“It’s Hidden in My Computer”: Exploring Account Management Tools and Behaviors

Eiji Hayashi and Jason Hong

July 8, 2013

CMU-CyLab-13-007

CyLab
Carnegie Mellon University
Pittsburgh, PA 15213

"It's Hidden in My Computer": Exploring Account Management Tools and Behaviors

Eiji Hayashi Jason Hong
Carnegie Mellon University
5000 Forbes Ave,
Pittsburgh PA, 15213
{ehayashi, jasonh}@cs.cmu.edu

ABSTRACT
A great deal of past work has investigated passwords in terms of the number of passwords users have, the way people generate passwords, the security of these passwords, and better ways to create passwords that were secure and memorable. However, little work has examined how people manage these passwords in the wild. In this paper, we report results of interviews we conducted with 22 people probing how people manage their passwords and other account information using password management tools, which range from a piece of paper containing one's passwords to applications specifically designed to manage account information. Through analyses of data, we found that majority of participants were using password management tools as backups and still tried to memorize passwords, and that having sense of control was of great importance for them in using password management tools. Furthermore, we identified features that could be implemented in password management applications to better satisfy users' needs.

Categories and Subject Descriptors
H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

General Terms
Security, Human Factors

Keywords
User Authentication, Passwords

1. INTRODUCTION
Passwords are the most commonly used form of user authentication. However, passwords represent a growing burden for end-users, in terms of having to memorize secure passwords, having to manage multiple accounts, and having to comply with different password policies for these accounts.

To mitigate the burden of passwords, people rely on several basic strategies. The most straightforward strategy to improve memorability is to choose simple passwords [6][21]; however these simple passwords have been shown to be highly vulnerable to dictionary attacks [15]. For example, analysis of 32M passwords exposed in a security breach at RockYou.com showed that the top 20 most common passwords could compromise over 5% of the accounts [5]. Another strategy to improve memorability is to create passwords using something related to individual users (e.g., family members' names and/or their birthday). However, these passwords based on individual information are vulnerable to educated guess attacks.

Another way of mitigating burden is to reuse the same passwords across multiple accounts. Gaw and Felten [10] and Hayashi and Hong [12] both reported that users often reused passwords. The problem, however, is that if one account using a shared password is cracked, other accounts can also be compromised. Furthermore, an attacker could target a service with the lowest security to obtain passwords to access services with higher security.

A third way to ease the burden of passwords is to use tools to manage passwords. These tools might range from writing down passwords on a piece of paper to specialized applications that can manage account information. There has been little past work investigating how people manage their passwords using these kinds of tools in the wild. Understanding current practices of password management tools, their affordances, and their weaknesses could help us develop better password management tools that are more useful, usable, and desirable.

In this paper, we report on the results of a study investigating how people manage their passwords using variety of password management tools. We conducted semi-structured interviews with of 22 participants who were already using one or more password management tools. In our interviews, we looked at three issues. The first issue was what kinds of password management tools they use, as well as the range of behaviors around these tools. The second issue was which accounts they shared with others (or others shared with them), and why. Very little past research has examined this aspect of sharing [13][20][22], and our conjecture was that password sharing was more common and had a richer range of behaviors than has been previously reported. The third issue was what kinds of features participants liked and disliked for a password management application. We had some surprising findings in terms of features, where some features that already exist were not highly desired (e.g. generating strong passwords), whereas other features that do not exist were highly ranked (e.g. notifications of when an account was used).

This paper made the following contributions. First, this paper provides rich qualitative data about the range of behaviors in how people use password management tools to manage their accounts. Second, this paper reports on users' account sharing behaviors in wider contexts, documenting a richer breadth of behaviors as to what accounts are shared, how they are shared, and why. Third, this paper provides design implications for developing password management applications that satisfy users' needs.

2. RELATED WORK

There have been numerous studies examining how people use passwords. Here, we have organized the related work into three categories: studies of password composition, or how people create passwords and the strength of those passwords; studies of password usage in practice, looking at a range of behaviors surrounding passwords and security; and software tools that people have created to manage accounts.

To some extent, our paper is related to investigations of security in the wild [7], which probed the steps that people took in practice to improve their perceived level of security (regardless of whether these steps actually improved security). Our paper is descriptive, in terms of offering qualitative findings of how people use password management tools in practice.

2.1 Password Composition

Much past work has examined password composition, which includes the strength of passwords in the wild as well as how people create passwords. Klein analyzed 13,797 passwords. He found that, using a dictionary consisting of 62,727 words, he could crack 25% of these accounts, indicating that many people chose simple passwords [15].

Yan et al. investigated the memorability and security of passwords composed using different approaches through a lab study with 288 students. The results showed that mnemonic passwords could improve security of passwords without undermining memorability [24]. Mnemonic passwords are typically created by concatenating one letter from each word of a phrase. For example, the phrase "I love to ski at Seven Springs!" could turn into a password "IL2s@7S!". However, Kuo et al. showed that users were likely to choose certain phrases in creating mnemonic passwords, making them potentially vulnerable to dictionary attacks [17]. Furthermore, even using mnemonic passwords, some users forgot which password is for which account, due to scaling issues and interference effects.

