BEAM: Reimagining Password Management

Amy Huang, Ching-Yi Lin, Jing Xiong, Ayo Animashaun

MIMS Capstone Project Report
May 2019

Introduction

Passwords and login information are not only a common part of most people's everyday life, but they also control access to some of the most important aspects of it, such as banking and finances, medical services, social media, and other sensitive personal information. However, many people still make and use weak passwords. Some will use the same password for multiple services, and some do use complex and unique passwords, but forget their passwords frequently.

Although there are existing password manager solutions that attempt to help people reduce the cognitive load of creating and memorizing complicated credentials, these types of tools have not been widely adopted. One study reported that only 12% of Americans used a password manager in 2016 [1]. Existing password manager solutions are likely not being used by many due to the perception of them being not valuable and/or difficult to use. How do we remedy this to make password managers more valuable and approachable?

Most people operate on the assumption that passwords should be kept secret and never shared. However, the reality is that password sharing is more common than we think. Have you ever managed joint banking accounts with your spouse? Shared shopping accounts, like Amazon? Shared Github accounts with your coworkers? Helped your parents or grandparents remember and manage their passwords?

The way people currently communicate actual usernames and passwords, either via emails or messaging applications without concern for message encryption, is compromising their digital security. In addition, once a password is shared, the owner has limited visibility about how the shared password is stored and used by others. However, we have found that password sharing can be a positive trigger to help introduce people to password management tools. We aim to design a solution that normalizes sharing and helps people feel more in control and competent when sharing passwords, with the ultimate goal of encouraging people to adopt better password management practices all around.

Related Work

Password Manager Adoption

Alkadi and Renaud investigated what factors impeded and encouraged adoption of password managers by analyzing reviews of two popular password managers, LastPass and 1Password, on application stores and an online survey with 352 responses. The identified a wide range of influential factors in the password manager adoption lifecycle, including (1) lack of awareness, (2) no perceived usefulness, (3) security concerns, (4) sense of mastery, (5) poor usability, (6) lack of knowledge, and (7) distrust [2]. However, there is no comparison on the effectiveness of different factors.

Password Reuse

Wash et al. [3] studied on people's choices in password generation and reuse. They analyzed self-reported online behavior data gathered from 134 participants for six weeks in 2016. They found there is statistically significant correlation between password reuse and strong password, which suggested that people actually reuse their strong password. Ur et al. found some people reuse passwords with no security concerns because they felt their password is strong enough to reuse [4]. Although password managers help reduce the memory demand for maintaining large sets of unique and complex passwords [2], having a password manager is not a statistically significant predictor of whether a password will be reused. Wash et al. found password manager don't affect reuse based on their regression analysis [3] and Pearman et al. also reached to the same conclusion from their study of 154 participants over an average of 147 days in 2017. They also found the presence of a password manager did not have a statistically significant predictive effect on a user's password strength [5]. However, since the results are purely obtained from quantitative data analysis, there is no qualitative analysis to provide more insights with regards to the reuse behaviors of people who have adopted password manager.

Password Sharing

Kaye summarized a variety of sharing scenarios from 122 participants' self reports in 2011. Partners and close friends share their email and social media accounts, "one third of respondents shared their personal email password, and a quarter shared their Facebook password"; children help their parents to remember passwords and share back with them when the parents forget the password; siblings temporarily grant access to the other for urgent matters; colleagues share passwords with each other for collaboration [6]. While password sharing is often seen as a bad practice, some studies show that password sharing facilitates trust and productivity, and that there are certain situations that password sharing is appropriate and necessary [7][8]. Kaye suggested "password sharing (is) not as a deviant practice to be stamped out, but rather a nuanced practice engaged in with thought and care."

Sharing could be either a positive or negative influencer to one's password behavior. As identified by Alkadi and Renaud, "safe sharing" is one of the encouraging factors that makes users perceive usefulness in password managers. Some users illustrated the use case of sharing passwords and personal information with their partners through password managers [2]. However, password sharing also could introduce serious risks in an organizational setting. Inglesant and Sasse found some organizations left extremely weak passwords unchanged for years for sharing because of the difficulty of distributing the new password to a number of users. In addition to the organizational long term sharing, they observed that ad-hoc and one-time sharing happens when employees try to share a time-critical work with their colleagues. The employee picks a random word to be the password and emails it to the recipient for one-time sharing with a mindset of "just get it done" [9].

Research

Generative Research Methods

Qualitative Interviews

We conducted semi-structured interviews to allow flexibility for participants to go into each talking point with as much or little detail as they wish. This type of interviewing style suited our research objectives because our team's main objective was to understand participants' password habits without any real expectation of the answers we were going to receive. In addition, our team wanted to be able to reframe (ie: shift perspective about) the problem to be solved, so semi-structured interviews provided an avenue for participants to discuss their pain-points in a narrative, which allowed the team to uncover previously unrealized possibilities for design. The method also gave us the ability to ask participants for more detail, and to follow up or delve deeper on any topics that came up in conversation.

The first round of qualitative interviews consisted of 2 cybersecurity experts and 9 users: 5 who have never used password management solutions, 3 current users of password management solutions, and 1 user who tried using it but gave up. The goal was 1) increase our understanding of the subject matter and 2) to understand people's behavior in creating and maintaining passwords and their experience with password management solutions or why they choose to not adopt it.

We also conducted a second round of interviews focused on understanding people's current experiences with sharing passwords. This round consisted of 7 interviews.

