BAO NGUYEN – BCN140030

MOFAN LI – MXL162930

CS 6349.001

**FILE TRANSFER PROJECT DOCUMENTATION**

**I. Project Description and Features**

*1. Description*

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 on different computers to communicate via network. All messages transported over the network shall be secured with respect to Authentication, Confidentiality, and Integrity.

*2. Features*

We use Java to build this program. There are 3 main modules (Commons, Client, Server), all lie within the *FileTransferApplication* project (\*). 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. This project supports Windows, Mac, and Linux.

The server does not initiate any message. It waits for the commands from the client and sends responses. The client is able to view the files it contains, to 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.

(\*) Please read the included *READ\_ME.txt* file for more information about program configuration and execution.

**II. Security Protocol**

*1. Authentication*

Authentication mechanism utilizes both Public Key Crypto and Secret Key Crypto. Details as follow:

Client:

Session 0:

Request CA Certificate to verify if valid Server

Create unique ID based on its creation time.

Create random secret character set for AES

Create random initial master key R.

Create encryption key E = R + 1 and Signature key S = R + 2 using AES

Encrypt AES language using certified server’s public key

Encrypt R and ID using AES then send all

Session 1 -> n:

E = E + 2 and S = S + 2

Encrypt ID using new E to get ID’ and send

Receive encrypted confirmation, decrypt and verify

Server:

Session 0:

Send CA Certificate

Receive encrypted language L’ via its public key

Decrypt L’ using its own private key to get L

Set AES language using L

Received AES encrypted R, ID

Decrypt R’ and ID’ using AES

Create encryption key E = R + 1 and signature key S = R + 2 using AES

Session 1 -> n:

E = E + 2 and S = S + 2

Receive encrypted ID’

Decrypt ID' using new E to get client's ID

Compare with stored ID to authenticate (make sure same client)

*2. Confidentiality*

We use SHA1 to encrypt our files which is generating and using one-time pad to XOR with data. The one-time pad shared key is generated using polyalphabetic cipher chosen at random from the character set (see more detail in the *AES.java* file). This gives the encryption unbreakable without knowing the key, since the characters is random, different from each session, and yields no statistical relationship to the language frequency.

File encryption:

b1 =SHA1(Kab|IV) c1=p1⊕b1

b2 =SHA1(Kab|c1) c2=p2⊕b2

… …

bi =SHA1(Kab|ci-1) ci=pi⊕bi

String encryption:

Polyalphabetic cipher that adds offset to each character of the original text to get the new text. Value of new text depends on the location of each character in the original text AND the value of the character in the language AND the offset value.

*3. Integrity*

We also use SHA1 to calculate the MAC (Message authentication codes), such that:

MAC = SHA1(Kab|m)

**III. Threat Models**

*1. Eavesdropping*

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 because they are encrypted with 1-time pad keys.

*2. Initiate a Conversation Pretending to be Client*

The project has one-way authentication, so the server cannot verify the client. It assumes the first client who successfully connects is the legitimate client.

*3. Break-in Attack*

The attacker can break into server’s machine and get its private key to decrypt the master key from client. BUT, since each session has a new key, and the master key is not used for encryption/decryption, stealing server’s private key does not help attacker to decrypt the captured messages.

*4. Man-in-the-Middle Attacks*

The attacker cannot get useful information if he doesn’t know all the keys (reason stated above).

The attacker cannot hijack the session using TCP hijacking because the authentication does not rely on IP address, but instead the content of the message.

The attacker can steal a message and does not forward to a party, in which case after sometimes both parties will end the connection due to timeout. Even though each party cannot do anything to prevent such an event, they still can detect the message has been stolen.

The attacker cannot successfully execute replay attack because each message is marked with a sequence number. If the receiving message does not have the expected sequence number, it will be dropped by the recipient. Intrusion detection will notifies the client/server after receiving more than 5 out-of-sync messages, which causes them to terminate the connection. Moreover, the initial number of message sequence is chosen randomly by the client, and the server just increment the message sequence onward. The attacker cannot simply counts the number of messages that has been sent to get the correct sequence number of a specific message. In addition, for regular polyalphabetic cipher, the same plaintext will always give the same cipher text. But we introduce the offset number that produce different cipher text given the same plaintext with different offset to truly produce a one-time pad. Therefore, the attacker cannot just create a message with his/her own sequence number and send, nor can he/she collects encrypted messages and studies to figure out the pattern.

The attacker cannot tamper with the message without being detected because the message is appended with a checksum and is signed by the sender.

*5. Denial of Service Attack*

If the attacker send a certificate request to initiate the session, but then hangs and does not send anything else (tries to keep the server busy waiting for the next message), the server can detect the empty input from that connection. It then terminates the connection with the attacker and accepting new connection (as fresh start).

**IV. Contributions**

Bao Nguyen: Communication protocol, Secret key encryption using poly-alphabetic cipher, Encryption & Decryption on Strings using poly-alphabetic cipher, Message sequence, Report, Intruder simulation – possible attacks

Mofan Li: Certificate, Encryption & Decryption on file using public key crypto, Message integrity for file using SHA1, Report

*(\*) If for any reason you cannot run the project from the submitted zip file, please check out our project on GitHub at* [*https://github.com/baonguyen96/FileTransferApplication*](https://github.com/baonguyen96/FileTransferApplication)*. Here you can see the distribution break-down as well.*