One possible way to make users choose secure passwords is to enforce strict password composition policies. For instance, a service can require users to choose passwords that contain numbers, symbols, uppercase letters and lowercase letters. Inglesant and Sasse found that even if organizations enforced strict password policies on users, the policies did not guarantee security for certain attacks (e.g., key loggers) while also frustrating users [13]. Shay et al. conducted a survey consisting of 470 students to investigate how enforcing a strict password composition policy affected users' perceptions of security. The results showed that the students were annoyed when university adopted a new password policy requiring more complex passwords, but at the same time, the students felt more secure [19]. Komanduri et al. investigated how various password composition policies affected the strength of passwords created under the policies. They found that simply requiring longer passwords made participants choose passwords with highest entropy [16]. These studies imply that choosing appropriate password policies is crucial to making password authentication systems more secure and usable.

Our paper also touches on password composition along with password management tools. We report on some strategies that people used to create passwords, as well as some strategies for how people record passwords in their tools so as to increase perceived security.

2.2 Password Usage in Practice

Many studies have investigated how people use passwords. Adam and Sasse conducted a study focusing on people's attitudes towards password authentication systems. They found that if the authentication system did not mesh well with people's work practices, people tended to circumvent the authentication system, in effect undermining security [6].

There have been other studies investigating password usage outside of organizations. Gaw and Felten interviewed 49 undergraduate students and found that the students had 7.8 accounts on average, with three or less passwords [10]. Florencio and Herley deployed a web browser extension that monitored authentication for online services. They deployed it to roughly a half million clients over three months, and estimated about 25 online accounts per client [9]. Hayashi and Hong conducted a diary study to investigate how many account people had and where they log into these accounts. They reported that participants had about 11.4 accounts on average and 84.3% of logins to these accounts happened either at home or workplace [12].

Our paper focuses less on password usage, and more about how people use password management tools in practice. For example, our work differs from the work above in looking at what tools are used, and what steps people take to protect those tools from unauthorized access (e.g. hiding a piece of paper with account information on it).

There have also been some past work looking at password sharing behaviors. Inglesant and Sasse found that people share passwords to exchange files and to share web spaces in companies [13]. Singh et al. conducted a qualitative study about how people shared banking passwords with spouses or significant others [20]. The closest related work is by Kaye, who conducted a survey consisting of 122 participants investigating how people share passwords. He reported that people shared their passwords with family members, friends and colleagues, across a number of different kinds of services and devices [14].

Our work on sharing of passwords has much in common with the work above. The main differences are that our analysis focused more on how passwords and accounts were shared, patterns in that sharing, and pain points in sharing, with the ultimate goal of using this information to build a better password management tool.

2.3 Password Management Applications

There are also numerous password management applications available. For example, all modern web browsers have a built-in feature for password management, for saving account information and automatically filling in this information later on. There are also several password management applications, which are standalone applications designed to manage login information [2][3][4]. Sometimes, these applications store additional information such as screenshots of web pages to better manage users' accounts [1].

Our work differs from this past work in terms of investigating how people actually use these password management applications (in addition to other kinds of tools, such as text files and pieces of paper). Our work also investigates the perceived value of different kinds of features for password management applications. We found that some existing features were not seen as very valuable, and that there were other features that do not yet exist but were seen as very desirable.

Type	#	Examples
Text Files	13	Excel, standard text files, sticky note application, notepad on phones
Browsers	20	Chrome, Internet Explore, Safari, Firefox
Physical Paper	7	Memo, note, a sheet of paper
Applications	5	LastPass, KeePass, aWallet, Keyring, Keychain Access
E-mails	2	Gmail, Hotmail

Table 1. Password management tools that our participants were using. Because most of them were using multiple tools, the sum of frequencies is more than the number of participants (N=22).

3. METHODOLOGY

To investigate how people use password managers in wild, we conduct semi-structured interviews. Existing work reported that a limited number of users adopted password managers [12]. Thus, to obtain rich data, we specifically recruited participants who manage at least five accounts using some kind of password management tool. We defined password management tools as systems that manage users' account information without depending solely on participants' memorization. Examples include using a sheet of paper, memos, sticky notes, browser auto-fill features, text files, and applications such as LastPass [4], KeePass [2] and KeyChain Access [3].

Participants were asked to bring their password management tools to the interview. We opted for this procedure so as to help prompt participants' memory, to help them describe their behaviors more accurately. We also asked participants to refer back to lists of accounts in their password management tools and to go through their accounts one by one in answering our questions when necessary; however, we did not examine their password manager directly to avoid violating their privacy and security.

In our interviews, we focused on collecting qualitative data about password management behaviors and tools, to understand the range of behaviors as well as interesting ways that people used these password management tools. The interviews were comprised of three parts. First, we probed what password management tools participants were using. Second, we investigated what accounts people shared, with whom, and in what context. Third, we asked participants to evaluate features that could be supported by password management applications based on how they had been managing their accounts in practice.

To be consistent as much as possible, we showed questions on a display in the structured part of the interview. Then, an interviewer asked follow-up questions. Each interview took about one hour. All the interviews were audio recorded and transcribed. Based on our participants' responses, we created an affinity diagram to extract underling themes in the password management domain.

3.1 Participants

We recruited participants via a participant recruitment website at Carnegie Mellon University as well as sending emails to local mailing lists. We recruited 22 participants, with age ranging from 18 to 62 years old with median age of 27. Three were undergraduate students, five were graduate students, 12 were full-time employed, one was self-employed, and one was unemployed. For the employed, they had a variety of professions, such as a photographer's assistant, a social worker, an office administrator, and a programmer. Six of them had technical majors. They also reported that, on average, they used computers 2 to 14 hours a day on weekdays with a median of 7.5 hours, and 1 to 14 hours a day on weekends with a median of 4.5.

Tools	Browsers	Paper	Apps	E-mails
Text File	12	2	3	1
Browser		7	3	2
Paper			0	0
Applications				1

Table 2. Numbers of participants using each combination of password management tools. There were four participants using more than two tools.

