Towards a Mental Model of Password Management Software

Martin Prinz
LMU Munich
Munich, Germany
prinzm@cip.ifi.lmu.de

Tobias Seitz
LMU Munich
Munich, Germany
tobias.seitz@ifi.lmu.de

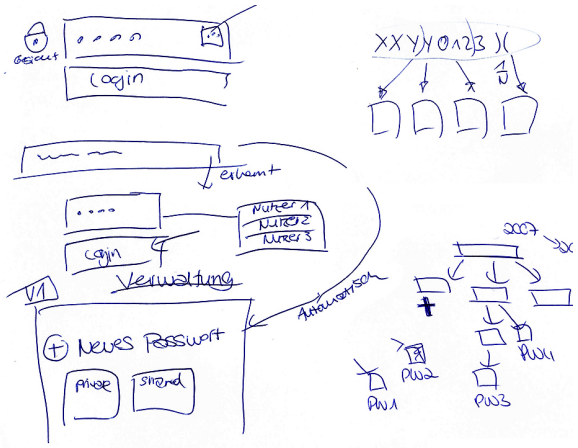

Figure 1: Collage of results of the sketching task about password managers, creation and coping strategies. The most common elements were lists, forms, and categories.

Abstract
Password managers offer a number of benefits but they are still not widely adopted. In this paper, we try to explain the low adoption rates with a mismatch of user expectations and current password management software. Understanding such mental models might help improving password managers and boost adoption rates. To get a better understanding, we conducted semi-structured interviews (N=14) with drawing tasks about password managers and password coping strategies in general. Our qualitative analyses through affinity diagrams reveal that users' individual coping strategies are a key need that may not be fully addressed by current solutions. Our findings show that adaptation and personalization are a way forward to increase adoption.

Author Keywords
password managers; qualitative analysis, usable security

ACM Classification Keywords
K.6.5 [Authentication]: Security and Protection

Introduction
Many companies strive for high security standards to protect confidential data and accounts, and this topic also affects individuals in daily life: Passwords and user names are still the most common concept to authenticate users. However, users often struggle to meet security require-

Figure 2: Final stage of the affinity diagramming process, which helps to create a mental model of password managers. The most prevalent topics that contribute to sense-making of password managers were Creation, Organization, Commitment, Log-In, and Individual Perceptions.

ments and tend to behave insecurely in favor of better usability [8]. For example, to alleviate the challenge of maintaining dozens of user accounts [4, 5], users re-use their credentials [3, 13] and/or choose easily memorable but predictable passwords [1], so data breaches become even more severe. While companies can enforce security policies, private users develop their own strategy for password management and account administration. Not only the creation of sufficiently strong passwords meeting composition policies, but also recalling the right ones is a challenge. Software for managing this information is intended to help users with this problem. However, password managers (**PWM**) are still underused ($\approx$ 12% of users) and most users ($\approx$ 86%) report to memorize passwords[1].

Our work contributes a qualitative user study which shows how individual preferences play a role for users' coping strategies and which should be considered for the enhancement of password managers. We further establish a first mental model of such tools to provide pointers how to analyze and potentially improve current solutions.

Related Work

We situate our work in understanding user behavior and attitudes regarding passwords. Here, large parts of the literature focus on *coping strategies* that emerge with a growing number of accounts [4, 5]. For example, Stobert and Biddle conducted qualitative analyses to formalize the way users live with their passwords (the "Password Life Cycle") [13]. This model depicts how users choose, commit, reuse, and reset their passwords. Their work also delivers valuable insights into memorization and organization strategies: Users have mental lists of passwords, e.g. a list for important accounts or a list per website topic. Without explicitly mentioning, the findings contribute to a mental model of password reuse. This is important, because reuse is one of the most common coping strategies [3, 6, 7] and many researchers discourage it, because a breach at one site can compromise many others [1, 10].

To facilitate coping with passwords and possibly minimize reuse, dedicated tools have been investigated and proposed. Besides industry-driven password managers, HCI research has proposed a number of alternatives. For instance, Stobert and Biddle also propose a password manager that is designed to boost trust as it does not directly store passwords, but rather offers a image cues to recall passwords [12].