Card Sorting

In our first round of interviews, we implemented a hybrid card sorting method which began as a closed card sort, but eventually allowed participants to create cards that may be missing from the card deck. In this version of our card sorting activity, participants who were current users of password managers were asked to categorize different features of current managers into

categories of most useful to least useful. This research technique provided the team with insights about how participants used their password managers, and exposed some of their motivations for doing so - the activity aided in corroborating our team's understanding of participant's mental models.

Later, in a summative assessment of our prototypes, we evaluated whether or product elicits the desired emotional response from users using another card sorting technique. We identified a balanced set of 30 positive, negative, and neutral adjectives that we wanted users to feel(or not feel) when using our prototype. We then created a set of flash cards with a single adjective per index card. After evaluating our product by accomplishing tasks, we asked them to pick four cards that described how the product made them feel. We then asked them to explain why they chose each card. Afterwards, we conducted affinity diagramming on some themes participants highlighted. This was particularly helpful for understanding the affective impact of our product on the users as well as giving us an opportunity to talk with users about facets of the product that we may not have had a chance to directly ask them about.

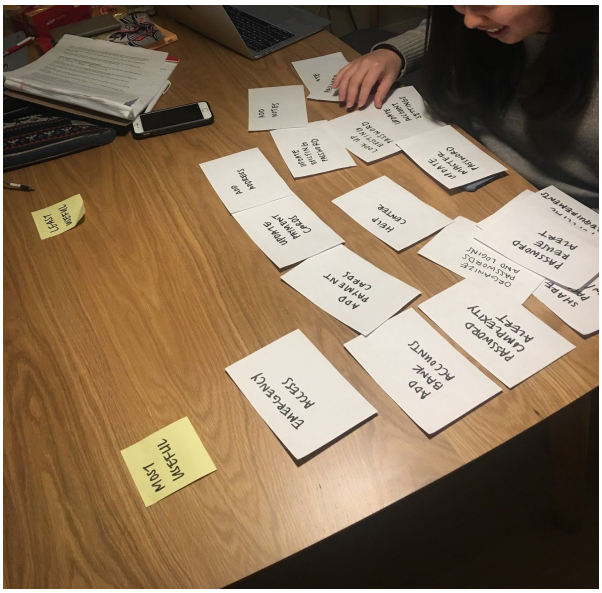

Fig 1. User conducting card sorting exercise for most to least useful features in password manager solutions

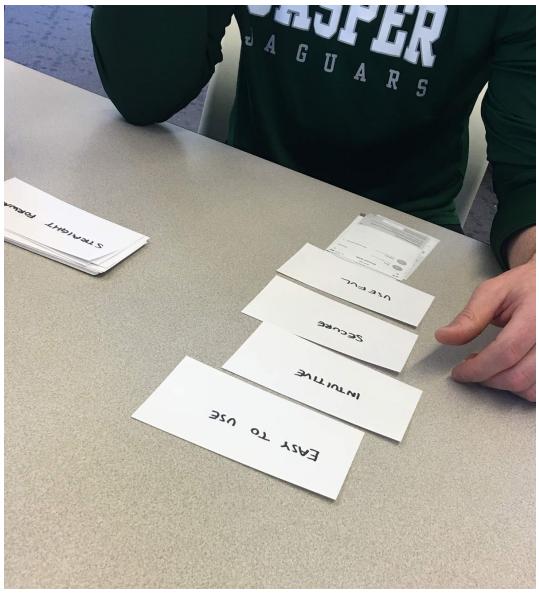

Fig 2. User selecting emotional response after testing the prototype

Competitive Usability Evaluations

We sought to understand how other password management solutions set up to solve the same design problem. Our team examined the relative strengths and weaknesses of competing designs in the password management space. The objective of this competitive evaluation was to see what competitors are doing, how they're doing it, what's working and what's not. These competitive evaluations allowed us to test several approaches that have been tried to solve the same design problem. In addition, the reactions of users provided some insight into how non-users react to password managers, and exposed their mental models and current behavior when managing passwords. Learning from others' designs helped our team create a better prototype.