4. FINDINGS

4.1 Password Management Tools

In the first part of our interviews, we asked about tools that participants were using to manage their login information including passwords. More specifically, we asked about:

- Tools that they used to manage their login information
- Accounts that were managed using the tools (as well as those that were not)
- Pros and cons of using their password management tools
- How they generated and updated passwords
- Their experiences in using their password management tools

Along with these issues, we asked many open-ended questions about their thoughts on these issues to deeply understand their behaviors and rationales behind the behaviors. Most of our participants' passwords were for online services, and so a majority of responses were related to online accounts; however, we did include passwords for other types of accounts, such as login accounts for computers, in our study.

Through the interviews, we found that participants were using combinations of five types of password managers for different types of accounts (Table 1). We discuss each of these five types in more detail below. Table 2 shows the number of participants using each combination. For instance, the top-left cell shows that 12 participants used both text files and browsers to manage their passwords. There were four participants who used more than two tools, so the numbers do not add up to 22. Table 2 shows that using physical paper or text files with a web browser is a typical combination. From our interviews, we saw that participants often wrote down login information for important accounts on a piece of paper while using the browser to save login information for less important accounts.

Our participants described a variety of rationales behind their choice of password managers. In this section, we first describe our findings related to each type of password management tool. Then, we describe themes that appear across multiple types of password management tools.

4.1.1 Text Files

The most popular password management tool among our participants was text files stored on computers and phones. Here, we use the term "text" quite broadly to include not just standard text files, but also Microsoft Excel files, sticky note applications, and notepad apps on smartphones. Four participants protected their text files using a password. Most of the participants stored both user IDs and passwords in those files.

***Simplicity*:** Almost all participants using text files as their password managers mentioned that simplicity was the biggest advantage. P21, who used a standard text file as her password manager, commented, "It's simple and easy to use. And I can edit it very conveniently." P5, who used an Excel file, said:

> "I think a text file is very simple. I don't need to install it [because it's already installed]. I can just copy the file from a computer to another one. It's simple and secure because the file has a password. I made the password [required to access the file] very difficult."

***Additional Protection*:** Similar to P5, many participants had additional security layers to protect their text-based files. Five participants used Excel files to manage their account information, and four of these had passwords on that file. Some participants only stored partial information about their accounts. For example, P5 reported that she often wrote down just half of her passwords:

> "For some passwords, I don't write down whole passwords. For instance, for a password, I'm using birthday [as a part of my passwords], and I only write down the month."

Similarly, some participants wrote down only user IDs or passwords to improve security, in case their text file was compromised. For example, P12 said:

> "I usually use a standard password. [So, I don't have to write it down.] But, user ID changes and the file has user IDs. […] I have four email addresses and use them for different websites."

P2 reported that she hid her text file in several ways: "I'm using a different extension for my text file. Also, I make it a hidden file." Instead of using a .txt file extension, she used .app, which stands for an application file on MacOS. She also added a hidden flag on the file so that the file was not visible in the graphical file system.

4.1.2 Browsers

Modern web browsers offer features for storing user names and passwords, and auto-filling this information on the appropriate web sites. This functionality was widely used among our participants: except for two participants (one using LastPass and one using a physical note to manage all login information), all of our participants stored some of their account information in their web browser. Eighteen mentioned that these accounts were not important ones; however, there were seven participants who stored login information for their e-mail services.

Convenience: The majority of participants using browsers mentioned that convenience was the main reason why they save their login information there. As a result, login information for frequently accessed accounts is likely to be stored in web browsers. P12, who primarily used an Excel file to manage her passwords, said:

> "For these accounts that I access very frequently, I don't want to refer back to my file. Because, when I'm working, every minute counts."

Another participant mentioned that he stored passwords even when he remembered them, "I remember most of my passwords. But, I store the passwords in a browser to save my time."

Importance of Accounts: Many participants choose whether to save passwords in their browsers based on the perceived importance of a given account. P2 said, "I store passwords for the accounts that do not have my credit card information." Similarly, P11 said:

> "These are less important accounts that I don't know whether I'll access them again. I don't want to use my standard passwords [that I use for many of my accounts] because, if someone gets my passwords [from the website], potentially, he can access many of my accounts. But, I don't want to memorize the passwords or don't want to take time to write the passwords in my file. So, I create kind of random passwords and save it [in a browser]."

Interestingly, seven participants reported that they store login information for their email accounts (Gmail and Hotmail) in their browser. They commented that these accounts were important for them; however, they decided to store the login information because they accessed these accounts very frequently. One of the seven participants (P3) also reported that he stored login information for his online banking accounts in his browser. P3 explained that he did have login password on his laptop, and that he always carried his laptop with him. Thus, although he was worried his laptop being stolen, the perceived convenience of storing login information in the browser outweighed its risk.

4.1.3 Physical Paper

Seven of our 22 participants used physical paper to store some of their passwords. Four participants used notepads to write down login information including service names, user IDs and passwords. They used the same notepads also to write down other information that they want to keep, such as dates and times of appointments, to-do lists, and something they found interesting. The other three participants used sheets of paper to manage their login information. In these cases, the participants wrote down login information on the sheet of paper. Only one participant (P3) used a small piece of paper, such as sticky notes, to write down passwords. P3 said, "I write down a password for [CMU's participant recruitment website] and tape it on my display. Because it's not an important account, I don't care. And I check the website pretty regularly."

