attacked, and sometimes had to made decisions without really knowing what had happened.

> "At least, I think that I've been hacked. [What kind of clues, what would be a kind of signal to you? Has it ever happened to you?] It has, because my friends told me they got these really strange emails, from my email, supposedly sent from me, that were obviously ads for something or other and they were like 'hey, this doesn't sound like you'." – P19

A few participants brought up changing their passwords in the case of more minor suspected security breaches. One participant told us that they changed their passwords when they thought a friend might have seen their list of passwords, and another participant said they had changed their Facebook password when they thought they might have left the account logged in on a friend's computer.

5.3 Selective Coding

The last coding step in Grounded Theory is selective coding, where the researchers attempt to identify a unifying *core code* that describes the underlying phenomenon in the observed and interpreted behaviour.

As we analyzed the data, a central theme about rationing and budgeting began to emerge. In all phases, our participants described ways in which they stretched thin resources: memorization, attention, creativity, and security knowledge. Similar to the way in which we ration and conserve time, energy, food, and money, participants were handling password management by devoting appropriate resources to accounts of great importance, and then devoting less energy to other accounts, and generalizing their approach to similar accounts to save effort. In their work on organizational security, Beautement et al. [5] suggest that organizations need to budget for the costs (both time and money) of organizational compliance. Our suggestion about rationing differs in that we identify that individual users are budgeting their own time and effort. We are not suggesting this arises because of a lack of willingness to comply, but rather from a paucity of cognitive resources.

In the following sections, we systematically examine how rationing plays a role in each of the themes of axial coding.

5.3.1 Choose Your Password

When choosing their passwords, participants rationed their efforts in a variety of ways. For participants with formulaic or algorithmic strategies, part of their investment was in memorizing their personalized strategy. By remembering that their strategy is to include a word related to the website, they reduced the amount of effort that it takes to choose a password on a new website. Participants who closely associated their passwords with a username were engaging in a similar strategy. Remembering usernames can be difficult, but if you have a consistent strategy to associate a password with a username, effort can be more effectively rationed to each account.

The interviews asked participants what they would do when creating an account if their password was rejected on the grounds of insufficient complexity (for example, lacking a symbol). Most participants reported that their strategy in this situation was to append a symbol to the password. Most participants referenced "their" symbol, and told us that they had a habitual symbol that they used in this situation. This coping strategy implies a way of rationing effort across situations that cannot be predicted. If participants knew their password would need a symbol, they would have begun with a symbol. But since they are unable to see the password policy, they have developed sensible coping strategies that conserve memory and effort in these situations.

Many participants told us that they reused pieces of passwords in a variety of ways. Many participants referenced appending different endings onto the same widely reused passwords. Participants also discussed using this strategy as part of their password changes; one participant told us that after he realized a friend might have got access to his list of recorded passwords, he had changed his passwords, but had simply added characters to the existing passwords.

> "Like I said, I have them all stored on a text file, right. And once, a friend of mine or an acquaintance borrowed that USB drive, and I felt that he would have access to everything so I went and changed everything. [Okay] But all I did was add like a letter or two." – P25

5.3.2 Reuse Your Password

One main way in which users ration their efforts is in not choosing a new password for every account. Reusing passwords allows users to conserve energy across their large number of accounts.

As participants discussed how they would create a password for a new account on an online shopping website, many digressed into a discussion about accounts that do not matter to them. One participant told us that she had a password that she used on accounts where she would not care if she was hacked. Another participant referenced having a password that she would not mind sharing with others. Whether or not these participants actually would not care if others had access to their account, their behaviour shows that they are rationing the effort they put into these accounts by the amount of effort they merit.

An important aspect of rationing is that those who deserve more should get more, and we found evidence that users were applying this principle in their password management strategies. Many participants referenced special habits for their online banking: participants told us that they did not reuse their banking passwords, that they would not log into their bank on a shared computer, and that they would not enable cookies or save their banking login in the password manager. All of these behaviours indicate that users are willing to ration more effort into accounts that they perceive as needing it.

Participants referenced using different behaviour in different contexts. Two participants referenced a different set of habits for their work passwords, and both implied that they were less careful about security for these passwords. It was difficult to know if this was because the information was seen as less personal, or because they felt that the physical environment was more secure, or if it was simply because they used those accounts more frequently, but they were assessing information about the context of use and rationing effort differently to it.

