**FILE TRANSFER PROJECT DOCUMENTATION**

By

BAO NGUYEN – BCN140030

MOFAN LI – MXL162930

CS 6349.001

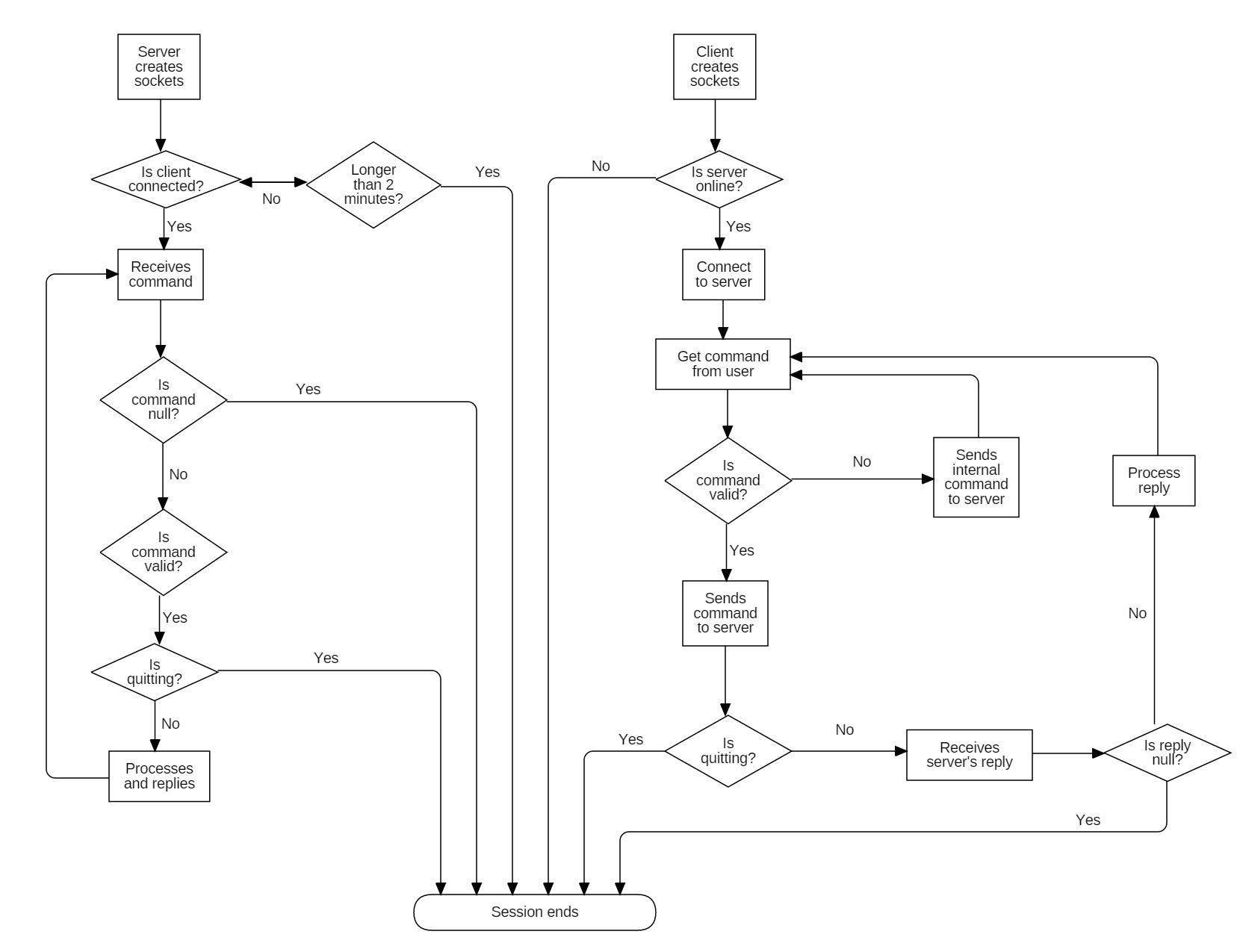
1. **Project description and solution**

The problem is to create a file transfer system that utilizes Socket Programming, Connection Management, Reliable Communication, and security protocol that utilizes SHA-1. It allows 2 individuals (1 server and 1 client) on different computers to communicate via network. This project supports Windows, Mac, and Linux.

We use Java to build this program. We create 2 different projects, a *Client.java* and a *Server.java*. The server sets up the sockets and wait for connection. The client sets up its socket and connect to the server. This program also records the start and end time of the session.

