600.442 Cryptography and Network Security Final Project

Secure Internet Chat Room

Lei Shen

Summer, 2000

This project aimed to develop a java-based internet chat program that will allow several parties to securely talk over the internet. This program will have several applicable uses such as allowing several trusted parties to exchange sensitive information over the internet. The program involves a server part and a client part. The following is some specific steps about how you can run these programs:

1. First you run the server program, when it starts, it generate a fresh triple-DES key and begin listening.

2. You start the client-side program. There are two versions, one is an applet that you run in your browser, another is a normal java application that you run in command line. You need to have Sun's Java Cryptography Extension (SunJCE) package installed on your computer and SunJCE installed as a security provider in your java.security file in order to run the program. This is because the program uses symmetric ciphers. The program first go through a secure password login process, with a mechanism as follows: it first ask you for your login name and password, and generates a fresh time-stamp and random number. It then creates a message digest of the four parameters (login, password, time-stamp and random number). It sends the server the login, time-stamp, random number and the message digest in the clear. The server then use the login to look through its database to find the password, and make another message digest using the received login, time-stamp, random number and the looked-up password. The server compare the two message digests, if they are the same, the client has successfully logged in. In this way the client doesn't send the password in clear form over the internet, which will prevent evansdropping. Also this login is session specific because of the time-stamp and random number, which can prevent a "replay" attack.

3. After successful login the server send the triple-DES key it generated, password encrypted using the client's password, to the client. Since every client will receive the same key, they will communicate using that key. More specifically, when a client types some chat message, it will be encrypted using the triple-DES key and send to the server, the server then broadcast the message to every client current logged in without decrypting it, and every client receiving that message will decrypt it using the same key.

Source codes of the project:

- **1. ChatServer.java (main server program)**
- **2. ChatApplet.java (client side program, a java applet)**
- **3. CheckValidity.java (server side program for secure password login)**
- **4. Broadcaster.java (server side program to broadcast chat messages)**
- **5. ReaderThread.java (server side program to listen to new chat message)**
- **6. WriterThread.java (server side program to write broadcasted messages)**
- **7. CloseWindowAndExit.java (server side program for event handling)**
- **8. ChatApplet.java (alternative server side program: a java application)**
- **9. chat.html (webpage to initiate the applet)**