Securing memos: All the participants using physical paper mentioned that they were concerned that an undesired person might gain access to their memos. Five of the seven participants reported that they always carried the memo with them. P7 noted, "I'm carrying my note with me. It's always in my backpack and it's always with me. So, I think it's safe." Furthermore, P22 explained that having the physical note gave him sense of security. He said:

> "I think it's the best way to have easy access to it. It's more personal. You can hide it. I think the feeling of touching it gives you sense of security much more than using something else."

The other two participants stored their memos in secure places. P12 noted, "I keep this [sheet of paper] on my desk, but I always lock my office when I leave." P20 said, "I hide this sheet of paper in a drawer. It has a lock and my office has a lock too."

Memos as a backup: The participants using physical memos also reported that they were not using random passwords even though they did not have to memorize the passwords. Rather than keeping login information on physical paper, they memorized passwords and wrote down passwords primarily as a backup. P22 commented, "I still need a sort of psychological security that, OK, I don't forget it." P9 also said, "I memorized most passwords, but, sometimes, I have to double check." In these cases, the participants actually memorized their login information and used

memo as a tool to retrieve their login information just in case they forgot it.

Some participants used physical paper as a backup for their digital files. P7 said, "I'm using a text file [on my computer] to manage my passwords. But, I also write them down on a piece of paper as a backup."

4.1.4 Password Management Applications

Five participants reported that they used password management applications. The applications were LastPass (for PC), KeePass (for PC), aWallet (for Android phone), Keyring (for Linux), and Keychain Access (for MacOS). Among these participants, one participant (P6) used LastPass as his only tool for managing passwords. Other participants supplemented these applications with physical paper or text-based files to manage a small fraction of their accounts. Three participants described that there were no clear distinctions between the accounts managed by applications and ones managed by text-based files. One participant (P15) said, "The passwords in my Excel file are old ones. When I moved from the Excel file to KeePass, I didn't copy all of them because I don't access some of them." Another participant (P8) reported:

> "I'm managing my personal accounts using a text file. But, for the work related accounts, I want more security. So, I save the passwords in Keychain rather than the text file. Keychain requires a password to access. So, it's more secure."

One interesting finding was only one participant used randomly generated passwords, despite the fact that all of the applications (except Keyring) support this feature. P14 explained:

> "I don't like automatically generated passwords because all systems fail. If passwords are automatically generated, they are not my standard passwords. I would forget or cannot figure out the passwords [when they are lost]. If they are my standard passwords, I can try some variations of them [to figure out the passwords]."

This comment implies that participants do not want to completely rely on applications in managing their password, and want some sort of backup in cases where the application failed.

4.1.5 Email

Two participants used email accounts to manage their passwords. One of them (P14) used Hotmail, and had one message that contained her user IDs and passwords for multiple services. She explained that when she created a new account, she simply replied to the message and added the new user ID and its password. She also had additional protection on her message. She said:

> "I actually have whole bunch of junk emails in the folder. This is the one that has my passwords. Its title seems like a spam. I'm trying to protect my passwords."

She also mentioned, "I'm using email [to manage my login information] because it's easy to access. I can access it anywhere."

Another participant (P16) used Gmail to manage his accounts. He described that whenever he created a new account, he sent an email to himself and then assigned a specific tag to the email with his login information, to make it easier to find these emails. He also had additional protection. He said,

> "I use service names as titles [of my emails containing login information], but I slightly modify them. Finding them is a little bit difficult."

He also mentioned that there were cases where he himself could not find the emails. He explained:

> "There were a couple of cases where I couldn't find emails [with login information]. I didn't use the accounts for a while and forgot the keywords to find them."

Interestingly, this challenge in re-finding one's passwords is not limited to email. In another case, one participant mentioned that he once hid a piece of paper with his passwords and later forgot where he hid it. In short, if users have information in multiple places, there is a risk of them forgetting where they stored the information.

4.2 Creating and Changing Passwords

In the first part of our interviews, we also asked how our participants created and changed passwords. We expected that our participants would use rather secure passwords because they did not have to memorize password when using password management tools. However, the majority of participants reported that they created their passwords by simply combining words and numbers.

4.2.1 Creating Passwords

Seventeen participants reported that they usually created their passwords using their own schemes, such as combining some information related to them (e.g., family members' names, pets' names, birthdays, street addresses, and phone numbers). P5 described:

> "I use birthdays. I have a mother, a son, many birthdays that I can use. In China, we have a lunar calendar. So, we can use [birthdays in] lunar calendar too [to create passwords]. I combine names and birthdays to create my passwords."

Three participants reported that they were reusing a small number of passwords for several accounts. P13 said, "I have one base password. I use it for many things." P19 commented:

> "I have three passwords. The easiest one is just numbers. The second one is characters plus numbers. The third one is the most complex one. It has long numbers and characters with symbols. I use the most complex one for my banks and other services related to finance. For the easiest one, I mostly use it for unimportant accounts. […] I also use the simplest one for Facebook and Gmail. I want to use an easy password because I type it frequently."

While memorability is well-known as an issue in passwords before, ease of typing is not as well-explored. Ease of typing also becomes more important if users do not want to store the passwords in browsers and have to access the account frequently.

Three participants reported that they created random passwords and let password management tools to save them. One participant was using the Chrome web browser and a physical note as his password management tools. Two participants were using password management applications (KeePass, and LastPass). P6 mentioned:

> "I like LastPass because it generates own passwords every time. So, getting one password isn't going [to let] someone get into all of my accounts."

We also asked whether he was comfortable with completely relying on LastPass. He answered, "I have a backup of the data. And nothing bad happens so far. So, I'm OK with it."

