Research plan

Introduction

This semester for my individual project I have decided to create an end to end encrypted (E2EE) messaging platform for both groups and one on one communication. I think this project is a good fit for this ‘Complex software systems’ semester, as I think implementing this well is quite complex, with all of the micro services which will be required. Last semester I had a course regarding cryptography and I learnt a lot of the base principles that would be required to implement this project, such as public key cryptography with Diffie Hellman, as well symmetric cryptography using ciphers like AES. This inspired me to do this project, as I am not sure how these principles would extend from one to one communication to group chats, and that will be my main subject of research.

Problem/Opportunity

Secure communication has become a critical requirement for both individuals and enterprises in an era of increasing cyber threats, surveillance concerns, and data breaches. While end-to-end encryption (E2EE) is well-established for one-to-one communication, extending this security guarantee to group chats presents unique challenges in scalability, key management, and usability. Understanding how E2EE can be effectively implemented in both one-to-one and group contexts is essential for the success of my individual project.

Main research question

How can an end-to-end encryption protocol be designed and implemented that enables users using modern communication platforms to securely exchange messages in both one-to-one and group chats with high scalability, usability, and forward secrecy?

Sub-questions:

1. How do established platforms (Signal, WhatsApp, Matrix) currently solve these design challenges, and what best practices can be adapted for a new secure

messaging platform?

2. How can cryptographic protocols be selected or designed to ensure forward secrecy and reliability for individual users in one-to-one chats?
3. How can group key management mechanisms be structured to enable multi-device users in group messaging contexts to exchange messages efficiently with scalability up to thousands of participants?
4. How can synchronization and device migration processes be designed so users can maintain secure communications across multiple devices while minimizing usability challenges?
5. Which trade-offs between encryption overhead and responsiveness in large group chats are acceptable to ensure smooth real-time communication at scale?

Research methods

Question	Methods	Strategies
How can cryptographic protocols be selected or designed to ensure forward secrecy and reliability for individual users in one-to-one chats?	Library, Workshop	Best good and bad practices, Literature study, Design Pattern research, Prototype
How can group key management mechanisms be structured to enable multi-device users in group messaging contexts to exchange messages efficiently with scalability up to thousands of participants?	Library, Workshop, Field	Best good and bad practices, Literature study, Design Pattern research, Prototype, Problem analysis
How can synchronization and device migration processes be designed so users can maintain secure communications across multiple devices while	Library, Field	Best good and bad practices, Literature study, Design Pattern research, Problem analysis

minimizing usability challenges?		
Which trade-offs between encryption overhead and responsiveness in large group chats are acceptable to ensure smooth real-time communication at scale?	Field, Workshop	Problem analysis, Prototyping
How do established platforms (Signal, WhatsApp, Matrix) currently solve these design challenges, and what best practices can be adapted for a new secure messaging platform?	Library	Literature study, Available product analysis

This research follows the DOT framework by combining library (e.g literature review), workshop (e.g Prototype), and field (e.g Problem analysis) strategies. This mixed approach is chosen to ensure both theoretical depth and practical applicability. The results are intended to directly inform my individual project’s technical design while also providing broader insights into secure communication - a skillset highly relevant for enterprise software development.