5.3.3 Commit Your Password

Memorizing passwords is one of the most difficult parts of the password management task for users. Passwords must be maintained over long periods of time, with sporadic and unforeseeable usage patterns. Using tools such as password managers and techniques to write passwords down is how users allot effort into the unknown needs of the future.

Availability and accessibility are key issues for password managers. Managers are typically only available on personal computers. Dedicated password manager software sometimes have associated smartphone apps that allow users to take their passwords away, but the browser-based managers are largely only tied to one computer. This means that users must ration the effort they put into making sure their passwords are available to them when they need them.

Participants in our study described using a combination of techniques to keep track of their passwords. Some participants were heavily invested in one strategy, but most participants appeared to know a few of their passwords, to have some of them written down, and to have some of them stored in a password manager. This strategy seems to ration effort across time and place – when at home, the password manager saves the passwords for almost all of their accounts, or they might have easy access to the recorded passwords. When elsewhere, they cope by remembering their passwords, or by carrying some of the passwords with them. It appeared that some participants were sacrificing convenience for security in these situations, which indicated another aspect of rationing in their coping strategies.

5.3.4 Forget Your Password

All of the participants in our study told us that they have reset passwords when they are forgotten. Participants clearly regarded this as being separate from a change of password, which seems to indicate that forgotten passwords are seen as part of the landscape of password management. Users expect to have to handle a loss of memory, or a failure of a coping strategy. It appears that the password reset mechanism allows users some flexibility in their rationing strategy. In particular, many participants appeared to rely on email resets. In situations where a password reset was not available, participants described rationing extra effort to the situation, often to ensure that the password was recorded.

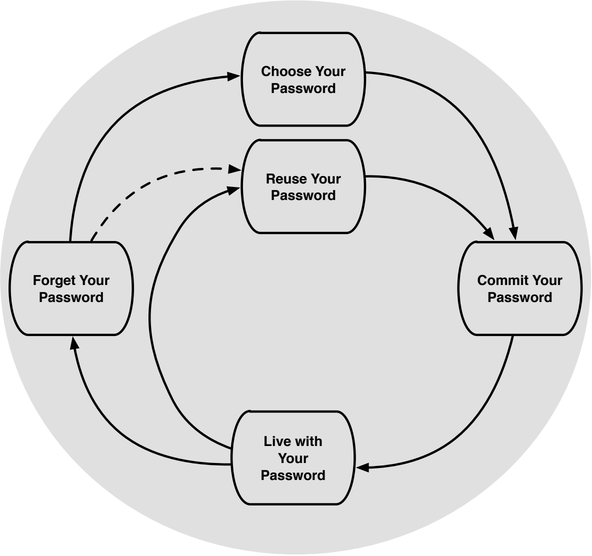


Figure 4: The password life cycle.

In the situation where they were resetting a password, many participants told us that they would reuse an existing password, or change the password to what they thought it had been or what it should have been. It appeared that their coping strategies were equipped to handle these situations without any particular sense of frustration or loss.

5.3.5 Live with Your Password

Throughout the interviews, we heard a number of remarks on the difficulty of password management. Although participants are resigned to the realities of passwords, they still present difficulties. Finding and implementing coping strategies for the difficulties of passwords involved effort and unpleasantness. Similarly, rationing itself is a difficult task! The decisions about how to allot time, energy, and effort are not always obvious to users. Users referenced lacking information that would have made it easier to cope: unseen password policies, misunderstood security requirements, and invisible security breaches.

5.4 The Password Life Cycle

In the final step of Grounded Theory, we look back at the identified codes, patterns, and relationships in order to form them into a theory.

Our theory is that there is a password life cycle – a progression of stages through which every password passes. Passwords are created, assigned to an account, then recorded or memorized, lived with, and then potentially forgotten. Old passwords are then reused or adapted in the creation of new passwords, and the cycle continues.

Figure 4 illustrates the stages of the password cycle. The cycle begins when the user needs to create a password for a new account. Theoretically, a user might begin with no passwords at all, and have to fabricate one from scratch, but they may also have existing strategies and password phrases that they will integrate into a new password. This password must next be committed, either memorized or recorded, so that it can be later used for login. Assuming the commitment process is successful, the user then lives with their password. They login and access their accounts successfully. If they successfully remember their password, and it is appropriate for reuse, they can then reuse that password. If the password must be changed (because it is forgotten, because someone else has learned it, or because of enforced password change policies), they must return to password creation.