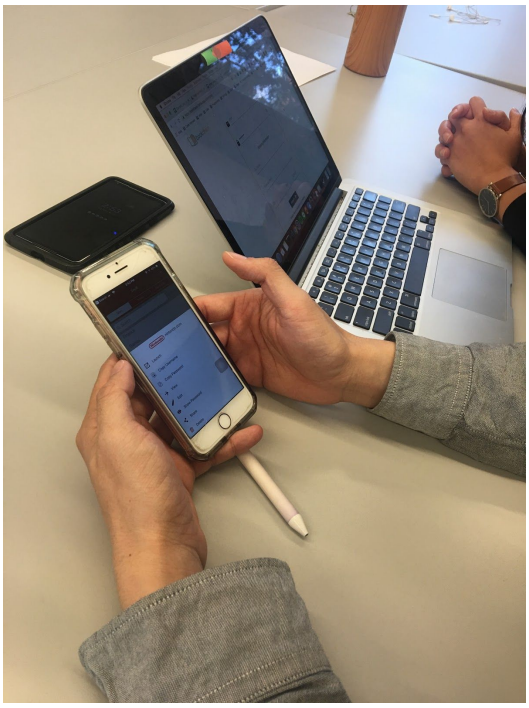

Fig 3. User performing usability tasks on the mobile version of LastPass

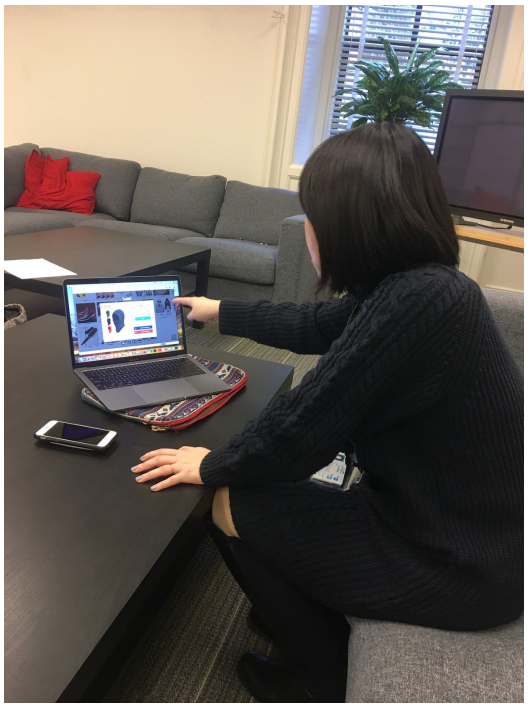

Fig 4. User performing usability tasks on the desktop version of LastPass

Formative Evaluative Research Methods

These research methods were used to discover insights and shape the design direction in the early stages of our product development.

Cognitive Walkthrough

This is a usability inspection method based on the belief that people learn design systems by trying to accomplish tasks with a system, rather than reading through instructions. In this usability evaluation method our team put ourselves into the shoes of our intended user group and walked through scenarios in our low-fidelity prototype. This method allowed our team to cover scenarios and identify a range of issues in our low-fidelity prototypes. When examining individual issues, we considered if the issue could be applied more generally across the product. The insights gained using this method were used for further iteration on the designs. This method was particularly helpful because it did not require recruitment of external participants, which was often time-consuming and resource-intensive. It also allowed us to inspect the usability of Critical User Journeys(CUJs) within the prototype.

Fig 5. The team performing cognitive walkthrough on paper prototypes

Rapid Iterative Testing & Evaluation (RITE)

RITE is a formative usability evaluation method that is designed to quickly identify any large usability issue that is preventing users from completing a task or does not allow the product to meet its stated goals. In employing this method, all members of our team observed all sessions, and following each session where a blocking usability issue was identified, agreed on a solution. The designers on the team then updated the prototype and another session was conducted to see if the solution fixed the problem. In situations where our team could not agree on the severity of a usability issue identified, we conducted an additional session before any changes were made to the prototype. We continued this cycle of immediately fixing and testing updated prototypes until multiple sessions were conducted where no further issues were identified. In contrast to traditional usability testing where five or more people see the same design, in our implementation of RITE, only two participants saw the same design before changes were made for the next session. This method required the dedication of our entire development team because all members needed to observe each session and brainstorm solutions following each session. In addition, the prototype had to be updated quickly and repeatedly. However our team felt confident that we built a product free of major usability issues after implementing this method with a total of 6 participants.

Research Results

Qualitative Interviews

The qualitative interviews with the security experts allowed us to understand the importance of assessing what a user's threats are and what they have to protect in order to build an appropriate tool for them. Practicing good security is also largely about having a back-up plan that prevents people from accessing your information.

From the users in the never used password management solutions group, we found they tend to create passwords that are easy to remember and only have a handful of passwords that they use on rotation. If they do need to keep track of their passwords then they either write it down

on paper, keep a digital note, or rely on memory. One user mentioned, “I write down my passwords in a notebook. I have my own system of generating passwords, it is usually a combination of things that are personal to me that I can easily remember.” Some users mentioned that they did not want to pay for a password management solution because they don’t see the value matching the cost. Others mentioned that they didn’t want to rely on a password manager to remember their passwords for them and them having to be dependent on the password manager all the time.

The current users of password management solutions were very conscious about the need to protect their digital security. They use system generated random passwords for their accounts and have unique passwords for almost all accounts. One user mentioned, “I usually use auto-generated passwords 95% of time.” All interviewees also expressed that at one point in time they had tried to influence their spouses and people around them to adopt better password security practices. Some were successful and some were not.

The user in the tried but gave up user group uses a variations of two passwords for all her online accounts. One of the reasons she didn’t continue to use one was because she felt that it was risky to keep all her passwords in one area. However, she does realize that she is doing the same thing now with keeping it in a Google doc. On the other hand, she uses a password manager for work because there are too many passwords to remember and they are updated quite frequently, which makes it hard to keep track.

From the first round of qualitative interviews, we concluded that some people may be satisfied with their current practices so since they aren’t encountering any problems, then they don’t feel the need to seek any solutions. However, from some of the stories, we noticed that password sharing with family and spouses came up a couple times and some struggles were mentioned. Thus, we made a hypothesis that users who need to share passwords with others might not have an effective way to share and manage those passwords. We conducted a second round of interviews focused on understanding people’s current experiences with sharing passwords to see if we could identify any specific problems in this area that we can solve. This round consisted of 7 interviews.

From the interviews, we found that sharing passwords was actually a very common activity. For example, some people had to help their parents and grandparents manage and remember their passwords. Married couples needed to share financial or insurance related accounts. Colleagues need to share passwords for work. We found that these people who did share passwords did not have a very secure way to share them. It was either over the phone, written in a text message, email, or using an existing password manager solution that did not work well for one or both parties. One couple we talked to uses an encrypted excel sheet for shared passwords, however, over time, the passwords became outdated due to lack of updates. “The excel sheet is local and password encrypted. But the ironic thing is that I think I forgot the password to that. I think I know what it is. I haven’t logged into that in a long time.”

Card Sorting

From the card sorting exercise of all the features in existing password management solutions, we found that users found the core functions to be the most useful. They wanted to look up passwords, update passwords, update master password, and add new logins/passwords.