Interference: When websites have specific policies about password composition, those who manually created passwords added minimum modifications on their own password schemes to satisfy the requirements. However, these slight modifications made it difficult for them to remember the passwords, in part due to interference effects with other similar passwords. P21 said, "Because I have so many accounts and so many related passwords. I couldn't remember all of them." P14 also reported:

> "Some passwords require me to include at least one capital. That is one reason why I have to use password managers because my standard password does not include capitals. I typically forget which letter was capitalized. Now, I have to use password managers."

4.2.2 Changing Passwords

Changing passwords periodically is recommended as a good practice in managing passwords, and it is even enforced in some critical services, such as online banking. Seventeen participants noted that they had at least one account that required periodically updated passwords. However, letting users update passwords without enforcement is challenging. Among the 22 participants, 12 participants reported that they updated their password only when enforced. Three participants said that they never changed passwords. P11 said:

"I only change my passwords when required. Creating passwords that are secure and easy to remember is difficult."

In contrast, seven participants changed passwords for important accounts regularly. P14 using an Excel file to manager her login information reported:

> "Sometimes, I go through these accounts. And, if I find some passwords are too old, I change them. I write when I created these passwords."

4.3 Sharing Accounts

In the second part of our interviews, we asked how our participants shared their accounts to deal with tasks in both personal and work contexts. Past work has looked at how people use passwords, but very little work has examined how people share passwords [13][22].

Kaye conducted a survey consisting of 122 participants investigating how people share passwords. He reported that people shared their passwords with family members, friends and colleagues [14]. Similarly, in the authors' personal experiences, we have shared passwords with family members, administrative assistants, and co-workers at a startup company, due to a variety of reasons, and using a number of different approaches. As such, we wanted to explore the range of these sharing behaviors with our participants. Furthermore, we go one step further, compared to the existing works, to obtain deeper understandings sharing behaviors by revealing difficulties, concerns, and strategies that our participants had taking advantage of face-to-face interview. In this section, we describe our finds around sharing behaviors.

4.3.1 Sharing Passwords

All participants except one reported that they shared passwords in the past. They shared their passwords with a small number of people, such as family members, friends and co-workers. Analyses of our participants' responses revealed that there were three different types of sharing behaviors: temporary access, repeated access and shared accounts.

Temporary access: There were cases where people wanted to give someone else temporary access to their accounts. In our interviews, we found that the most common case was a person asking a friend to access their accounts to check some information (e.g., email or Facebook). Eight participants reported that they either shared their passwords and asked somebody to access their accounts, or someone else asked them to do the same. Four of them said that they shared passwords at least once a month. P9 explained:

> "When I didn't have access to my email, I need information in my email. So, I called my friend and asked him to do it."

P9 did not use smartphones; thus, he did not have access to his email when he was away from his computer.

A slightly different form of temporary sharing is to let someone else use an account after the account owner has logged in. Twelve participants reported that they had logged in and let another use their accounts or vice versa. For personal uses, this typically happened in the context of e-commerce. P20 reported, "It was my husband's Eddie Bauer account. I didn't want to set up a different account, and just used his account."

Repeated access: Eight participants reported that they shared passwords for repeated access. For most of the cases, they asked other people (or they were asked by other people) to help deal with tasks using their (or others') accounts.

In the context of personal use, P1 said that he shared his password for his school account with his parents to let them pay tuition. P18 reported that her daughter was sharing a password for the daughter's bank account with her. She commented, "I asked her to share the password. I want to check if there are any problems."

Interestingly, we found that sharing passwords for repeated access occurred more frequently in work contexts. P4 said:

> "I know some of my wife's accounts. She is teaching courses [at a university], and I'm helping her. To deal with things, I need to access her accounts."

Similarly, P14 helps take care of grant applications at a university. She reported:

> "I know a lot of passwords for the system. Just as a practical matter of being able to do the work, they have to assign me a special account. But they don't have time to do it. So, the way they manage it is to let me have all the user IDs and passwords to go into their accounts."

Shared accounts: We also found that people sometimes created shared accounts rather than sharing accesses to existing accounts. Sixteen participants reported that they have at least one account shared among multiple people. For instance, our participants shared bank accounts, Netflix accounts, accounts for paying utility bills, and Google accounts.

P12 described:

> "We have some shared accounts in Dropbox. When we work as a team, someone has to keep files consistent. In these cases, we shared a Dropbox account. Sharing one account is easier to manage for us [than configuring shared folder in Dropbox]. I have this type of account for all the projects I'm working on. After we finish projects, we just leave the accounts."

There are some accounts shared by a large number of people. P5 reported:

"In my child's kindergarten, parents share one gmail account. 20 to 30 people are sharing it. And we use the account to upload and download some files. […] We are using year and a class name as a password [for the account]."

We also found that our participants used very simple passwords for shared accounts. Because they knew that these accounts were shared before putting any data in them, these accounts were less likely to have sensitive information. Consequently, people used very simple passwords to make sharing passwords easier.

4.3.2 Difficulties and Concerns

When participants described their experiences of sharing passwords, we asked them whether they had any difficulties and concerns when they shared passwords.

Eight participants described that sharing passwords was uncomfortable for them. P9 noted, "I don't really want to know their passwords. It's too personal." P10 also commented, "Sharing password really makes me uncomfortable." P16 said:

"I don't like sharing passwords usually. […] Even if it's with somebody I trust, I don't want to share [passwords]. I'm using the same password for a long time. So, revealing one password potentially allows the person to access other accounts too."

