Programming Assignment 2

Authors: Tan Ting Yu (1002169) and Chong Lok Swen (1002468)

Date: -

**How To Run**

Ensure that you are in the /PeaceAndPrograss/src/equality/ directory.

Server:

java ServerWithSecurity [port number] [cp (= 1 or 2)]

Client:

java ClientWithSecurity [server IP address] [port number] [file name] [cp (= 1 or 2)]

Local Test:

Compile and run LocalTest.java, which uses port number4321 and will prompt the user to input the desired cp(= 1 or 2) before proceeding with file upload.

\* ensure that .crt (of certification authority and server), .der (server’s RSA private key) and source files (.txt) are in the working directory

\* downloaded files are saved in the *recv* folder

**CP-1**

The uploaded file is not encrypted, as such can be easily intercepted and interpreted. After verifying SecStore's certificate, the client should use SecStore’s RSA public key to encrypt the file before sending it to SecStore. As only the SecStore knows the private key, intermediary routers and communication links will not be able to decrypt the data.

A screenshot of a cell phone

Description generated with very high confidence

*Figure 1: AP and CP-1 specification.*

**CP-2**

**A screenshot of a cell phone

Description generated with very high confidence**

*Figure 2: AP and CP-2 Specification.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | |  |
| **File Name** | **File Size (bytes)** | **Upload Time (ms)** | |
| **CP-1** | **CP-2** |
| rr | 2047652 | 7486.115 | 1641.243 |
| ulysses | 1566847 | 4498.788 | 1431.908 |
| dataforfit | 255465 | 850.3077 | 691.2032 |
| vocab | 20240 | 530.7098 | 508.9372 |
| onedaydiffs | 6837 | 478.3206 | 470.6343 |
| *Table 1: Upload time of files with different sizes.* | | | |
|  | | | | *Figure 3: Graph of upload time against file size.* |

For small file sizes, the performance of both CP-1 and CP-2 are similar. However, from the above graph, CP-1’s line has a much steeper gradient than that of CP-2, the time taken by CP-1 increasing significantly quicker than CP-2 as the file sizes become larger. Hence, CP-2 is the more practical choice.