Competitive Usability Evaluations

We conducted usability testing of two existing password management solutions, LastPass and 1Password, on 5 users who have never used password management solutions before. We found that branding and color played an important aspect on whether the application was deemed trustworthy. The idea of auto-generated passwords also caused some skepticism and confusion. The overlapping product reaction cards that the most users chose were efficient, surprised, and overwhelmed.

Rapid Iterative Testing & Evaluation (RITE)

We received the following feedback from the usability testing:

- “Intuitive to use, and it’s appealing. I like the interface. It’s really quick. and I think it’s **innovative** because of the permissions for sharing.”
- “I like the **expiration settings** for password sharing”
- “I think it's trustworthy because of the helpful prompts at certain times. **I felt like it was looking out for me.** “
- “I really like the idea of secret phrase because it **adds extra layer of security.**”

- “I think a great use of this app would be when a close family member has passed and they may have most or all passwords for accounts they are able to easily share it before they pass.”

Key Insights and Patterns

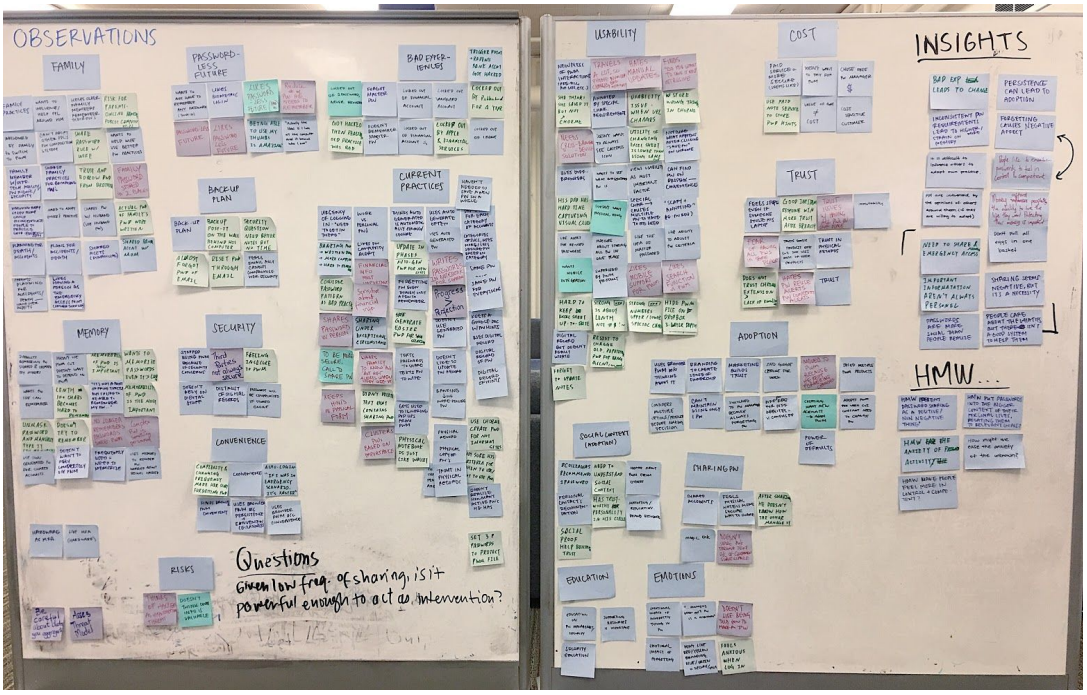

Fig 6. Affinity diagram to identify key insights and patterns

We consolidated our observations and created an affinity diagram to find patterns. From all the user interviews and usability testing, we found the following key insights and patterns:

- Inconsistent password requirements leads to a strain on memory
- Sharing seems negative, but it’s a necessity
- Passwords are more social than people realize
- Forgetting causes negative affect - feelings of lack of control
- People need to share and maintain emergency access
- People care about the “what if”s but there isn’t a good system to help them

Passwords are often seen as a personal item that should not be shared with others. However, when you have to help your family members remember their passwords or share important bank or insurance account passwords with your spouse, then password sharing becomes a necessity. The current solutions on the market have password sharing capabilities, but the

added complexity of additional features makes the point of entry seem intimidating. How might we normalize password sharing and provide a safe way to do it? How might we ease the anxiety of the unknown? How might we make people feel more in control and competent when sharing passwords?

Design

Overview of Concept

Our proposed solution is a password management application that is focused on sharing. As previously discussed, sharing is an activity that many people already do, albeit in relatively unsafe ways. We propose that our application can normalize sharing and turn it into a positive trigger for improving password security.

Our solution is a mobile application and a desktop browser extension that helps users store and manage their online account credentials and also provides ways share and manage access to those credentials. We provide visibility into when the receivers of their credentials are using their credentials to access their account.