Some participants touched on difficulties in sharing passwords. P4 mentioned, "When telling [their] passwords, people forget details of passwords, such as upper case vs. lower case." Similarly, P22 commented, "When I told my password to my girl friend [to let her access my account], she complained that my password was too complicated!" P14 commented:

"I'm sharing many passwords [to access others' accounts]. But, they have to change the passwords periodically. So, whenever they change passwords, we have to share the password again. But, sometimes, they forget to tell me new passwords."

We also found that our participants adopted strategies to make sharing secure. Seven out of the eight participants described that they told their passwords to others (or vise versa) verbally over the phone. P11 commented:

"I usually avoid sending my passwords via email or SMS because, if it's written, they can check it afterwards."

In most cases participants said that they trusted the persons whom they shared passwords with; however participants sometimes changed their passwords after sharing it. P8 said:

"I changed my password after sharing it [with my friend] because I felt uncomfortable. Just to make sure that he can't access to my account later."

P7 observed that he had difficulty in changing a password:

"I told my password for Instagram to my girlfriend. I wanted to show some photos. But, she went through all photos including very private ones. […] Then, I decided to change the passwords. I usually create my passwords using something related to me. And I thought that, wait, she knows this, she knows that. I worried that she may be able to guess my passwords."

Interestingly, P7 also reported that, despite experiencing this incident, he was still sharing some of his passwords with his friends.

Overall, the fact that our participants still share passwords despite these difficulties and concerns indicates that sharing passwords is necessary in many cases to deal with tasks efficiently in practice.

4.4 Features of Password Managers

In the last part of our interviews, we investigated how users perceived existing features of password management applications, as well as potential new features. Towards this end, we asked participants to evaluate 15 features that password management applications could support (Table 3). These features were generated based on an analysis of features in these applications as well as brainstorming by our team.

We described these features one by one and asked participants to rate them using a 5-point Likert scale (1 being least important and 5 being most important). After participants rated all features, we asked participants to choose their five most important features, to compensate for any potential biases in ratings (such as giving 5 to all features). Furthermore, we asked participants to provide qualitative feedback about these features. Table 3 shows the descriptions of features, the median ratings, and the frequencies of being chosen as one of the top five features.

One very interesting result, one that matches our findings of how people used password manager applications, was that users did not prefer *automatically generated passwords*. Participants mentioned that they understood that randomly generated passwords were more secure than manually generated passwords, and that they did not have to remember the passwords if they were using password management applications. However, they still mentioned that they wanted to have control over their passwords. P11, who saved some of his password in a browser, said:

"I know that I don't have to memorize passwords [when using a password management application]. So, using randomly generated passwords shouldn't be a problem. But, I still feel a little bit uncomfortable [using randomly generated passwords]. I guess I'm worrying that there might be some cases where I can't use the password manager, but, still, I have to access my accounts. If I create passwords, I may be able to recover the passwords even if I don't remember them exactly."

P4 directly mentioned control: "I want to have control on my accounts. So, I don't like automatically generated passwords."

The most straightforward way to address these concerns is to let password managers have easy and reliable ways to recover users' account information when they fail, such as making a remote backup periodically (which was also a feature preferred by participants) or providing a mobile phone version that users can use to retrieve information from the remote backups.

Another interesting finding in this data is that our participants highly valued the *notification* feature, something that is not supported by existing password managers. P3 commented:

"I'm constantly checking my bank accounts to see if there is something strange. […] I do want to have that feature for my bank account and for other accounts too."

When we asked about password management tools, almost all participants mentioned that they were concerned about cases where someone who obtains access to the applications would access to all accounts. A notification feature would let users detect suspicious activities and potentially mitigate damages (e.g., remote wipe login information to prevent further accesses).

Another feature preferred by participants and not supported by existing password management applications was a *dedicated browser*. In this feature, we assumed that a password management application has its own web view integrated with the application,

and that the web view does not use extension or plug-ins that can be installed in browser applications. P11 commented:

> "I'm not sure what plug-ins and what extensions are running in my browser. In many cases, I just install plug-ins when webpages ask me to install one. Then, it becomes too complex to manage them. If there is a browser that I can use without worrying about them, that would be useful."

Finally, participants showed interests in the *temporary sharing* feature. As described in Section 4.3, our participants have to share their passwords in many different cases although they are concerning sharing their passwords. Thus, it would be natural for participants to prefer this feature. P6 commented:

> "I like this feature because it obfuscates my passwords even if I need to share my accounts. I don't have to change my password after sharing accounts."

Also, P14 described:

> "This feature helps us a lot. We often need to use somebody's account to do the work. Because I never used such feature, I'm not quite sure, but it seems useful."

Although there would be technical challenges in implementing this feature, letting people share accounts in a safer way would be more beneficial rather than prohibiting sharing accounts.

5. DISCUSSION

In the analyses of our data, we found several common themes in their behaviors surrounding their password management tools. In this section, we discuss these themes and their implications for password management application design.

5.1 Control and the Necessity of Password Managers

Our participants indicated that they wanted to have control over many aspects of their accounts. One example we have already seen is wanting notifications of when an account was used. Another example participants reported was that they tried to memorize their passwords even if they stored the passwords in password management applications. Perhaps the most surprising behavior we saw was that participants preferred creating passwords using their own schemes rather than using password generators provided by password management applications.

At the same time, people also observed that they needed password management tools. P20 noted, "It's not benefit. It's necessity." P21 echoed a similar sentiment:

> "The number of passwords that I have to manage increases every month. […] I can't handle them without [password management] tools. It's simply impossible to memorize all passwords."

