End-to-End Secure Chat Application

Crypto Ninja

February 10, 2017

Bandini Bhopi (CSULB ID: 016130983)
Brin Pereira (CSULB ID: 016134272)

1 Motivation

Internet and mobile communication (Smartphones) have reshaped our view and experience of the world around us. With the increased in the use of online services, concerns about security and privacy is becoming important. Unfortunately, majority of the online applications are vulnerable to malicious attacks. For example, chat applications offer different services and built-in features to their users while in majority of the cases, they neglect security aspects of their usages and messages. Our Project aims at building secure chat application which will allow us to safely exchange private information by ensuring Confidentiality, Integrity and Availability.

2 Problem Statement

The project is to create secure chat application which will focus on below features:

1. Only the intended recipient should have access to the messages.
2. The data should be protected from the damage, eavesdropping while it is transmitted and stored.
3. For improved and strong protection, encryption key is stored locally.

3 Proposed Solution

We proposed a standalone chat application for secure messaging. Application will include one-to-one chat which will be encrypted. Basic features include registration and login. Email / phone confirmation will be needed to complete the registration. Encryption key will be stored locally. Individual users have a mechanism to authenticate each other, assuring themselves they are communicating with the right person.

4 Approach

We will address above mentioned issues in following way:

- End-to-End Encryption text messaging using AES or similar.
- Secure Key Exchange using Diffie–Hellman or similar.

5 Implementation Details

- Server Side Implementation

  We will use PHP for server side coding. The chat server will host on LAMP stack.

- Client Side Implementation

  We will use Android for client side coding.

6 Project Time-line & workload distribution

6.1 Bandini Bhopi

- Login, Registration, End-to-End Encryption – Documentation (1 Week)

  Documentation including necessary diagrams like Use-cases, Flow-chart, attack tree etc.

- Key Exchange (2 Week)

  Secure Key exchange process assuming untrusted connection.

- Encryption (1.5 Week)

  Encryption of the message being transmitted by the sender.

- Decryption (1.5 Week)

  Decryption of the message being received by the receiver.

- Testing of Local chat storage protection and U2U authentication (2 Week)
- Bug fixing (1 Week)

6.2 Brin Pereira

- Local chat storage protection – Documentation (1 Week)

  Documentation will include all important diagrams for implementing one-to-one chats.

- Login and Registration - Implementation (2 week)

  Implementation of login and registration page and also including Email or SMS confirmation

- Design and develop GUI of chat application (2 week)

  Designing user-friendly GUI using Android.

- User-to-User Authentication (2 Week)

  Implementation of user-to-user authentication to check whether the intended recipients is the right person.

- Testing of Login, Registration and End-to-End Secure chat.
- Bug Fixing (1 Week)