Phang Teng Fone 1003296
Gerald Lim 1003371

Programming Assignment 2 Report

Fig. 1 below gives the basis of a possible protocol. However, there's one problem with the. What is the problem? Explain it in your handout for submission, and give a fix for the problem.

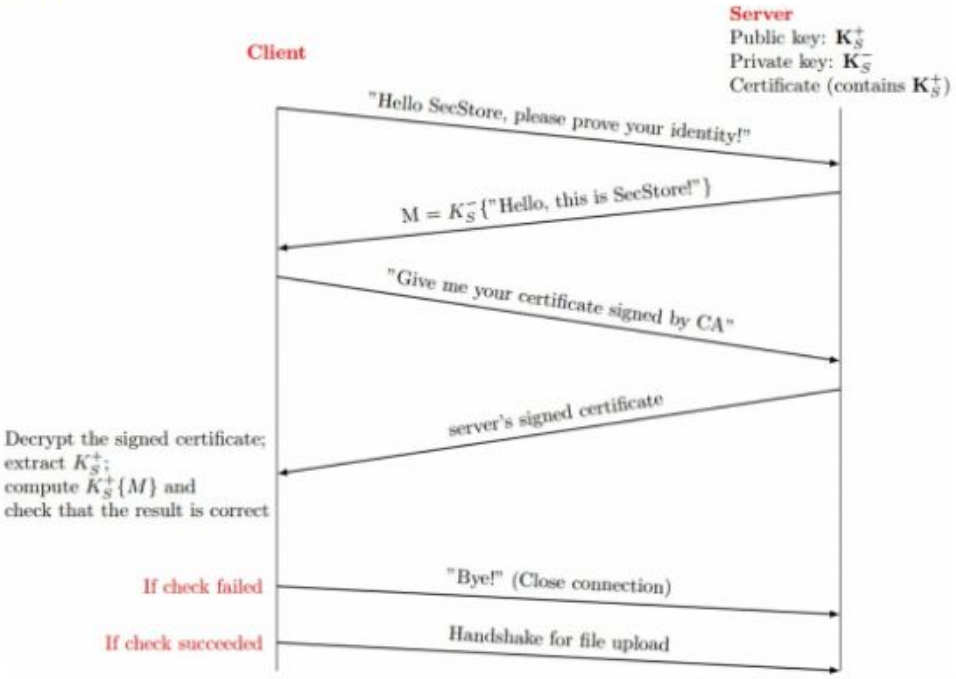
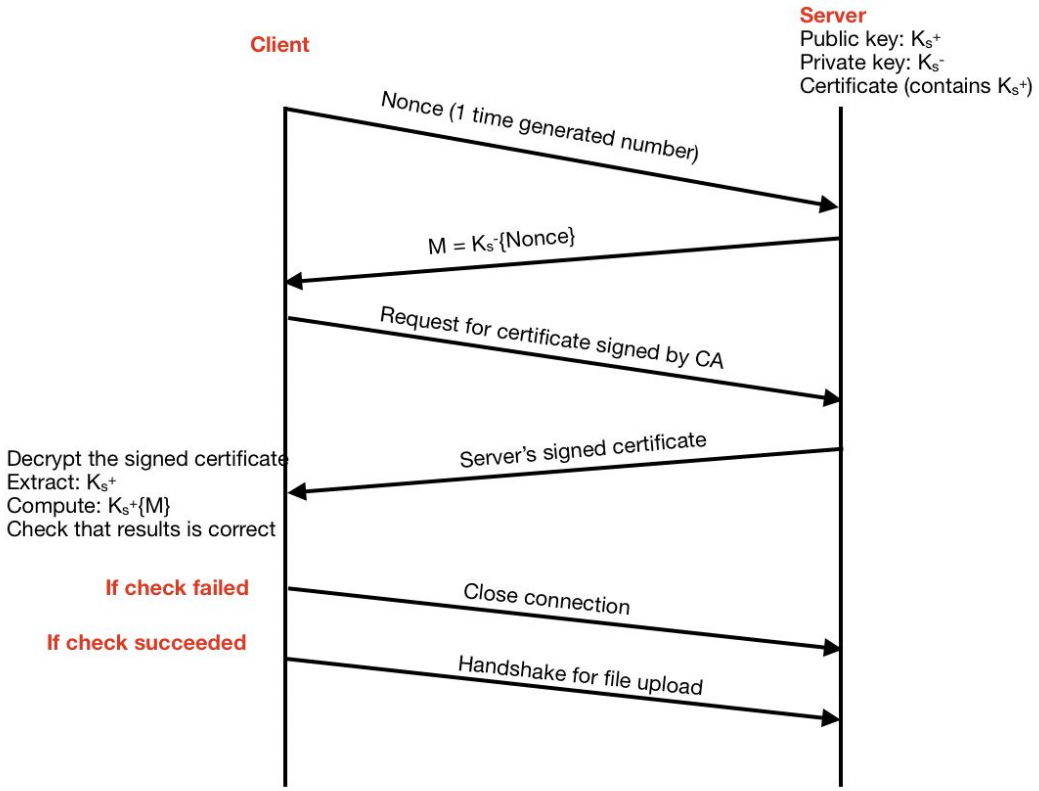


Fig. 1: Basis of Authentication Protocol

The issue with the handout is that the client is susceptible to playback attack. T(malicious attack) may record and playback the encrypted message that comes from the server. The client cannot tell if the encrypted message comes from the server or T. Therefore, authentication is compromised.

