End-to-End encrypted Java chat application

Background

In today's digital age, where more and more people have become connected to the internet, ensuring the security and privacy of communications has become paramount. With the increasing prevalence of cyber threats and privacy concerns, there is a growing demand for secure messaging solutions that offer end-to-end encryption. End-to-end encryption ensures that only the intended recipients can access the contents of the messages, protecting them from interception or eavesdropping by unauthorized parties, including service providers and malicious actors.

The goal of the project

The goal of this project is to develop an end-to-end encrypted Java Chat application that provides users with a secure platform for communication. By leveraging cryptographic APIs available in Java, we aim to implement robust encryption mechanisms to safeguard the confidentiality of messages exchanged between users.

Relevance to language-based security

Language-based security focuses on using programming languages and their features to enhance the security of software systems. In the context of this project, Java provides a rich set of cryptographic APIs and features that enable developers to implement secure communication protocols and encryption mechanisms. By leveraging these language-specific security features, we can ensure that our chat application is resilient to common security vulnerabilities and attacks, such as eavesdropping.

Overview of the planned work

The chat application is already implemented as a separate project(see https://github.com/ksedix/Java-Client-Server-Chat). The work will consist of utilizing Java cryptographic API's to enhance the security aspect of the chat application and implement end-to-end encryption to make it secure.

Schedule

Week 1-2: Integration of cryptographic APIs for end-to-end encryption.

Week 3-4: Implementation of user authentication and key exchange mechanisms.

Week 5-6: Development of message transmission and decryption functionalities.

Week 7-8: Testing, validation, and documentation of the chat application.

Our target grade is 5. By creating a comprehensive end-product that can be used in real-life for secure communication, we think the value of such a product deserves this grade.