Finally, other researchers followed a mental model approach to understand how users make sense of security mitigations. For instance, Kang et al. utilized drawing tasks to establish users' mental model of data disclosure on the Internet [9] to find guidelines for more privacy-sensitive solutions. Bravo-Lillo et al. focused on creating a mental model of security warnings [2] to improve their framing and timing.

User Study Method

In our work, we aim to answer how non-users and active users of password managers make sense of their functionality and benefits. To do this, we chose semi-structured interviews including drawing tasks and qualitative analyses as this proved to be a good fit for this problem space [9, 13].

Questions and Participants

The interview was designed around three main questions: **(1)** *What are passwords used for?1* **(2)** *How do you cope with multiple accounts?* **(3)** *Could you sketch the functionality of a password manager?*

Where appropriate, we inquired personal experiences and

[1] US-American population only, http://www.pewinternet.org/2017/01/26/2-password-management-and-mobile-security/, May 24 2017

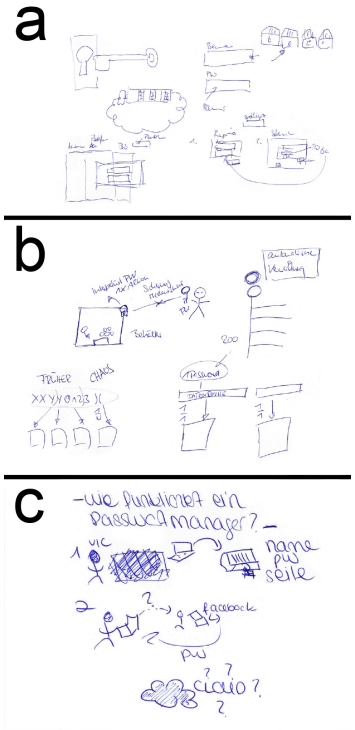

Figure 3: Outcome of the drawing tasks. (a) visually rich sketch with metaphors, interactions and form elements. (b) list and category visualizations. (c) actors, symbols, interactions

expectations towards PWM. We encouraged participants to sketch their explanations. If PWMs were too unfamiliar, we briefly explained their central motivation.

We approached people in cafes and on the street (like [16]). Participants were aged between 20 and 41 years. After the first six interviews, we changed this strategy because the sketches were too vague for deep analysis. Hence, we conducted eight more interviews with professional experience designers and concept developers. We expected they could better visualize their mental models, especially because all of them were non-IT-experts, but actively use password management software. All interviews were audio-recorded.

Interview Results

We made affinity diagrams to analyze the interviews (cf. Figure 2). The process was based on Young's proposed design strategy to create mental models [17].

Selection and Coping Strategies

All of the participants claimed to reuse passwords, which reportedly also causes them trouble when recalling the correct username-password combination. Their coping strategies were all well-known from literature [13]. However, we found that our participants were sometimes unaware of their own coping strategies. When we inquired more detail, most interviewees realized they categorized their passwords. The password categories were often derived by the context of the account, e.g. the URL, perceived importance, time of creation and the password policies of the website. In addition to contextual factors, individual algorithms seem to play a major role to establish password selection strategies. For instance, two participants reportedly memorize a list of words or a reduced alphabet that they combine into new pseudo-unique passwords. One participant generated a random password once, memorized the result, and reused it. Password reuse was not only justified by the number of accounts. If in a hurry, people reported to reuse a memorized password.

Impact of Password Managers

Six participants did not use a PWM (henceforth *non-users*), while eight actively used special software (henceforth *active users*). All active users reported that using password managers at work made them adopt such tools in private, too. After exposure at work, they migrated their passwords step by step into the software. Four active users reported that password sharing was the main advantage in the professional field: They can share access to different online tools to certain user groups and customers easily. However, they reported to keep creating passwords manually for the most important personal accounts and do not store them.

Drawing Task Outcome

Generally, sketching was difficult for all participants. While most could easily draw metaphors and their general idea of what passwords are used for, sketching the workings of a PWM was hard. Active users created sketches that had more detail regarding interaction and functionality.

Non-users: The sketches of non-users were all based on simple lists where each entry contains the website's name, URL, a user name and the password. The idea of a master password keeping this list safe was an emerging theme in the drawings. We noticed that this could be a result of their own password management strategy, which relied on handwritten lists and Word documents. None of the drawings indicated how people would interact with a PWM.

