CPRE 492 STATUS REPORT #9

February 28, 2020 - March 12, 2020

Group: SDMAY20-52

Project Title: KEY EXCHANGE OUTSIDE OF TCP/IP

Client & Advisor: Julie Rursch

Team Members:

- Logan Woolery — Lead Integrations Engineer
- Jacob Moody — Server Developer Lead
- Joel Wacker — Android Developer
- Andre C — Quality Assurance Tester
- Jack Potter — Client Architecture Tester
- Jordan Svoboda — IOS Developer

Past Week Accomplishments

- Andre- Client-side development
  - Assisted with client side implementation
    - Networking functionality completed
    - Information retrieved from network is stored in local database
  - Started process of creating “beta” version of application
    - Created new branch
    - Started merging functionality into workable version for demo to Client/Advisor
- Jacob-Continued development of backend code
  - Deployed instance of server code
  - Switch from PGP to raw RSA
- Jack
  - Client side development/implementation
    - worked with Joel on QR code interface
    - research on implementing chat interface
  - Client side testing
    - general usability testing
  - Peer review project
    - video voiceover
- Joel
  - Restructured code on implementation branch
  - QR code reader reworked interface
    - Integration with database (scanned codes now can be inserted into database)
  - UI planning for adding contacts

- ➢ Further research on flutter plugins for QR Code generation

- ❖ Jordan-Implementation of client-side encryption
  - ➢ Implemented functions that use our public-private keypair for message signing and verification
  - ➢ Added database to store encrypted messages on the device
  - ➢ Modified chat database by including a column that stores server IP and port
    - ■ This allows us to support user-run servers

- ❖ Logan
  - ➢ Begin final implementation of messaging interface

Pending Issues

- ❖ Design/Rendering of chats needs implemented in Flutter
- ❖ GUI design needs to be improved
- ❖ Development of tests for code (both Client and Server)
- ❖ Message signing method was reevaluated due to Flutter library incompatibility
  - ➢ Changed from using PGP to RSA due to RSA support
  - ➢ Server and client design will be updated to reflect this change

Individual Contributions

Team Member	Contribution	Weekly Hours	Total
Jacob Moody	Development	11	42
Joel Wacker	App Development	14	49
Andre C	App Development	19	70
Jordan Svoboda	iOS development	20	64
Logan Woolery	UI/UX	6	36
Jack Potter	Client R&D	7	35

Plans for Coming Week

- Andre-
  - Continue to integrate functionality for a workable “beta” version
    - Messages sent/received from server are handled properly
    - Database testing and integration for user and message objects
    - Test message storing and retrieval from local database
  - Continue to work with team to finalize database schema for client device

- Jacob-
  - Continue to help debug client/server interaction
  - Improve GoDoc for code
  - continue measuring performance metrics for possible problematic areas

- Jack
  - Permissions issues
    - iOS permissions differ from Android permissions
  - Chat interface work
    - make intuitive, should feel native

- Joel
  - Implement QR Code generation in flutter
    - Have codes generated from keys stored in database
  - Cleanup QR Code reader code
    - Remove unneeded files and merge into beta branch
    - Make the UI more intuitive

- Jordan- Continue client side encryption implementation
  - Integrate messaging signing functionality into our application
  - Database integration and creation for user and message objects
    - Ensure messages are properly stored and created
    - Same with new chats
  - Develop a widget to display messages and allow for message creation
  - Write more thorough tests for the database and cryptography functions

- Logan
  - Finalize messaging flow
  - Finalize Ui/X flow