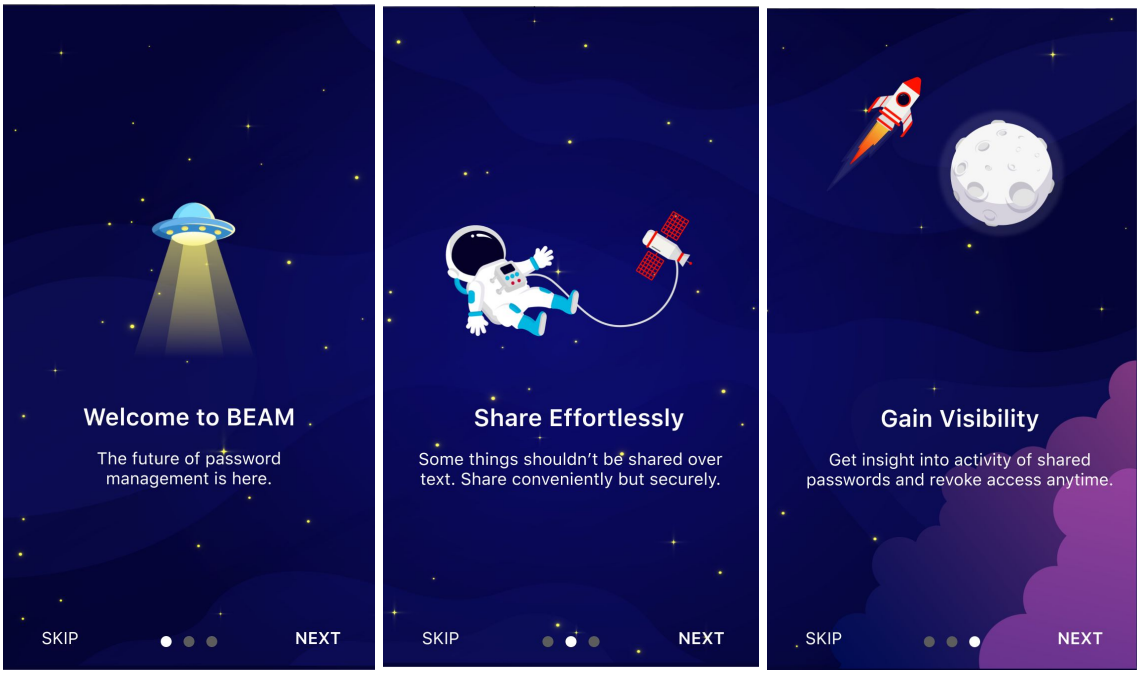

Fig 7. Walkthrough process of BEAM

Key Design Decisions

Sharing as a trigger

We assume that most people just starting to use a password management solution will have mostly the same few passwords being reused for many accounts. However, it's a lot of work to start changing all of your passwords at once. We try to make this process gradual instead, making it easier to achieve. We remind users to update their passwords during key moments, such as before sharing and after revoking access. If the user follows our prompts, they can prevent receivers from seeing passwords that might be repeated for other accounts. They can also ensure that access is truly revoked by changing the password to their account. Finally, this also helps them slowly update their passwords to be unique across their web accounts, making it a more manageable process to increase their overall online security.

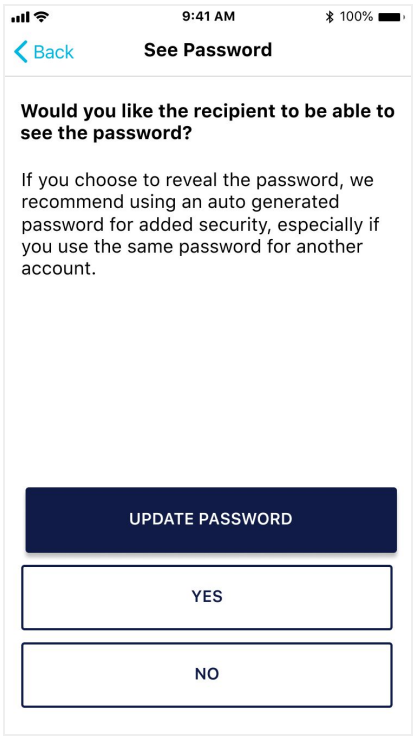

Fig 8. Prompt received when sharing password

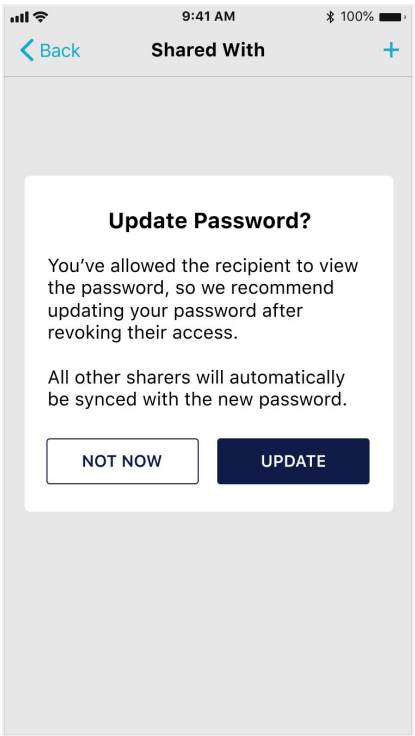

Fig 9. Prompt received when revoking access

Guided password update process

We guide users through the entire process of updating their password, including helping them keep track of their current password, generating or helping them remember their new password, and updating Beam records after the process to ensure that the changes are recorded.

