UNIVERSITY OF BIRMINGHAM

School of Computer Science
College of Computer Science FT

MSc. Project

Secure E2EE Chat System Based on Signal Protocol

Submitted in conformity with the requirements
for the degree of MSc. Computer Science
School of Computer Science
University of Birmingham

Ziyan Wang
Student ID: 2014988
Supervisor: Dr Mihai Ordean

September 2020

Declaration

The material contained within this report has not previously been submitted for a degree at the University of Birmingham or any other university. The research reported within this report has been conducted by the author unless indicated otherwise.

Signed ....

Ziyan Wang

MSc. Project
Secure E2EE Chat System

Ziyan Wang

Contents

Table of Abbreviations

- 3DES – Triple DES
- 3G – Third Generation

1 Overview

This paper is about upgrading a chat system using Signal Protocol to implement a secure end-to-end-encryption chat system. This report focus on having a brief introduction about Signal Protocol and describing how to implementing a Signal Protocol based end-to-end-encryption system including on client, server and database sides. The existing chat system is developed by myself previously using gradle6 and jdk11. To improve the security of the communication, the project using Signal Protocol to encrypt the messages including on client, server and database sides.

1.1 Abstract

As people's awareness of safety increases, normal symmetric encryption and asymmetric encryption like TLS, AES cannot satisfy their needs: even though the security of transmission can be guaranteed, the server still needs to decrypt the encrypted messages. So once the malicious people use it to get users' sensitive information on server side, users' privacy will be leaked. Besides, the normal symmetric and asymmetric encryptions keep using the same cipher key during the transmission, once the hacker cracks one encrypted package, the previous and future encrypted packages will be exposed immediately.

In this situation, the Signal Protocol is developed to solve this problem. It implement an end-to-end-encryption protocol to make sure only the call parties can decrypt the encrypted messages, and the cipher key will be changed in each transmission round which can not be referred forward or backward. The server does not decrypt the messages but only forwards the packages to the right users and the database also does not store the decrypted messages from users which greatly reduce the risk of user privacy leakage.

This report describes the fundamental of Signal Protocol and the whole process of implementing it on a existing chat system including on client, server and database sides. On client side, users' communication messages are encrypted by Signal Protocol, only the receiver and other essential information are exposed to the outside. On server side, the server handle the received packages corresponds to their type and only forward the encrypted messages to the corresponding users. Server does not use the libsignal-protocol-java packages which can guarantee the server cannot decrypt the messages. On database side, it only stores users' public keys for other users initializing the pairwise chat, so once the database is breached, there is no damage caused to users.

At the end, the project implements an end-to-end-encryption chat system including pairwise chat, group chat, local history messages storage, multi-device system and message backup functions etc.

Keywords: Signal Protocol, end-to-end-encryption, chat system

1.2 Acknowledgements

The success of the project cannot be separated from the help of many people and papers.

First I need to appreciate my Project Supervisor, Mihai Ordean, we have a detailed meeting every week. After each meeting, I can find new directions and questions. Also it's his progress to let me set this subject which I have never touched before.

I also need to thanks my friends, who have given me a lot of advice about this project and listened to my new ideas and my own explains to the project.

Finally, I need to appreciate my family, they spend endless hours to support my project by helping me find the related papers and test the project's robustness which is significant to the development of the project.

2 Introduction

2.1 Overview

The aim of the work described in this Report is to improve the security of a chat system based on Signal Protocol which people can be not worried about their privacy leakage.

2.2 Problem statement

Under the rapid development of the information age, the encryption protocol also have a new revolution. At the beginning, people transmit the messages in plain text which is a original way and information can be obtained easily. So symmetric encryptions born in this situation. The call parties need to negotiate a common cipher key to encrypt the messages during communication. Although the symmetric encryption is quite difficult to crack. But the benefits of cracking are huge. So maybe the hacker will monitor on several days' packages and spend some times to crack the encrypted messages to get the cipher key. And then the he can decrypt any other messages before or after without the knowledge of both parties. Besides, the common cipher key's exchange is also a problem, call parties need to negotiate it via a safe way such as face to face or the cipher key can be obtained by malicious people.

To solve the symmetric encryption's key exchange problem, asymmetric encryption is developed. The server and client will use some asymmetric algorithms to obtain the future common symmetric cipher key. The progress is the security of transmission is improved, the hacker cannot get the common symmetric cipher key easily while two parties are exchanging it. However, the problem mentioned before is still not solved: once the hacker cracks one of the packages, all the packages are exposed to the hacker which will cause unpredictable losses. Besides, the credit of server is also a problem. Usually the call parties are client and server, server decrypt encrypted messages from clients and then forward them to the corresponding users or store them in database. Which means, some unethical companies may sell users' chat history or the hackers can focus on attacking the database to get the information, both of them can have serious consequences.

In this situation, the public needs a new protocol to protect their privacy. Whisper is a good inspiration to develop a new protocol. Only the two parties of communication know what they are talking about. The server are only responsible for forwarding users' messages but not decrypting them. Also, the server does not store the decrypted even encrypted messages in database to make sure the security of users' privacy is guaranteed by users themselves. That is the original purpose of Signal Protocol. It not only combines the symmetric and asymmetric encryption, but also adds a new algorithm to provide forward and future security: Double Ratchet.

2.3 Project aim

This project is aim to implement an E2EE chat system using Signal Protocol which can improve the communication security of it. The project does not only develop an E2EE chat program, it focuses on a whole E2EE chat system including server, client, database sides.

2.4 Project structure

The existing chat system is developed by jdk11 and gradle6. It can be divided into three parts: client, server and database. The client is developed using javafx11, it uses MVC architecture to link the data and view. In transmission aspect, it uses socket programming to communicate with server. The communication package has a specific format: each package has a type, both client and server will handle the package corresponding to each type.

On server side, it connects to the bham's database via bham's SSH service. The database uses PostgresSQL database which served by bham.

The project's main work is on client side where the Signal Protocol encrypt the chat messages of user. The client implements several functions such as pairwise chat, group chat, chat history storage and history messages backup etc. On server side, most of the work is about how to handle the packages from client. For example, server needs to response to users' key bundle requests and forwards the packages to the right users. In database, it simplify the structure of tables, because there is no need to store the chat data in database. But some creation and modification are needed to achieve a Signal compatible system like create a new table to store users' key bundles, add deviceId field in users table to implement a multi-device system.

2.5 Outline of each section

In the next set of sections, the report introduce the further related knowledges and the specific implementation and the final result of the system.

In chapter 3, the report introduce some further background materials that reader needs to know to understand the solution. It focuses on how Signal Protocol works and the context of related existing work.

In chapter 4, the report describes the user specification of system, main design of solution and concrete implementation of upgrading the chat system using Signal Protocol including client, server, database sides. It also shows how the project and the writing of a substantial piece of software is managed. Finally, the report presents the whole implemented system's usage result to discuss its success and robustness.

In chapter 5, the report summarise the achievements and the deficiencies of the project. The things that could or would have done are listed for further evaluation.

In chapter 6, the report give a brief statement of how the solution addresses the problem stated at the beginning and provide an evaluative statement based on the results.

In chapter 7, the report explains the file structure of the code and introduces how to run the project code in detail. The proposal and schedules are also presented in this chapter.