Corporate Secure Chat (End-to-end chat application)

Team - Digital Chaos

September 14, 2016

Gaurav R.Bhor (014872960)
Divya Dudagonda (014849989)

1 Motivation

Companies are always concerned about the privacy of its affairs. Valuable information, if leaked may cause a catastrophic loss to the company; not just in terms of profit but also in terms of reputation. Hence, it is imperative to secure all possible modes of communication inside the company.

2 Problem Statement

Major concerns in this application are:

- Communication in the application needs to be secure.
- When a message is sent, only the intended receiver should be able to read it.
- Eavesdropping or altering of messages should not be allowed.

3 Proposed Solution

We propose a standalone chat application which will be used by the employees of the company i.e. having emails ending in *company.com*. The application will include one-to-one and group chat which will be encrypted. Basic features like registration and login will also be included. Email confirmation will be needed to complete the registration process.

4 Approach

How are we addressing the issues?

- We propose to implement end-to-end encryption. This will be done using a AES or similar
- Exchange of public keys through an unsecured channel. This will be done using Diffie Hellman (or similar).
- Message sending and receiving in group chat using client-side fan out.
- Encryption of group chat messages will be done using RSA (or similar).

5 Implementation Details

- Programming Language:

  PHP for server side coding and Android for client side coding.
- Framework:

  We will most likely use a PHP framework to minimize the amount of boilerplate code.

- Hardware Requirement:

  A simple HTTPS Server which will host the LAMP server stack.

6 Project Time-line and Work Distribution

6.1 Gaurav Bhor

- Login, Register and Group chat - Documentation

  Documentation including necessary functional and non-functional diagrams for implementing Login, Register and Group chat modules. The documentation will be updated on a regular basis as the project progresses.

- Login and Register (2-4 days)

  Creating Login and Registration modules for the employees of the organization.

- Group chat: Creating groups, sending and receiving messages (3 weeks)

  Basic message exchange between members of the group. We will follow a client-side fan out mechanism.

- Group chat: Key Exchange (3 weeks)

  Exchanging keys securely on an non-trusted connection.

- Group chat: Encryption (3 weeks)

  End to end encryption of messages being transmitted to each group member. We will be implementing a public key encryption algorithm like RSA (or similar).

6.2 Divya Dudagonda

- One-to-one chat - Documentation

  Documentation including necessary functional and non-functional diagrams for implementing One-to-one chat and all modules involved. The documentation will be updated on a regular basis as the project progresses.

- One-to-one chat: Sending and receiving messages (3 weeks)

  Exchange of messages between two users.

- One-to-one chat: Key Exchange (3 weeks)

  Exchanging keys securely on an non-trusted connection. We will be implementing Diffie Hellman (or similar) to achieve this.

- One-to-one chat: Encryption (3 weeks)

  End to end encryption of the messages being transmitted in one-to-one chat.

We dedicate the first two weeks for documentation and research. We plan to complete the project by the third week of November. The last week of November will be completely dedicated for testing and debugging.