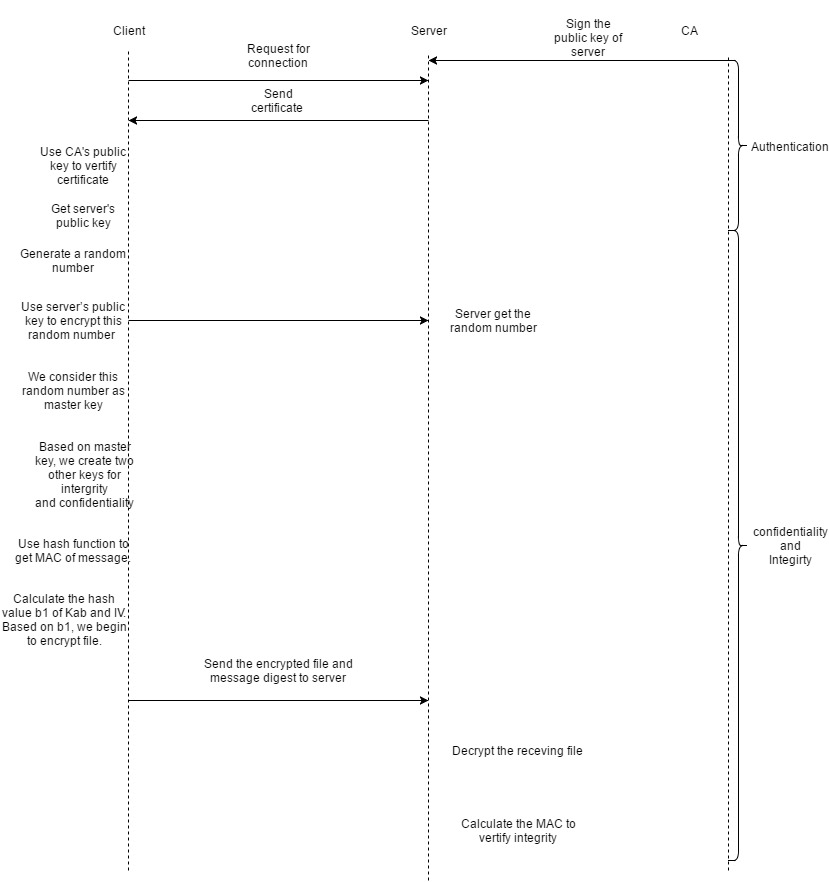
There are several commands that allows the client to communicate to the server. The server does not initiate any message. It waits for the commands from the client and sends responses. The client can request server to view all the files the server contains, to download files from the server, or to upload files from local host to store in the server. All messages transported over the network shall be secured with respect to Authentication, Confidentiality, and Integrity.

There are several occurrences when the program ends (the flow of the program is provided in the next section of this report):

1. If the server waits too long without any connection from the client, the program ends at that point.
2. If the client tries to establish a connection without an active server (on the other word, the client starts before the server does), the program ends immediately.
3. After the connection is established, they can continue communicating (the client starts first) until the client says “quit”. When this event occurs, all sockets are closed and the program ends.
4. During the session, if either the server or the client goes offline for any reason (indicating by a null message received by the other party), the one who remains online displays an error message to the screen to indicate the event and the session ends safely (without crash).
5. **Implementation**
   1. *Abstract Flow chart*

*Basic flow of program. Authentication mechanism will be added as separated diagram.*

* 1. *Security Protocol*

**

1. **Code executions**
   1. *Compile and Run*

There are two ways to run the system: via IDE or via Command Line environment.

To run program via IDE (this was developed via IntelliJ IDEA from Jetbrains), first open project FileTransferApplication. Then, individually run Server module and Client module. From this step just simply follow the prompt.

To run program in the command line environment, first navigate to where the Server folder and the Client folder located on your local machine. In each module, navigate to the src folder. Run command “javac Server.java” for Server and “javac Client.java” for Client to compile the code. Then run “java Server” to start the Server and “java Client” to run the Client. After this, run as program instructs.

1. **Detail about security protocol**
   1. *Authentication*

Server has a certificate which is its public key signed by CA’s private key. The client has CA’s public key. When server receiving the connection request from client, server will send the certificate to client. Client uses CA’s public key to verify the certificate and get server’s public key. After authentication, client generates a random number. We consider this random number as a master key.

Encrypt master key with server’s public key and send it to server.

* 1. *Confidentiality*

In this project, we use Sha1 to encrypt our files which is generating and using one-time pass to XOR with data.

b1 =Sha1(Kab|IV) c1=p1⊕b1

b2 =Sha1(Kab|c1) c2=p2⊕b2

… …

bi =Sha1(Kab|ci-1) ci=pi⊕bi

* 1. *Integrity*

We also use Sha1 to calculate the MAC(Message authentication codes).

MAC =SHA1(Kab|m)

1. **Threat model**
   1. *Eavesdrop*

Even if attacker can watch the message between client and server pass over the network, the attacker still can’t learn the contents of message between client and server.

* 1. *Initiate a conversation pretending to be Client*

The project has one-way authentication, so it can’t verify the client.

* 1. *Lie in wait at Server’s network address and accept a connection from Client*

The server will use certificate signed by CA to verify itself.

* 1. *Read Server’s database*

The attacker can get server’s private key to decrypt the master key from client.

* 1. *Man-in-the-Middle Attack*

The attacker can’t get useful information if he doesn’t know server’s private key or master key.

1. **Issues and Solutions**