P7, who used a text file, Chrome, and a notepad, observed:

> "I used to have the same password for all accounts, pretty much everything. But, I got hacked, and they got into different websites. So, I started changing my passwords for every different website. […] [If you use password management tools] you don't have to have exact same password for everything. You don't have to remember passwords."

Furthermore, three participants reported that they always went back to password management tools to check login information except for a few accounts that they used very frequently (e.g., email accounts or Facebook). P15, who used KeePass, said:

> "The only password that I don't use a password manager is the password to log into the password manager. There are some accounts that I access frequently and memorize passwords for. I generated passwords by myself for these accounts. But, occasionally, I forget the passwords. Then, I go back to password managers to retrieve the passwords."

As such, it may be useful to examine more ways of offering people a greater sense of control over their accounts, to facilitate the adoption of password managers. One possibility is to develop systems that let users access login information even when they do not have direct access to the applications, such as storing login information on their smartphones, or implementing a one-time master password that lets users ask somebody that they trust to check login information of a specified account without revealing those of other accounts.

5.2 Password Managers as Backups

One theme that appeared across multiple types of password management tools was using password management tools as *backups*. This is typically true for physical paper. This usage could be because referring back to pieces of paper takes time and people try to memorize login information to save time. Nine participants using text-based files to manage their login information also commented that they were using the files as back up and did not refer back to their password management tools in most cases.

Even a participant (P4) who stored all of his account information including his online bank information in a browser explained:

> "I'm probably accurate [in remembering passwords] at 90% of the time. But, in the 10% I'm inaccurate. So, if there is a thing that makes sure that I'm not falling in the crack, it would be beneficial."

Similar to using password management tools as backups, five participants commented that the biggest benefit of using password management tools was that they knew one place where they could find all login information. P10 said:

> "I started using the sticky note [application] to manage my passwords, mainly because I started getting too many passwords that I couldn't memorize. And I wanted to make sure that I had one place I can reference back to."

Because participants regard password management tools as backups or a last resort, providing reliable backup and recovery becomes important. Existing password management applications do have backup features; however, it is also important to provide straightforward way of recovering all login information from backups.

5.3 Detection

Existing password management applications are focusing on *prevention*. Most of them provide random password generator that would prevent attacks directly targeting passwords, such as dictionary attacks or educated guess attacks. Some applications allow users to store URLs of websites to prevent phishing attacks. However, none of the password management applications focus on *detection*.

Category	Feature	Description	Rating (median)	Chosen as Top 5 Features
Password	Password Generation	Users can automatically generate a random sequence of letters, numbers, and symbols by clicking a button.	2	6
	Password Update	Users can configure some of their accounts' passwords to be periodically (e.g., every 60 days) updated automatically.	3	3
Login	Auto-fill	A password manager automatically fills password fields when users open pre-configured web pages	4	3
	Auto-login	When users click an account in a password manager, it opens its login page in a web browser and logs into the account on behalf of the users.	4	4
	Dedicated Browser	Users can login to their accounts using a web view implemented in the password manager without any browser extension or plug-ins to complete important tasks (e.g., online banking)	4	11
Security Lock	Master Password Lock	Users can lock password managers using a master password.	5	15
	Location Lock	Users can lock/unlock password managers based on devices' locations.	3	2
	Phone Lock	Users can lock/unlock password managers based on whether they have their phone nearby.	3	3
Management	Account Categorization	Users can organize their accounts into multiple categories (e.g., personal/work, or low/medium/high importance).	4	6
	Synchronization	Users can configure their account information to be synchronized among multiple devices.	4	7
	Data Backup	Users can configure password managers to take backups of their account information periodically to network storages (e.g., Dropbox).	5	11
	Information Management	Users can store additional information (e.g., insurance information, drivers' license information, address and/or credit card information) in password managers.	4	8
Detection	Notifications	Users receive notification on their phone when someone accesses their accounts using password managers. Users can configure which accounts send notifications.	5	17
Sharing	Temporal Sharing	Users can give another person who is using the same password manager one-time access permission to their accounts without revealing passwords.	4	7
	Repeated Sharing	Users can give another person who is using the same password manager access permission to their accounts without revealing passwords until they decide not to share the accounts anymore.	3	2

Table 3. Features that password management applications could support and users' evaluation of the features.

When discussing password management tools, almost all participants commented that they were concerning someone may access their login information stored in their password management tools. P5 said, "My only concern in using a password manager is, someone may have access to it." We believe that adding notification features will mitigate these concerns. P21 commented:

> "I like Gmail. It tells me when someone access to my account from a different IP address. It helps me find what's going on. It makes me feel comfortable."

As such, a detection feature could give users a stronger sense of having control, and makes them feel comfortable with using password management applications. Furthermore, providing notification features, which cannot be supported by physical paper or text files, could increase the benefit of using password management applications to attract more users and let them manage their login information in safer ways.

6. LIMITATIONS

Although we believe that this paper provides new kinds of insights about the range of behaviors in using password management tools, there are some limitations. The first limitation is that we focused on participants who were already using password management tools. As such, we have rich qualitative data about the way our participants used password management tools and difficulties in using them. However, it would be also important to investigate people who are not using password management tools to understand why they are not using them.

A related limitation is that we do not know how many people currently use various password management tools, and how well our population matches this distribution. As we have emphasized, our goal in this paper was not to quantitatively assess password management tools, but rather to qualitatively understand the range of behaviors surrounding password management tools.

