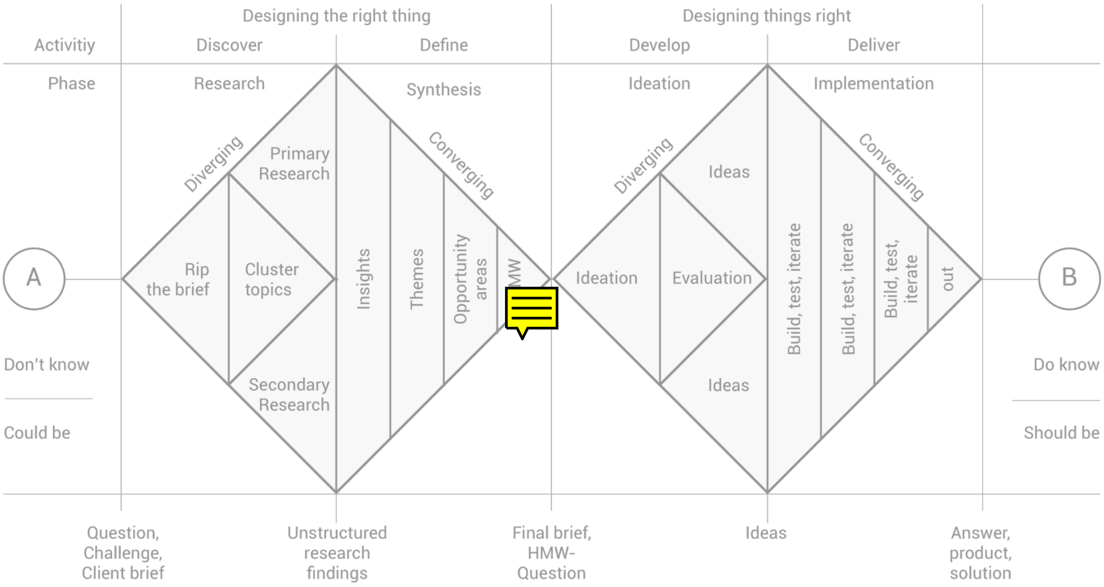

Figure 13.1: One version of the "Double Diamonds" to structure a traditional Human-Centered Design process. The P4P framework partially adapts this process and tailors it to password authentication. Image by Dan Nessler https://medium.com/@dan.nessler *(last accessed 24.03.2018)*

Eight Recommendations for the Future

The above summary allows [illegible] give recommendations on service design and research areas. Some bullets confirm prior work and listing them again should be seen as an emphasis.

1. **Consider the evolution of mental models**. Coping strategies adjust to the task load generated by passwords, which fluctuates throughout the years. Users might see complexity as the primary strength component, but this might change as service providers adjust to the recommendations from empirical usability research.

2. **Put less emphasis on password *strength***. Some researchers have demonstrated that beyond the threshold for online attacks, the benefits of increased password strength are limited. The most important scenarios that really require a strong (and usable!) password are master-passwords and accounts holding particularly sensitive data, e.g. a Dropbox that is full with health records or credit card details.

3. **Remove restrictions, give autonomy**. Service providers should eradicate unjustified complexity requirements, because they have strongly contributed to unreasonable mental models in the past. Instead, foster password diversity through autonomy, i.e. by empowering users to be creative and make informed decisions. We found that users want to be reasonably secure, but often lack the creativity to come up with adequate

passwords. The *show-explain-help-empower* paradigm can overcome this creativity barrier and act as an overall guideline for authentication even beyond passwords.

4. **Prepare for more requests of password replacement schemes**. More and more people are willing to use biometrics as primary authentication method[1]. They will expect this technology from products. However, companies often market biometrics as panacea for usable and secure authentication, and fail to make users aware of the ramifications. Therefore, passwords are going to be met with resistance, and we need to reassure users that passwords have irrefutable benefits in certain situations.