Active users: Active users had clearer ideas of what a password manager does. In contrast to the non-users they could immediately start drawing without further explanations. The results however did not focus on lists storing the passwords but mostly showed the interaction procedure

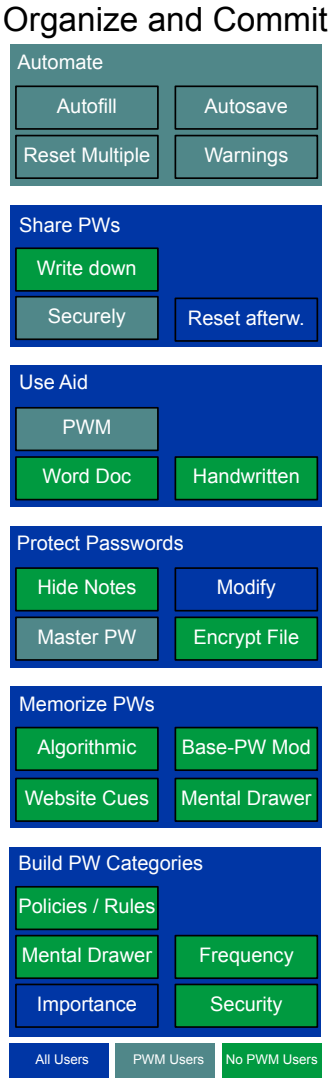

Figure 4: Task tower of mental space "organize and commit", adjusted vertically for space reasons. Different colors indicate which user group is more likely to take a certain action.

and website forms (see Figure 1 & 3). Account sharing and cross-platform access to passwords were mentioned as the most important features in addition to the basic functions. Active users expressed clear expectations about what PWM should and should not do, for example automate logins while staying in control of the password selection.

Mental Model of Password Managers

From the interviews and drawing analysis, we derive a first mental model of password management and dedicated tools to support it. The resulting mental spaces were:

Create: Users have certain expectations and needs when they create accounts. This task tower consists of contextual influences like policies or personal preferences. Also, our participants expect guidance from tools to create secure credentials. This can be simple password generators, feedback and improvement (e.g. [11, 14]), and suggestions on how to find mnemonic devices.

Organize and Commit: Every participant mentioned some way of organizing their passwords. Here, the key needs are memorization techniques and building implicit or explicit categories. Users who already have a PWM expressed the need for automation (see Figure 4).

Log-In: Our participants expect deep integration into browsers and other places that need credentials. Here, password managers should offer control over automatic and manual log-ins, and participants indicated that different device types play a role for log-ins. For instance, the PWM should be a central tool to log in across devices. Moreover, the system should support failures appropriately, e.g. password resets in case the stored password is invalidated.

Respect User Perceptions: Our participants had individual perceptions of password security, too [15]. Thus, a PWM must show careful explanations when it offers help that does not match users' expectations. Our participants also felt that PWMs should not offer to store banking account details, which we interpret as trust issue.

Implications and Conclusion

In short, we found that while PWMs were a black box for non-users, active users often regarded PWMs as database for passwords, which also has some automation features. Based on the results, we show how adaptation might boost the user experience of future PWMs.

Customize and Personalize Most participants continue to create passwords with their individual strategy even after adopting a password manager. To support this, users could specify their password creation algorithm to speed up creating memorable passwords (e.g. [11]). Also, the PWM should offer a set of default password-"lists", because users are often unaware of their categorization approach until they see an example. The PWM could ask whether it should automatically put passwords into lists based on the perceived importance or strength of the password.

Adjustable degree of user control While active users liked automation, they also emphasized to stay in control of what is stored by the PWM. Non PWM users are also fully in charge of their passwords, which we interpret as central need. Future PWM systems can adapt to this and refrain from storing banking credentials to boost trustworthiness.

Usage context Exposing employees to password management software can positively influence personal security strategies. Tools thus can also adapt features to their usage context, to bring more benefits even to people who have not used a PWM, e.g. by focusing on the "list" metaphor.

In the future, we will further substantiate the mental model by investigating how it translates to implementations of current password managers and how they can be improved.