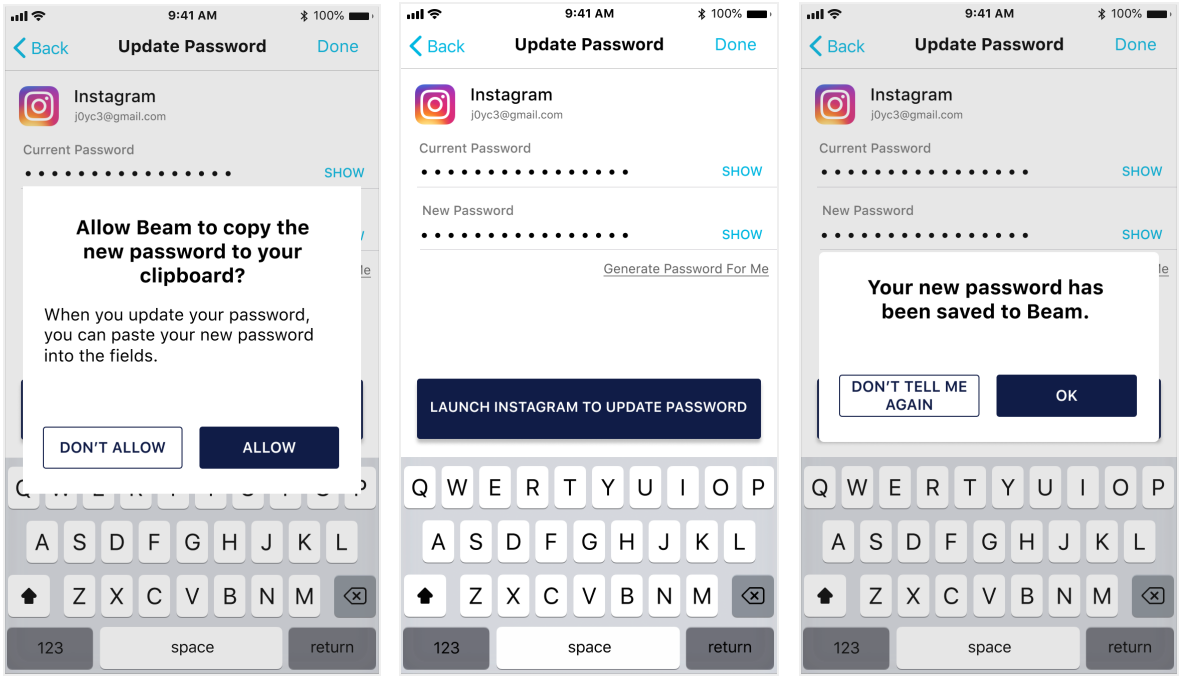

Fig 10. Guided process to update password

More control over sharing

Users are given unprecedented control over how their credentials are shared. They can fine-tune the sharing duration, control whether or not the receivers can see their actual credentials, and require a secret phrase as an extra layer of security. They can also opt to only give one-time access which will allow the receiver to launch the account only once.

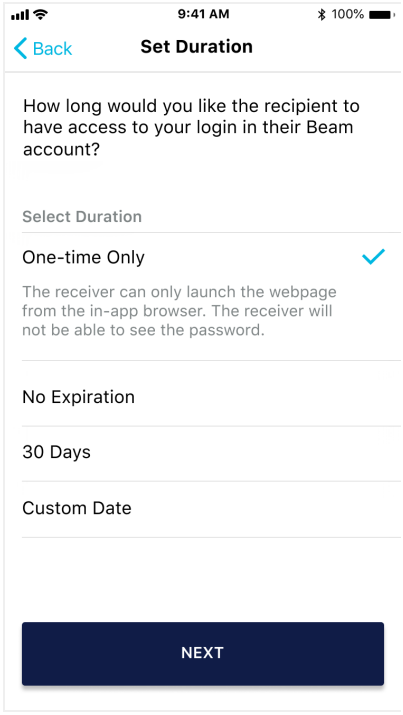

Fig 11. User as ability to specify access duration

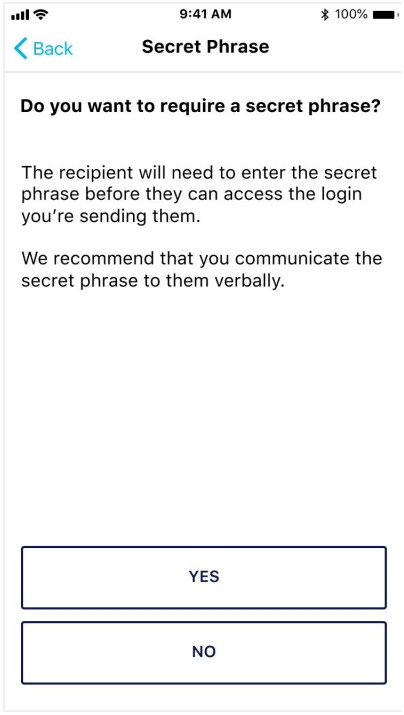

Fig 12. Secret phrases provide an extra layer of security

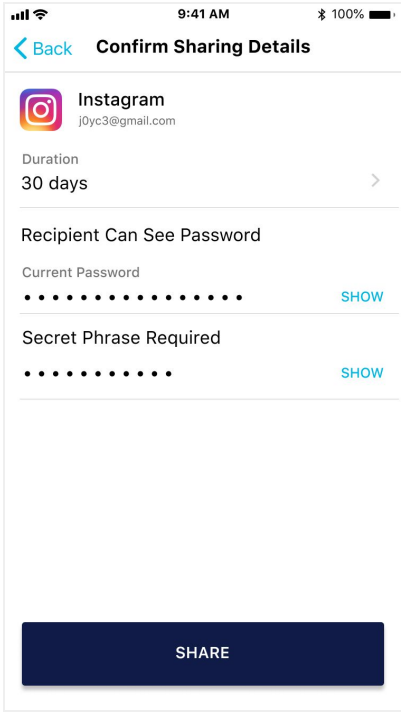

Fig 13. User can confirm sharing details before sharing

Visibility into receivers' activity after sharing

Receivers who are not given view access must access the senders' accounts via Beam's in-app browser. This means that Beam is able to provide senders visibility into the usage activity of their credentials after sharing, allowing them to be better informed about when and how often their receivers are accessing their accounts.

