Deniz Aytemiz

CS/ECE 5590: Written Homework Assignment

1. TLS/SSL protocol stands for Secure Socket Layer.
2. TLS/SSL ensures the confidentiality, integrity and authenticity of the network communication.
3. Firstly, client C sends a request to the server. In turn the server should respond with the central authority signed certificate. Client takes this certificate and verifies it to another server to ensure the public key given within the certificate is actually the public key of the website/application. This is to prevent man-in-the-middle attack in which an attacker can imposter as the server establishing the connection and steal clients credentials. After the public key is verified, the client encrypts a message with PubK received and sends it to the server. Server should be able to decrypt the message with its private key. If this is done successfully, the client can establish a successful connection with the website.