REFERENCES

1. Joseph Bonneau. 2012. The science of guessing: Analyzing an anonymized corpus of 70 million passwords. In *Proceedings - IEEE Symposium on Security and Privacy*. IEEE Comput. Soc, 538–552. DOI:http://dx.doi.org/10.1109/SP.2012.49

2. Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. 2011. Bridging the Gap in Computer Security Warnings: A Mental Model Approach. *IEEE Security and Privacy* 9, 2 (2011), 18–26. DOI: http://dx.doi.org/10.1109/MSP.2010.198

3. Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and Xf Wang. 2014. The Tangled Web of Password Reuse. February (2014), 23–26. http://www.jbonneau.com/doc/DBCBW14-NDSS-tangled

4. Dinei Florêncio and Cormac Herley. 2007. A Large-Scale Study of Web Password Habits. In *Proceedings of the 16th international conference on World Wide Web (WWW '07)*. ACM, 657–665. DOI: http://dx.doi.org/10.1145/1242572.1242661

5. Dinei Florêncio, Cormac Herley, and Paul C. Van Oorschot. 2014. Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts. In *Proc. USENIX Security*. USENIX Association, San Diego, CA, USA, 575–590. https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-florencio.pdf

6. Shirley Gaw and Edward W. Felten. 2006. Password management strategies for online accounts. In *Proceedings of the second symposium on Usable privacy and security (SOUPS '06)*. ACM, New York, NY, USA, 44–55. DOI: http://dx.doi.org/10.1145/1143120.1143127

7. Eiji Hayashi and Jason Hong. 2011. A diary study of password usage in daily life. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. ACM, Vancouver, BC, Canada, 2627. DOI: http://dx.doi.org/10.1145/1978942.1979326

8. Philip Inglesant and Martina Angela Sasse. 2010. The True Cost of Unusable Password Policies: Password Use in the Wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. 383–392. DOI: http://dx.doi.org/10.1145/1753326.1753384

9. Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. "My data just goes everywhere": User mental models of the internet and implications for privacy and security. In *Symposium on Usable Privacy and Security (SOUPS) 2015*. USENIX Association, 39–52. https://www.usenix.org/system/files/conference/soups2015/soups15-paper-kang.pdf

10. 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. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. 2595–2604. DOI: http://dx.doi.org/10.1145/1978942.1979321

11. Sanam Ghorbani Lyastani, Sascha Fahl, and Michael Backes. 2016. Improving Password Memorability and Strength Using Mangling Rules. In *Symposium on Usable Privacy and Security - Extended Abstracts (SOUPS '16)*. USENIX Association, Denver, CO, USA.

12. Elizabeth Stobert and Robert Biddle. 2014a. A Password Manager that Doesn't Remember Passwords. In *Proceedings of the 2014 workshop on New Security Paradigms Workshop*. ACM, New York, NY, USA, 39–52. DOI: http://dx.doi.org/10.1145/2683467.2683471

13. Elizabeth Stobert and Robert Biddle. 2014b. The Password Life Cycle: User Behaviour in Managing Passwords. In *Proceedings of the 10th Symposium On Usable Privacy and Security (SOUPS '14)*. ACM, New York, NY, USA, 243–255.

14. Blase Ur, Felicia Alfieri, Maung Aung, Lujo Bauer, Nicolas Christin, Jessica Colnago, Lorrie Faith Cranor, Henry Dixon, Pardis Emami Naeini, Hana Habib, Noah Johnson, and William Melicher. 2017. Design and Evaluation of a Data-Driven Password Meter. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems (CHI '17)*. ACM, Denver, CO, USA, 3775–3786. DOI: http://dx.doi.org/10.1145/3025453.3026050

15. Blase Ur, Jonathan Bees, Sean M Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. 2016. Do Users ' Perceptions of Password Security Match Reality ?. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16)*. ACM, San Jose, CA, USA, 3748–3760. DOI: http://dx.doi.org/10.1145/2858036.2858546

16. Emanuel Von Zezschwitz, Alexander De Luca, and Heinrich Hussmann. 2013. Survival of the shortest: A retrospective analysis of influencing factors on password composition. In *Human-Computer Interaction – INTERACT 2013, Lecture Notes in Computer Science*, Paula Kotzé, Gary Marsden, Gitte Lindgaard, Janet Wesson, and Marco Winckler (Eds.). Vol. 8119. Springer Berlin Heidelberg, 460–467. DOI: http://dx.doi.org/10.1007/978-3-642-40477-1_28

17. Indi Young. 2008. *Mental models: aligning design strategy with human behavior*. Rosenfeld Media.