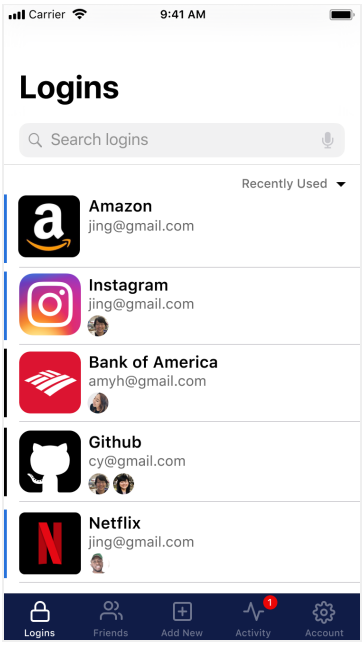

Fig 14. Homepage shows all logins that are personal and shared from others

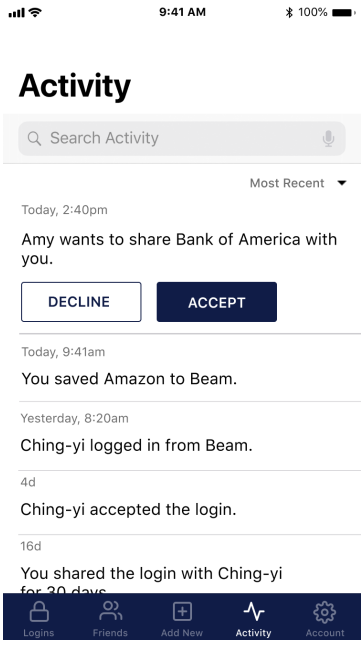

Fig 15. Activity gives an overview of password activity and users can see sharing requests

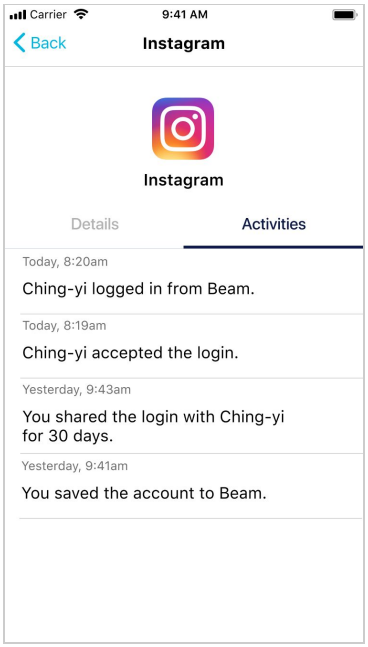

Fig 16. Activities view within a specific account gives an overview of password activity for a particular account

Risk management

While other password managers also offer some controls over sharing such as allowing the receiver to see or not seeing the password, they don't account for the fact that, in reality, there are many ways for the receiver to save the password without them knowing. Our design mitigates some of these risks by only allowing receivers to access the account from our in-app browser if the sender chose not to reveal their password to them. We also remind the sender to update their password after revoking access or after access expires for their receiver in cases where the receiver was allowed to see the password to ensure that access to their account is truly revoked.