5. **Extend the method space**. We note a strong tendency towards studies facilitated through mTurk. While the methodology is robust for eliciting quantitative data, the results are only one side of the truth. MTurk studies answer *what works best*, but often fail to explain *why* things work best. Therefore, resurrecting mixed-methods approaches that address qualitative aspects is recommendable for future USEC research.

6. **Stay realistic**. Nudges wear off over time, so we have to constantly create new persuasive strategies. Then again, users quickly resent paternalistic guidance and also prefer things to stay as they are. We have to acknowledge that there is only so much we can do. Persuasive support strategies will not work for all users in the same way, but if they reach even a small target group and make their lives a little easier, I believe that they are impactful enough.

7. **Follow risky ideas**. If we look at the current landscape of research on password support, the design space appears narrow: most published research tackles password meters in different facets. I argue that taking inspiration from other research areas, e.g. behavioral economics, can generate ideas outside the usual spectrum. They might be risky in terms of predictable effect size, but they certainly can counteract habituation effects.

8. **Give feedback**. Researchers cannot expect that service providers read academic research papers (let alone dissertations). Therefore, we as a community of user advocates have to become active and point out where things go wrong. For instance, it is important to report issues with password policies to service providers. I have engaged in discussions with globally operating companies and was met with an open ear for improvement areas. In the end, this might translate research into graspable impact.

Conclusion

This thesis has presented a new perspective on a well-known and perhaps unsolvable problem: coping with passwords is hard and annoying for most of us. Nonetheless, reducing the frustration component is a highly desirable goal. Hence, we contributed new insights into the factors that shape coping strategies (mental models, personality) and how to design for the

[1] https://www-03.ibm.com/press/us/en/pressrelease/53646.wss *(last accessed 26.03.2018)*

feasible to take the opposite approach. Since we were able to answer our research questions satisfactorily, the choice of our methods was plausible, but future studies might need to reconsider them.

Moreover, we refrained from collecting plain-text passwords for ethical reasons. While other researchers save passwords in clear text, they also need to provide a higher standard of protective mechanisms, like locking access to the data and analyzing it off-line. Since we did not the resources for such procedures, we found it more reasonable to hash passwords if they needed to be stored. This limits the available depth of post-hoc analyses, which is a caveat. At the same time, the consistent usage of the zxcvbn estimator provided sufficient and reliable details about passwords for the analyses we required. We did, however, have to modify it in order to strip it from sensitive information.

13.2.3 Real-World Measurements

Apart from the log analysis of *PASDJO*, we could not collect data *in the wild*. The concepts we evaluated in Part III were not yet mature enough to warrant production-level deployment of the nudges. We tried to increase ecological validity by following established practices in password research (cf. Section 3.1). While these attempts let us assume that participants immersed themselves in the tasks, there is always a small gap between study and real-world contexts. Therefore, we have to leave deployments of our concepts, e.g. emoji-passwords or feedforward techniques, to future work. Moreover, coming back to recommendation 5, we might be able to assess the ecological validity of the existing data through ethnographic methods, e.g. diary studies or contextual inquiry.

13.2.4 Ethics and Risks

Studying the users' psyche, like cognitive biases and personality, to aid the design of persuasive interventions bears certain ethical risks. Often, we investigate unconscious phenomena, for instance, how the decoy effect influences users' decision-making. Therefore, we need to always consider how findings in this area might be exploited. There was a recent episode of questionable analysis of personality profiles: Cambridge Analytica, a British political consulting firm, accessed Millions of Facebook users' data without their consent to target political campaigns based on their personality and other factors[2]. Although studying users' personality to support them in password authentication appears less critical than politically motivated manipulation techniques, we still have to weigh the benefits against the risks. For instance, if future research corroborates our findings about the associations between personality and password selection, this might allow adversaries to target attacks more efficiently.

[2] https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html *(last accessed 27.03.2018)*

Thus, the P4P framework includes this important aspect in the hope of seeing more discussions of ethical risks in the future.