A secure client-server mobile chat application implementing elliptic curve integrated encryption system (ECIES) and other security features.

Daniel Furnivall

School of Computing Science
Sir Alwyn Williams Building
University of Glasgow
G12 8QQ

A dissertation presented in part fulfilment of the requirements of the Degree of Master of Science at The University of Glasgow

1st April 2022

Abstract

abstract goes here

Education Use Consent

I hereby give my permission for this project to be shown to other University of Glasgow students and to be distributed in an electronic format. **Please note that you are under no obligation to sign this declaration, but doing so would help future students.**

Name: ______________________ Signature: ________________________

Acknowledgements

acknowledgements go here

Contents

Chapter 1: Introduction

Secure messaging apps intro

1.1 Why are secure chat applications needed?

1.1.1 Family & friends

1.1.2 Whistleblowers & journalists

1.1.3 Political dissidents

1.1.4 Crime

1.1.5 Data security

1.2 Existing applications in this field

1.2.1 Telegram

1.2.2 Whatsapp

1.2.3 Signal

1.3 Issues

1.3.1 Closed source

1.3.2 Tradeoffs between security and usability features

1.3.3 Nation state control

Chapter 2: Analysis/Requirements

Chapter 3: Design & Implementation

3.1 Tools Used

There are two primary components to the overall system - one or more clients applications which communicate with a central server.

3.1.1 Client

The final client application was written entirely in Kotlin (v1.6.10) using the Android Studio IDE.

BouncyCastle

Room ORM

3.1.2 Server

3.1.3 Report

This dissertation was written entirely using Vim with the VimTex plugin.

3.2 Encryption Implementation

3.2.1 Asymmetric component

3.2.2 Symmetric component

3.2.3 Difficulties

3.2.4 Storage of encryption keypair

3.3 Persistence and storage considerations

3.3.1 Storage of self-destruct duration

3.3.2 Existing user persistence and reconnection flow

3.4

3.5

Chapter 4: Evaluation & Testing

Chapter 5: Conclusion

Appendix A: First appendix

A.1 Section of first appendix

Appendix B: Second appendix

Bibliography