Rationing is present at every step of the password life cycle. Users ration effort at creating new passwords, they reuse passwords to put more protection on the most valued accounts, they reduce the effort of memorization by saving passwords in managers or by writing them down, and they strategically budget the attention they pay to passwords on existing accounts. Users save resources from inconsequential accounts so that they can devote them to to more important accounts. Allotting time, attention, and energy to different accounts forms the backbone of users' coping strategies. As with other forms of rationing, users scrimp on effort for some accounts to save it for others.

Rationing contributes to the cycle of password reuse. As effort is reduced from some accounts, it is saved for new ones. Reused passwords are handed down from existing accounts, saving the user the time and energy of creating and memorizing a new password.

6. DISCUSSION

Our theory suggests a number of ways in which the design of security products could better support users.

6.1 Writing Passwords Down

While writing passwords down is an intuitive and reasonable way of handling security, users need helpful guidance on the right way to store these passwords. Writing passwords down is conventionally understood to be insecure, but many security experts actually advocate writing passwords down [6, 16] if they can be kept in a physically secure location. Many users do write their passwords down, but the caveat about storage is poorly understood by users. In our study, participants reported keeping their password lists in their email, in Dropbox, on their cell phones, or saved on their computer desktops. Recording passwords is a sensible way of conserving effort, and users should be encouraged to make the small changes that could make this habit safer.

To address the storage problem and guide users to safer password storage, a plausible solution might be the development of a service specifically to securely store passwords. Password storage notebooks do exist (*e.g.* The Personal Internet Address & Password Log Book [1]), but there is no equivalent online service. In the absence of a trustworthy electronic service, it seems possible to better emphasize the notion of physical security of stored passwords to users, and suggest secure and sensible places to keep lists of passwords.

6.2 Password Cues

Another finding of our study is that participants often had trouble matching passwords to usernames or to websites. If users were able to better match their passwords to websites, they would not have to resort to strategies where they reveal multiple passwords to potential attackers by trying all of them at login. We suggest that image cues could help users better associate passwords with accounts. Websites could be designed to associate these cues with usernames and present them at password creation and at every login. Since the cues would have no relation to the password, it would not be necessary for them to be secret. This could be similar to the image-based anti-phishing mechanisms found on some financial websites (for example, Bank of America's SiteKey [4]). The explicit nature of these cues would help users associate passwords with websites. Although some users currently try to create a cued match from password to website by including website-related information in their passwords, these strategies can place an additional burden on the user because they must then remember the cueing strategy in addition to the cued password. Reducing this burden would allow users to transfer effort into other aspects of the password task.

6.3 Password Managers

We were surprised to find that none of our participants used a dedicated password manager, and surprised even that not everyone was using the browser-based password managers. As long as they are well-designed, and do not store passwords in the clear, password managers seem to offer one of the best solutions for password management: comprehensive, convenient, and safe. However, most of our participants appeared unaware of prominent password managers, and some participants expressed distrust in this software. We suggest that the better integration of password managers into operating systems and browsers would help with both visibility and trust. A few participants in our study did mention having passwords saved in Apple's iCloud Keychain, although it wasn't clear that any of the users were taking advantage of the password creation mechanism, or the cross-device capabilities.

We speculate that password manager software could be improved to integrate password cues and to facilitate reuse. We know that not all websites will want to integrate these kinds of features into their existing mechanisms, and the advantage of a password manager is that it is controlled by the user, and does not require changes to existing websites. A well-integrated password manager would let users ration effort into a mechanism that genuinely kept them safer.

6.4 Single Sign-On

Although the use of single sign-on would address many of users' password problems, the participants in our study appeared either unaware of or ill-informed about single sign-on. Although a single sign-on "button" was equally visible to all participants in our interviews (on the website screenshot), only two commented on it at all. One said she used it sometimes because she had trouble remembering even her reused passwords, but another participant explained that she would not use it because she did not want information cluttering up her Facebook page.