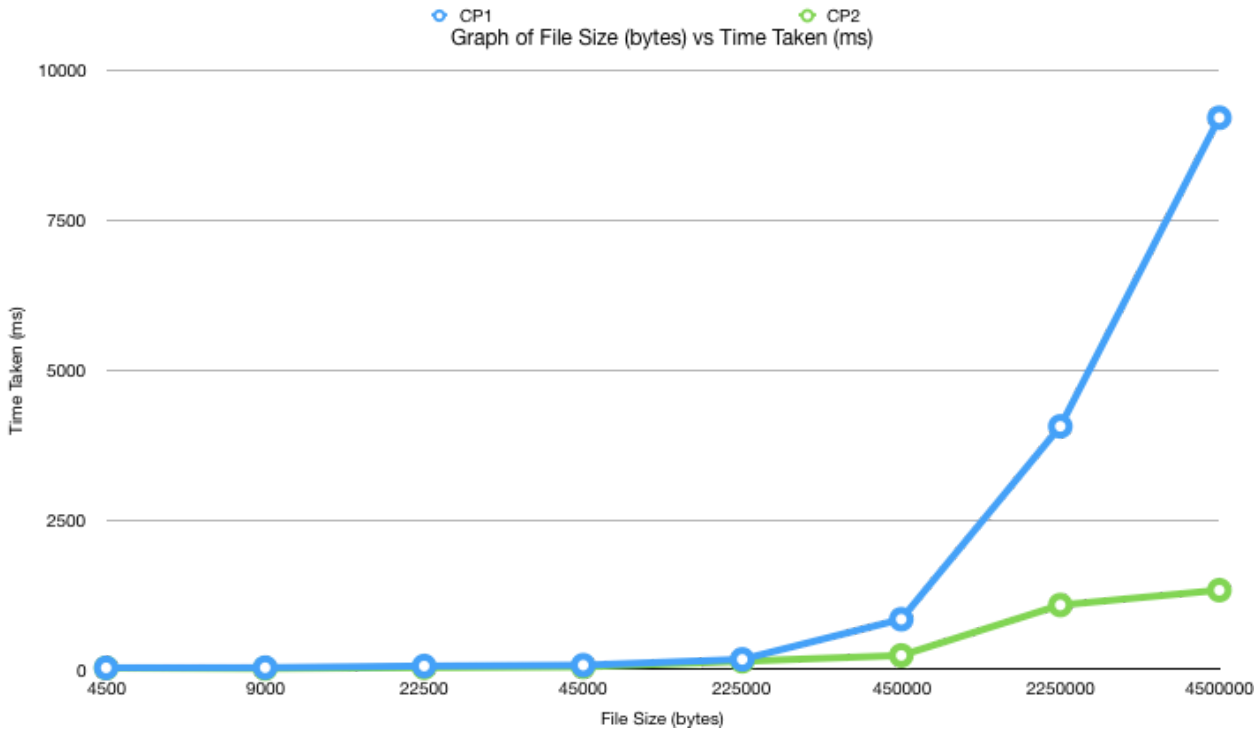


Proposed Solution

- The client first sends a nonce (1 time generated number) to the server
- The server the encrypts the client's nonce its own private key using RSA encryption and sends it back to the client
- The server also sends its signed certificate along with the encrypted nonce
- The user retrieves the CA public key from the certificate provided by a known organisation
- The user validates the server signed certificate and verifies the CA public key with the server signed certificate
- If the above two conditions pass, authentication is a success and client can begin sending encrypted files, otherwise server may be a malicious attacker

The proposed solution ensures authentication and confidentiality as malicious attacks such as playback attacks can be prevented. This can be observed in 2 scenarios:

- A nonce is unique, T cannot record and playback the same encrypted message multiple times. If the decrypted nonce and the actual nonce are different, T will be exposed.
- A failed verification of the CA public key with the server certificate will indicate the inauthenticity of the server's certificate, hence exposing T



CP1

File Name	File Size	Time Taken
100.txt	4,500 bytes	26.982311ms
200.txt	9,000 bytes	29.992244ms
500.txt	22,500 bytes	57.022084ms
1000.txt	45,000 bytes	71.034611ms
5000.txt	225,000 bytes	168.586852ms
10000.txt	450,000 bytes	838.779694ms
50000.txt	2,250,000 bytes	4061.229645ms
100000.txt	4,500,000 bytes	9216.593608ms

CP2

File Name	File Size	Time Taken
100.txt	4,500 bytes	25ms
200.txt	9,000 bytes	16ms

500.txt	22,500 bytes	31ms
1000.txt	45,000 bytes	43ms
5000.txt	225,000 bytes	137ms
10000.txt	450,000 bytes	234ms
50000.txt	2,250,000 bytes	1076ms
100000.txt	4,500,000 bytes	1324ms