CPRE 492 STATUS REPORT #8

February 14, 2020 - February 27, 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 almost complete
    - Was able to implement GET functionality in app
- Jacob-Continued development of backend code
  - worked on deploying
  - increase error verbosity
- Jack
  - Client development
    - some cleanup
    - attempted optimization, realized this was premature
  - Continued experimenting with implementation of dart QR code libraries
    - will probably use qr.dart by kevmoo for generation
    - will probably use qr_code_scanner by juliuscanute for scanning
  - Fixed minor android permissions issue
  - Pushed audio research to next week
  - fought android studio build issues

- Joel
  - Application testing on physical Android device
    - Tested on ZTE and OnePlus phones
  - Further hardware permissions fixing
  - Researching QR code generation
  - Planning integration of generated keys into QR codes or audio files

- Jordan-Implementation of client-side encryption
  - Implemented Public-Private key pair generation
  - Worked on implementation of message signing
    - Modelled on PGP message signing (Hash encrypted message to create a digest, sign this and append it to the message)
    - Need to research possible libraries that could handle signing using asymmetric keys
- Logan
  - Begin refining basic ui elements, make it unpainful to use
    - "Make it look like a front end dev at least glanced at it"

Pending Issues

- Implement message signing in Flutter
- Design/Rendering of chats needs implemented in Flutter
- GUI design needs to be improved
- Development of tests for code (both Client and Server)

Individual Contributions

Team Member	Contribution	Weekly Hours	Total
Jacob Moody	Development	12	31
Joel Wacker	App Development	18	35
Andre C	Client side functions	18	51
Jordan Svoboda	iOS development	14	44
Logan Woolery	Testing	12	30
Jack Potter	Client R&D	11	28

Plans for Coming Week

- Andre-
  - Finish development of client-side networking
  - Test networking for connectivity issues
    - Test error handling
    - Handle exceptions/errors that server might issue to client
  - Work with Jordan for storing data retrieved from server
- Jacob-
  - Help debug client / server interaction
  - Improve GoDoc for code
  - continue measuring performance metrics for possible problematic areas
- Jack
  - Finish QR implementation
    - squash bugs
  - Investigate alternative channels of communication
    - Audio via 3.5mm jack
    - NFC
- Joel
  - Finish QR implementation
  - Begin work on other hardware communication
    - Audio
    - NFC
- Jordan- Continue client side encryption implementation
  - Write more thorough tests for the database and cryptography functions
  - Add a column to the database that stores the path to the file containing the messages in the related chat
    - This will allow for easy modification (like addition of new messages) and easy deletion of chats that are no longer needed/readable due to key changes
  - Continue implementation of message signing
- Logan
  - Restructure FE to be useable
  - Work with testers to figure out UX designs