Design Document

Kripanand Jha & Vinuth Chandra S

October 3, 2016

Abstract

This document gives an overview of the **assets** and how the "Keyloggers Chatbox" application is designed to protect these assets against various attacks at different levels. It provides a step by step flow as to how users will be authorized and authenticated.

Goals

- User Authentication
- Message Integrity
- Message Confidentiality

Assumptions

1. The SSL being used is trusted

Database Design

System Design

Chatbox would have one server which would be the main point of contact for all authorized users. Users have to first register themselves in order to start using the application. The application will ask the user to enter a name, phone number and email ID. Once this information is available, two distinct codes will be sent to the user, one via a text message and the other by email. The user has to enter both these codes in order to authenticate himself. Once authentication is complete, the user will be prompted to set a password and he/she can log in with their phone number and their password. The application will also prompt the user to change the password every two months. A "Forgot Password" option will be provided for the user once this button is clicked, the authentication process will be re-triggered. Figure 1 shows the handshake between the client and server for authentication.
To provide confidentiality and integrity of the message being transferred to the server should be protected from external and internal eavesdroppers. The message received to the server should be encrypted and stored along with the details of the sender and receiver. The message should be decrypted correctly and sent to the correct receiver.

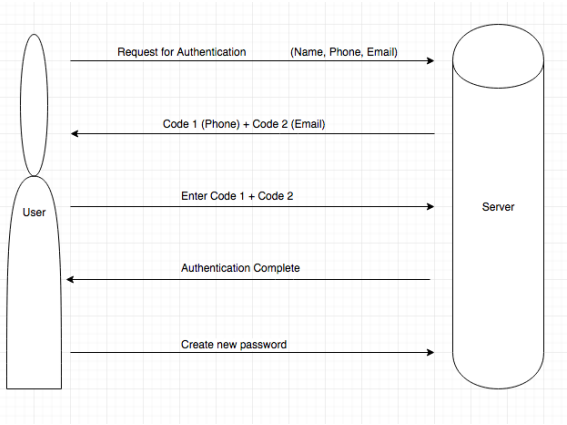

Figure 1: User Authentication .

Figure 2: Application .