Her explanation showed a strong misconception about how single sign-on works. Instead of understanding that Facebook's role in single sign-on is to verify your identity, she thought that she was signing into Facebook and using the online store as a part of Facebook. This indicates a need for independent single sign-on providers, who do not have a stake in personal information. The biggest current providers of single sign-on are Google and Facebook, both of whom have other reasons to be interested in browsing and usage patterns. Although users do not completely understand how single sign-on works, they do not want their activities to be visible to uninvolved parties. A better option for single sign-on providers would be independent entities who only verified authentication attempts, similar to the certificate authorities who currently issue SSL certificates.

Addressing the issues with existing single sign-on services would allow users to take advantage of these services, and allow them to better ration and conserve their password efforts. Single sign-on gives the user the advantages of reusing passwords without the risk, and allows them to harness existing strategies while remaining more secure.

6.5 Extra Information

When discussing information that participants look for when creating passwords, a few participants mentioned password strength meters and a number of participants brought up the subject of password policies. Participants wanted to know password rules before picking a password so that they didn't have to waste effort creating the "wrong" password, and wanted the additional guidance of a password strength meter. Providing strength meters and making password rules available before they are broken are minimal efforts that could simplify users' password experiences.

Throughout the discussion, but particularly when they were discussing security breaches, participants referenced a lack of information about their passwords and accounts. When discussing suspected hacks, they expressed uncertainty about whether they had been hacked, and an absence of information to turn to. This lack of feedback is an inherent characteristic of security [23], but we still think that more information could be made available to users. Most websites log information about sign-ins and actions, and this information could be made available to the user. Obviously, this information could not assist in attacks where the attacker gains complete control of the account, but in many cases, participants still had access to their accounts (and were able to change their passwords) and could have used a resource to help them find additional information about account usage.

Having to search for clues about malicious usage is yet another security task that consumes users' time and resources. Making this information readily available would allow users to sensibly ration and conserve their efforts when handling compromised accounts or passwords.

6.6 Threat models

One of the emergent themes during the interviews was confusion about threat models and the nature of the threat. Although worried about security, participants seemed unclear about the type of threats that concerned them. They did not differentiate between targeted personal attacks, anonymous large-scale password hacks, and the loss of private data, although they referenced all three during the discussions. Correspondingly, participants did not seem to appreciate that the defences for different attacks might vary based on the nature of the account in question. This lack of understanding has an impact on how users ration their password efforts. If they are confused about the type of threat, they may misdirect their efforts, leaving valued accounts unprotected and over-protecting less vulnerable accounts.

Understanding of threat models informs how users categorize their accounts for reuse. In order to reuse passwords safely, users must be able to better assess their security needs on websites. If users are going to reuse passwords, either by themselves or with support from a password manager, it is important that they understand the consequences. For example, it is probably unwise for users to reuse passwords from high-importance accounts on low-importance accounts.

Assessing the threat models is important, but users are also trading off their time. Herley [12] points out that if users were to follow all given advice, the security benefits would be swamped by the time spent following the advice. He proposes instead an economic model where both threats and benefits are assessed. In order to consider both threats and benefits, users need to be able to reason about the severity and likelihood of threats, and to consider carefully benefits such as uninterrupted routines and time that can be devoted to primary tasks.

7. CONCLUSION

In this paper, we presented our study on how users cope with the difficulties of living with passwords. We conducted interviews, and performed analysis using the Grounded Theory methodology. We found that users have complex coping strategies that combine a variety of tactics. They ration effort to devote resources to accounts they feel of greater importance and minimize their effort for accounts of lesser importance. Over time, this leads to a life cycle of password usage whereby passwords are developed, reused, and adapted.

We suggest that our findings indicate new opportunities for better supporting users, and we describe some possibilities. For example, password managers might be designed to facilitate safe reuse. A proactive alternative to strength meters could help users pick appropriate passwords for each account. Accounts could help users by providing cues and password rules to help users link passwords with accounts.

The work described here is theory-building, rather than theory-validating. A large scale survey could investigate the generalizability of these findings, and see how they are supported in the larger population. Future work in this area might include the development of a survey instrument to investigate how passwords pass through the life cycle. Additionally, the information collected in this survey is self-reported. A study investigating the match between users' reported security behaviours and their real life habits could shed light on users' ideas of what they are supposed to do, as well as provide more concrete detail for design.

Our contribution in this paper is the identification of important patterns underlying user coping strategies. Users are not stubbornly refusing to follow password advice, they are instead carefully managing their resources to cope with impossible demands. Their solutions are often flawed, but they deserve consideration and may indicate better strategies for security. In choosing where to build roads, it may be best to pave the paths that users already walk.