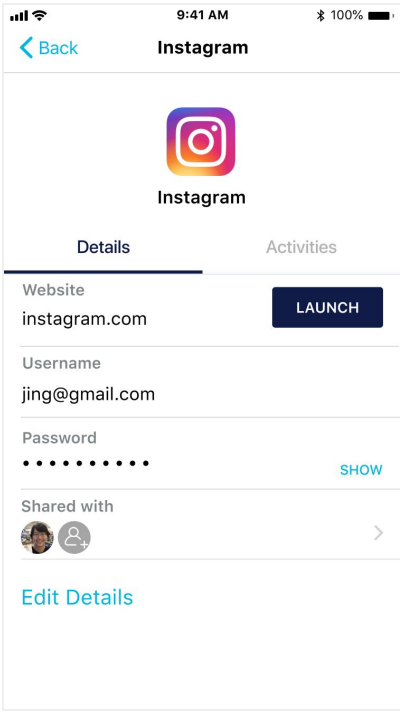

Fig 17. User can share from the Details view

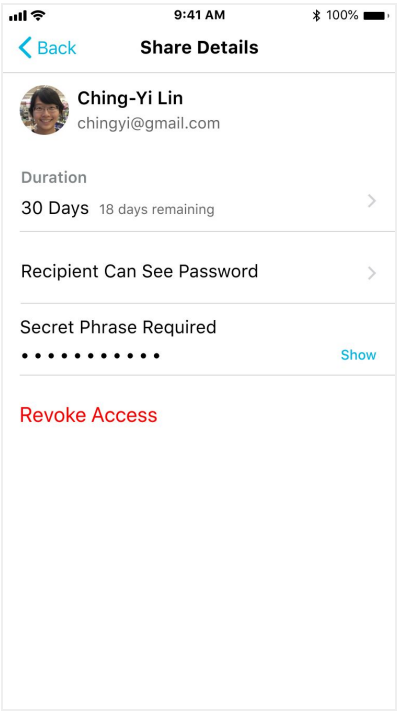

Fig 18. User can revoke access at anytime

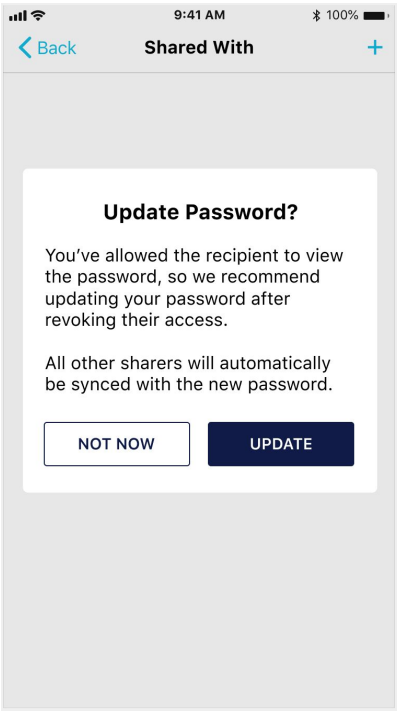

Fig 19. Alert to update password if user chooses to revoke access

Development

We were able to develop a native iOS mobile application using Swift. We chose to develop a native mobile application because there is a lot of uncertainty with the hybrid app framework in terms of support and compatibility to the native iOS framework that our app depended on. We needed to integrate with the iOS Authentication Services framework (https://developer.apple.com/documentation/authenticationservices) in order to provide the user with autofill functionality. We also needed to make an app extension as a credential provider (https://developer.apple.com/videos/play/wwdc2018/721/) in order to retrieve the stored credentials and autofill for the users when the app is not running.

Tech Stack

Realm (https://realm.io/)**:** We used Realm as the database of our mobile app to store apps local data.

CloudKit (https://developer.apple.com/icloud/cloudkit/)**:** In the current version, we used CloudKit to share credentials between users.

Data Storage: In the current version, we store the credentials locally. We also provide iCloud sync option for users to back up their encrypted credential data. The encrypted data will be transmitted through CloudKit provided by Apple with out-of-box security and privacy. We chose CloudKit because it has strong emphasis on users privacy and security, and its official support provided by Apple.

Future Work

In future research, we hope to investigate user conceptions of trust and reliability while using the application 'in-situ.' This research would be conducted in a diary study in which we collect qualitative data about user behaviors, activities, and experiences over time. This data will be self-reported by participants longitudinally. The research would also provide insight into what capacity users engage with the product, as well as what their primary tasks are. In addition,

designers may be able to learn what motivates people to perform specific tasks, particularly sharing, and how users are feeling and thinking when using the application.

We also hope to conduct a beta test of the application with a small group of users including target demographics that we were unable to reach during the RITE usability evaluations. These demographics include the elderly, adolescents, and people with disabilities. The beta test would allow the development team to iterate on the design by fixing usability issues logged by beta testers. We hope to conduct these beta tests prior to a full release of the application in the iOS App Store, and a subsequent release in the Android app store.

Conclusion

The development of our application required a deep understanding of the complete range of functional, emotional, and social needs people have when handling passwords which allow them to gain access to various online capabilities. In our research we sought to understand motivations for different password management behaviors. In addition we examined the desirability and ease of use of our application, as well as reactions to innovative new features such as ‘length of sharing permissions’ and ‘secret phrase multi-factor authentication.’ Our design goal was to ease the burden and anxiety that comes with this shift in cognitive awareness.

In our design we sought to constructively balance the often competing values of security and ease of use as it relates to the maintaining of passwords. While password sharing may be infrequent, it is nevertheless pervasive in that many people have to do it occasionally. Our app utilizes this behavior as a triggering point for the use of our application as a password management tool. We employed straightforward and easy to understand language in our prompts to encourage users to adopt safe practices when sharing passwords. We hope that by using this tool, users will not only be able to organize and safely share their passwords, but also learn about and become more aware of where risks lie for their online security.

Acknowledgements

We would like to thank Professor Niloufar Salehi, University of California, Berkeley Center for Technology, Society & Policy (CTSP), and University of California, Berkeley Center for Long-Term Cybersecurity (CLTC) for their support and guidance throughout this project. We would also like to thank all the individuals who participated in the interviews and usability testing sessions.

References

1: A. Smith. 2017. What the Public Knows About Cybersecurity. http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/.

2. Alkaldi, N., & Renaud, K. (2016). Why do people adopt, or reject, smartphone password managers?.

3. Wash, R., Rader, E., Berman, R., & Wellmer, Z. (2016). Understanding password choices: How frequently entered passwords are re-used across websites. In Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016) (pp. 175-188).

4. Ur, B., Noma, F., Bees, J., Segreti, S. M., Shay, R., Bauer, L., ... & Cranor, L. F. (2015). " I Added'!'at the End to Make It Secure": Observing Password Creation in the Lab. In Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015) (pp. 123-140).

5. Pearman, S., Thomas, J., Naeini, P. E., Habib, H., Bauer, L., Christin, N., ... & Forget, A. (2017, October). Let's Go in for a Closer Look: Observing Passwords in Their Natural Habitat. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (pp. 295-310). ACM.

6. Kaye, J. J. (2011, May). Self-reported password sharing strategies. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 2619-2622). ACM.

7. Zhang-Kennedy, L., Chiasson, S., & van Oorschot, P. (2016, June). Revisiting password rules: facilitating human management of passwords. In 2016 APWG symposium on electronic crime research (eCrime) (pp. 1-10). IEEE.

8. Park, C. Y., Faklaris, C., Zhao, S., Sciuto, A., Dabbish, L., & Hong, J. (2018). Share and share alike? an exploration of secure behaviors in romantic relationships. In Fourteenth Symposium on Usable Privacy and Security ({SOUPS} 2018) (pp. 83-102).

9. Inglesant, P. G., & Sasse, M. A. (2010). The true cost of unusable password policies: password use in the wild. ACM.

Graphics attribution:
Graphics used in mockups have been designed using resources from Freepik.com