Another limitation is that we relied on self-reports. In our interviews, we asked participants to bring their password management tools and to refer them when answering questions directly related to the tools. However, some of our questions, such as questions related to sharing, were based on self-report. Thus, participants' responses could be inaccurate.

Finally, our evaluation of password management features was limited by not having a working prototype. Although we explained the features in a consistent way, participants' interpretations of these features could vary. Although we still believe that the results of our interview provided useful insights for development of password management applications, further investigation with working prototypes would be necessary to fully understanding users' responses to these features.

7. CONCLUSION

In this paper we investigated how people manage their passwords with various tools through semi-structured interviews consisting

of 22 participants. Because of relatively small number of participants, we do not claim that our finding can be generalized for general population. However, we still believe that our analyses of the interviews provided many insightful qualitative findings about the participants' behaviors and perceptions of password management tools.

We found that our participants showed strong preference to having control over their account information in many aspects when using password management tools. Regardless of the tools that they were using to manage their login information, most participants reported that the tools were essentially backup measures. They also described that the biggest advantage of having password management tools is that they had one place to refer back when they lost passwords. Furthermore, even though they did understand that they did not have to memorize passwords when using these tools and that randomly generated passwords were more secure than manually generated passwords, they still wanted to use passwords composed based on their own schemes (e.g., combining words and numbers related to them) rather than using randomly generated passwords to have control over their passwords.

We also found that our participants shared passwords as well as account in many different occasions. These sharing behaviors can be divided into three categories: temporal accesses, repeated accesses, and shared accounts. Participants also commented that they had difficulties and concerns in sharing accounts. For instance, they could not access shared accounts because another individual sharing the account changed passwords without letting them know the new passwords.

When we asked about possible features that password management applications could support, our participants showed strong interest in a notification feature, which is not supported by existing password management applications. With the notification feature, password management applications send notification to users' phones when someone accesses accounts stored in the applications. This indicates that having notification features strengthen users' sense of control and make more users adopt password management applications instead of physical paper or standard text-based applications, such as Excel.

These results suggested that, although password management tools some of users' need, there are aspects that existing password management tools do not address. We believe that our exploration provided rich qualitative data that help us to understand users' behaviors around password management tools and to develop password management applications that streamline users' password management practices.

8. REFERENCES

[1] 1Password. https://agilebits.com/onepassword. Mar 8th, 2013.

[2] KeePass. http://keepass.info/. Mar 8th, 2013.

[3] KeyChain Access. http://www.apple.com/osx/apps/all.html#keychain. Mar 8th, 2013.

[4] LastPass. https://lastpass.com/. Mar 8th, 2013.

[5] Your Top 20 most frequently used passwords. http://www.tomshardware.com/news/imperva-rockyou-most-common-passwords,9486.html. Mar 8th, 2013.

[6] A. Adams, M. A. Sasse. Users are not the enemy. Comm. of the ACM (1999)

[7] P. Dourish, E. Grinter, J. D. Flor, M. Joseph. Security in the wild: user strategies for managing security as an everyday, practical problem. Personal and Ubiquitous Computing (2004) vol. 8 (6)

[8] D. Florencio, C. Herley, B. Coskun. Do strong web passwords accomplish anything? In Proc. USENIX Hot Topics in Security (2007)

[9] D. Florencio, C. Herley. A large-scale study of web password habits. In Proc. of WWW (2007)

[10] S. Gaw, E. W. Felten. Password management strategies for online accounts. In Proc. of SOUPS (2006)

[11] E. F. Gehringer. Choosing passwords: security and human factors. In Proc. of ISTAS (2002)

[12] E. Hayashi and J. Hong. A diary study of password usage in daily life. In Proc. of CHI (2011).

[13] P. Inglesant and M. A. Sasse. The true cost of unusable password policies: password use in the wild. CHI (2010)

[14] J. J. Kaye. Self-reported password sharing strategies. In Proc. of CHI (2011).

[15] D. V. Klein. "foiling the cracker": A survey of, and improvements to, password security. In Proc. of USENIX Security, (1990).

[16] Saranga Komanduri, Richard Shay, Patrick Gage Kelley, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Serge Egelman. 2011. Of passwords and people: measuring the effect of password-composition policies. In Proc. of CHI (2011).

[17] C. Kuo, S. Romanosky, L. Cranor. Human selection of mnemonic phrase-based passwords. SOUPS (2006)

[18] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. Mitchell. Stronger password authentication using browser extensions. In Proc. of the USENIX Security (2005).

[19] R. Shay, S. Komanduri, P. G. Kelley, P.G. Leon, M. L. Mazurek, L. Bauer, N. Christin, L. F. Cranor Encountering stronger password requirements: user attitudes and behaviors. In Porc. of SOUPS (2010)

[20] S. Singh, A. Cabraal, C. Demosthenous G. Astbrink M. Furlong. Password sharing: implications for security design based on social practice. In Proc. of CHI (2007)

[21] M. Sasse, S. Brostoff, and D. Weirich. Transforming the 'weakest link'— a human/computer interaction approach to usable and effective security. BT technology journal, (2001).

[22] Supriya Singh, Anuja Cabraal, Catherine Demosthenous, Gunela Astbrink, and Michele Furlong. 2007. Password sharing: implications for security design based on social practice. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '07).

[23] K.R. Walsh, B. Ives, H. Schneider. The Domino Effect of Password Reuse. Comm. of the ACM (2004)

[24] J. Yan, A. Blackwell, R. Anderson, A. Grant. Password memorability and security: Empirical results. IEEE Security & Privacy (2004) vol. 2 (5) pp. 25-31