8. ACKNOWLEDGMENTS

We would like to thank the anonymous reviewers and our shepherd for their help in improving the paper. We would also like to thank the Government of Canada for support from NSERC ISSNet and the GRAND NCE, as well as support from an NSERC Canada Graduate Scholarship, and an NSERC Discovery Grant.

9. REFERENCES

[1] The Personal Internet Address & Password Log Book (Organizer): Peter Pauper Press. `http://www.amazon.ca/Personal-Internet-Address-Password-Organizer/dp/1441303251`.

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

[3] E. Albrechtsen and J. Hovden. The information security digital divide between information security managers and users. *Computers & Security*, 28(6):476–490, Sept. 2009.

[4] Bank of America. SiteKey at Bank of America. `www.bankofamerica.com/privacy/sitekey`.

[5] A. Beautement, M. A. Sasse, and M. Wonham. The compliance budget: Managing security behaviour in organisations. In *Proceedings of the 2008 Workshop on New Security Paradigms*, NSPW '08, pages 47–58. ACM, 2008.

[6] W. Cheswick. Rethinking Passwords. *Queue*, 10(12), Dec. 2012.

[7] S. Chiasson, P. Van Oorschot, and R. Biddle. A Usability Study and Critique of Two Password Managers. *15th USENIX Security Symposium*, pages 1–16, 2006.

[8] A. Das, J. Bonneau, M. Caesar, N. Borisov, and X. F. Wang. The Tangled Web of Password Reuse. In *NDSS 2014*, 2014.

[9] D. Florencio and C. Herley. A Large-Scale Study of Web Password Habits. In *International World Wide Web Conference Committee (IW3C2)*, May 2007.

[10] S. Gaw and E. W. Felten. Password Management Strategies for Online Accounts. In *SOUPS '06: Proceedings of the Second Symposium on Usable Privacy and Security*. ACM, July 2006.

[11] E. Hayashi and J. Hong. A diary study of password usage in daily life. In *CHI '11: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM Request Permissions, May 2011.

[12] C. Herley. So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In *NSPW '09: Proceedings of the 2009 Workshop on New Security Paradigms*. ACM, Sept. 2009.

[13] S. Komanduri, R. Shay, P. G. Kelley, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor, and S. Egelman. Of Passwords and People: Measuring the Effect of Password-Composition Policies. In *Proceedings of the 29th Conference on Human Factors in Computing Systems (CHI)*, New York, USA, 2011.

[14] LastPass. The Last Password Your Have to Remember, 2014. `www.lastpass.com`.

[15] E. Rader, R. Wash, and B. Brooks. Stories as Informal Lessons about Security. In *SOUPS '12: Proceedings of the Eighth Symposium on Usable Privacy and Security*. ACM, July 2012.

[16] B. Schneier. Choosing a Secure Password, Feb. 2014. `http://boingboing.net/2014/02/25/choosing-a-secure-password.html`.

[17] 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 *SOUPS '10: Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM, June 2010.

[18] M. Steves, D. Chisnell, A. Sasse, K. Krol, M. Theofanos, and H. Wald. Report: Authentication Diary Study. Technical report, National Institute of Standards and Technology, Information Technology Laboratory, Gaithersburg, MD, Feb. 2014.

[19] A. Strauss and J. Corbin. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. SAGE Publications, Thousand Oaks, California, 2nd edition, 1998.

[20] S.-T. Sun, E. Pospisil, I. Muslukhov, N. Dindar, K. Hawkey, and K. Beznosov. What Makes Users Refuse Web Single Sign-On?: An Empirical Investigation of OpenID. In *SOUPS '11: Proceedings of the 7th Symposium on Usable Privacy and Security*, USA, 2011. ACM.

[21] E. von Zezschwitz, A. Luca, and H. Hussmann. Survival of the shortest: A retrospective analysis of influencing factors on password composition. In *Human-Computer Interactionâ INTERACT 2013*, volume 8119 of *Lecture Notes in Computer Science*, pages 460–467. Springer Berlin Heidelberg, 2013.

[22] R. Wash. Folk Models of Home Computer Security. In *SOUPS '10: Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM, July 2010.

[23] A. Whitten and J. D. Tygar. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *USENIX Security Symposium*, pages 169–183. Carnegie Mellon University, Aug. 1999.