CPRE 492 STATUS REPORT #7

January 13, 2020 - January 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 Testing
- Jack Potter — Client Architecture Tester
- Jordan Svoboda — IOS Developer

Past Week Accomplishments

- Andre- Continued testing components
  - Began creating tests for server
  - Got Flutter installed and running on Macbook for client testing

- Jacob-Continued development of backend code
  - Fixed failed unit tests

- Jack
  - Researched proposed “double encryption”
    - Symmetric key does serious encryption
    - Private key also used for second layer of encryption
    - Thwart known-plaintext attacks
    - Prepared for group presentation

- Joel
  - Research into Android and iOS hardware permissions with flutter
    - Finding how to ask for access to Bluetooth, Camera, Microphone, etc.
  - Breaking code into multiple files
    - Each page of the app should be a file
    - Organize for group editing and pull requests

- Jordan-Implementation of client-side encryption
  - Implemented code for reading and writing to a file on the client device (for storing keys locally)
    - Able to write text to a file, store it through reboot and then read that text back
    - Fairly barebones, will need some modifications and testing for actual usage
  - Researched and started implementing a cryptography library
    - Worked with the steel_crypt library
    - Found functions for symmetric key generation and encryption/decryption with those keys

- Logan
  - Research into UI/UX in flutter

Pending Issues

- Continue getting code merged into Git repository
- Need to find a way to implement PGP keys in Flutter
- GUI design needs to be improved
- Encryption needs to be implemented on client side

Individual Contributions

Team Member	Contribution	Weekly Hours	Total
Jacob Moody	Team Meetings Development	11	91
Joel Wacker	App Development Presentation	7	86
Andre C	Team Meetings Testing	7	90
Jordan Svoboda	Team Meetings iOS development	10	93
Logan Woolery	Team Meetings Testing	8	88
Jack Potter	Research	7	90

	Team meetings		

Plans for Coming Week

- Andre-
  - Continue development of test cases for server
  - Get Flutter code installed on Android and IOS for usability/compatibility testing
- Jacob-
  - Fix unit test fails
  - Continue work on final project

- Jack
  - Assist Joel with QR Code implementation and testing
- Joel
  - Further server integration from client side
    - Testing API Post requests
  - Seperate application out more, and delegate work as needed

- Jordan- Continue client side encryption implementation
  - Finish implementing symmetric key generation and encryption/decryption
    - Make sure we can store a generated key and ciphertext
    - Make sure that a key will encrypt and decrypt correctly
    - Test this code to make sure it is secure
  - Find a way to implement PGP keys into our application for authenticating with the server and message integrity verification
    - No libraries for this in Flutter, so I need to do some research on this

- Logan
  - Begin UI implementation