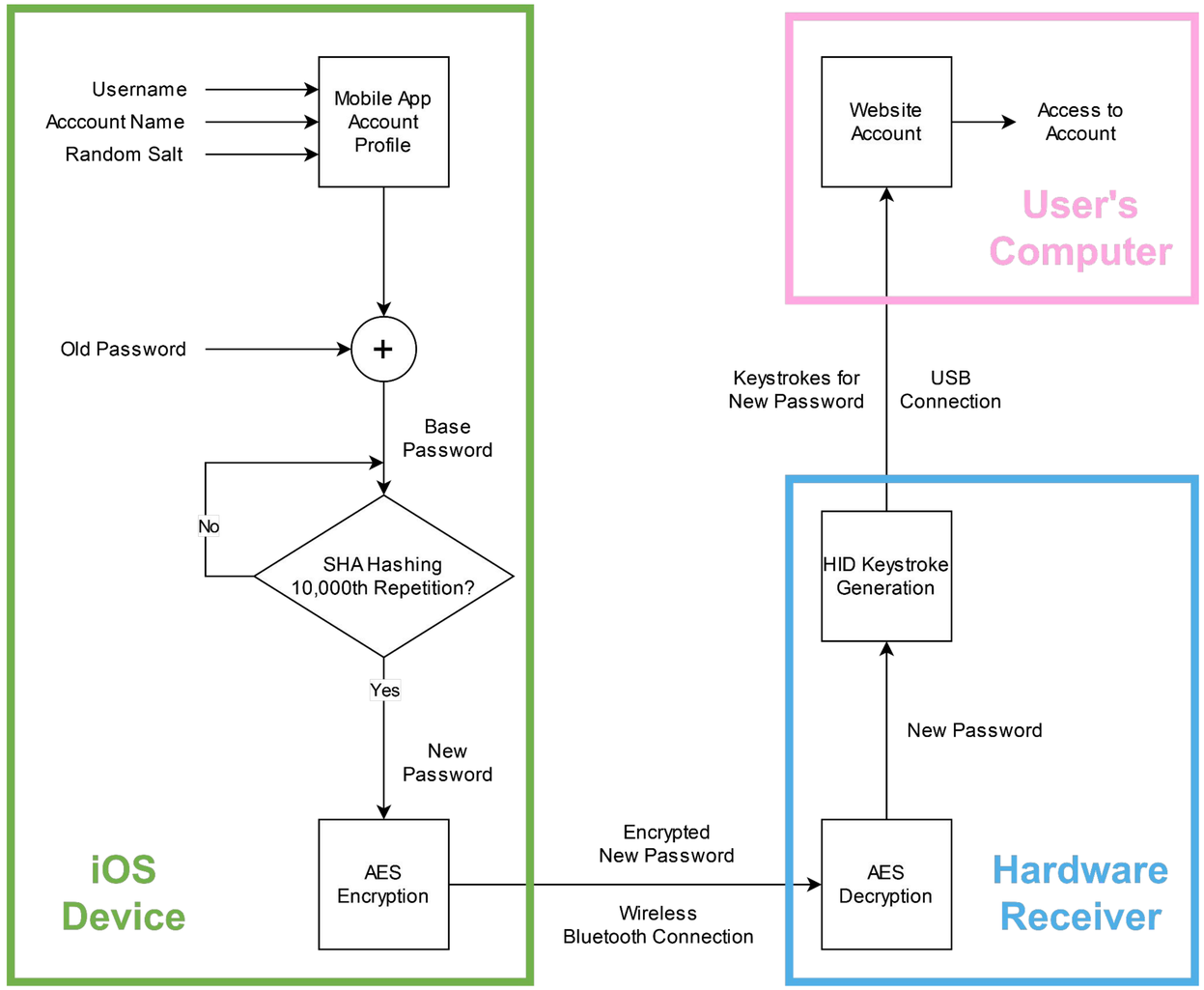
KeYoga Password Generation System

Project

- Many of us use easy-to-remember, but insecure passwords for our online accounts. These can pose risks to our personal data and online safety.
- Two factor authentication (2FA) is inconvenient to use because few 2FA systems are interoperable with all of our online accounts.
- KeYoga uses a simple mobile app paired with a USB receiver that allows users to generate secure passwords on their mobile device and automatically authenticate and populate those passwords into any login screen on their computer.

Methods

- KeYoga's mobile application allows users to store listings for all their online accounts in a single, easy-to-access place. This application stores non-password data which is used in the generation process for new passwords.
- The user types their easy-to-remember password into the mobile app which can then generate a new, more secure password to be used with the user's account.
- This new password is sent via an encrypted Bluetooth connection to a USB receiver which is plugged into the user's computer.
- The USB receiver automatically authenticates and decrypts the new password. The password is then typed into the password field of the user's account on their computer.



Conclusion

- KeYoga provides a simple and quick method for generating and using secure passwords for a wide variety of password-based accounts.
- With further refinement, KeYoga could become a publicly accessible tool for anyone with a mobile device and USB computer to use.
- Developing this project served as an opportunity to learn iOS application development and basic GUI design principles.

College of Engineering
UtahStateUniversity

Hunter Jackson - A02324319@aggies.usu.edu

Thank you to Connetic for contracting this project