Design challenge and Scoping

- We were hired to create something that would allow customers to perform the activities most important to them when seeking to fulfill specific security needs
- What stuck out from the challenge was that we had to allow customers to do what was most important for them and it had to fulfill a need for security. We started with a braindump in Miro. While grouping the words we noticed that everything we listed required a form of authentication to log in. That is when we decided to focus on account management.

Research and analysis

- Interview guide was designed to get an idea on what concerned potential users cyber security in general. There were 6 interviews completed.
- The next step was to conduct surveys. Survey focused specifically on thoughts about password security. There were 29 in total and it made the assumptions from our interviews solid.
- Patterns began to emerge. Focus was on convenience or security, but never both. For instance people would not write passwords down and memorize them, but used the same password for multiple accounts. While others would use different passwords in accounts, but write them down. Some people even stored them on digital files. Passwords are forgotten and the process to reset them is tedious. All of the people we interviewed didn't trust password auto fill, but did trust biometric scanning. However 5 of the 6 people we interviewed still used autofill
- The next step was to conduct surveys. There were 29 in total and it made the assumptions from our interviews solid
- only a third of our survey participants memorize their password. 45% use a password manager or autofill.
- 66% don't believe autofill is safe, even though it was the most used category for tracking passwords.
- 28 out of 29 respondents believe two-factor authentication makes password security stronger.
- 100% of respondents use cellphones daily and 90% use laptops daily
- "Access to accounts and sensitive information is changing as more finger print, face scanning, and other methods of verification are being utilized. Eventually, passwords may be a thing of the past as methods of encryption improve." - comment really stuck out in the surveys
- From the research and interviews we came up with two personas for potential users. Technical Tommy wants controls of how passwords were stored and used, while still being able to login accounts quickly. Two flaws that stand out regarding the challenge was that passwords weren't effective since he often reuses them and the distrusts of having companies manage/store passwords. Busy Betty believes best practices for security are too time consuming and wants to be able to rely on technology to speed that process up. Finds it inconvenient to have to type in passwords.

Ideation

- Where the project really took shape transformed a focus of password manage into a multi-platform app
- Decided on an app that would manage passwords, but with a twist. Users could combine current biometric 2 factory authentication with logging in if they wish, but a more secure token could also be used. A token would be a picture of whatever the user decided. Could have multiple tokens and require them before logging into any account
- hand drawn sketches will hurt your eyes so we'll save that for the wireframes

Design

- Looked at some current password managing apps. How to log into the accounts would be revolutionary, but didn't want people to feel unfamiliar with the process. Designed sitemap based on this.
- In our user flows we wanted to highlight a user like technical tommy signing up for the app and registering his first token. We believed it would win a user like him over into trusting a password manager since it would show he still has control over his password and can add additional authentication. Two factor seemed to be big with the research we gathered.
- Next was to highlight the convenience. Busy betty is always on the run being able to open the app and quickly be signed into the service she wants answers her frustrations directly
- pictures of wireframes. Tried to mimic password managers and traditional mobile design, since we had 100% cellphone use daily

Validation

- Designed a usability test case to highlight key aspects
- creating a new account, editing/creating tokens, changing account information, change settings, adding a new account
- Turned our wireframe into a working prototype as close to a mobile product as well. Little changes were necessary.
- our usability testing exposed ideas that we thought were good, but were either poorly executed or not intuitive enough for users

Iteration

- Took the feedback of not having confirmation for login and password when registering a new account.
- No toast message appears when making changes in settings
- no save button when making changes to account information
- 50/50 on users identifying the clock. Able to understand that green is good and red is bad, but not sure what the meaning of the clock is.
- Hard for users to navigate to token, needed a more identifiable icon.