Incognito : Secure Chat

Scrypt Miners

February 11, 2017

Suyash Deshmukh (016105854)
Samruddhi Kalyankar (016110365)

1 Motivation

In modern era, a lot of information is passed through many insecure communication channels and monitored proprietary servers. This information can be used against the communicating parties if acquired by adversaries present in the network. Hence, it is important to provide an end to end secure messaging application for exchange of sensitive information by implementing various security techniques.

2 Problem Statement

1. The information exchange happens via an untrusted server hence the information should be encrypted.
2. The encrypted information should be readable only by the intended receiver.
3. Any kind of passive or active attack to this communication should not be allowed.
4. Authentication process must be provided between communicating entities so as to ensure that they are communicating with the intended person.
5. Key exchange process should be secure, reliable and seamless.

3 Proposed Solution and Approach

3.1 Proposed Solution

A proposed solution to a secure chat application is as follows:

- Basic features like sign up to create a new account and sign in for the existing users.
- Sign up process will require a email confirmation to create a new account.
- Main features like Encrypted One-to-one Chat and Group Chat.
- Authentication of communicating users.

3.2 Approach

An approach to our proposed solution will be as follows:

- Key Exchange mechanism through communication channel using Diffie–Hellman key exchange protocol (or similar).
- Message encryption for end-to-end encryption using standards like AES or similar.
- Encryption of messages in Group chat using RSA (or similar).

4 Implementation Details

This chat application requires implementation of mobile application and a web server.

- Programming Languages:
  Client Side: Android Platform for mobile application
  Server Side: PHP

- Framework:
  For server side implementation, we will be using a suitable and well established PHP framework.

- Hardware Requirements:
  Secure HTTPS server for LAMP server stack.

5 Project Timelines and Workload Distribution

First two weeks of the project will be utilized to perform documentation and analyze the problem. We will be identifying the use cases and attack surfaces to implement better security measures. The project workload has been distributed equally so that each individual will get to implement important security features of the application.

5.1 Suyash Deshmukh

1. Documentation - One to One Chat :
   Design documentation for functional as well as non functional requirements of One to One Chat.

2. Login & Register Module : (1 Week)
   Module to register new users with their email addresses and provide access to existing users.

3. Encryption - One to One Chat : (3 Weeks)
   End to end message encryption in One to one chat module.

4. Key Exchange Group Chat : (3 Weeks)
   To perform key exchange on untrusted communication channel.

5. Message Exchange - Group chat : (3 Weeks)
   Sending and receiving of messages between group members in group chat module.

5.2 Samruddhi Kalyankar

1. Documentation - Login, Register & Group Chat :
   Design documentation for functional as well as non functional requirements of Login, Register & Group Chat.

2. Key Exchange - One to One Chat : (3 Weeks)
   Implementation of Diffie-Hellman or similar key exchange algorithm.

3. Message Exchange - One to One Chat : (3 Weeks)
   Sending and receiving of messages between two communicating entities.

4. Create Groups - Group chat : (1 Week)
   Module to create, edit and delete groups for group chat feature.

5. Encryption - Group chat : (3 Weeks)
   Encrypted messages to be transferred to each member of the group chat.

Last week in the project timeline will be completely dedicated for testing purpose.