Network Security(CS6500) - Tutorial 5
Public Key Infrastructure

March 29, 2019

Questions

1. Generate a self-signed certificate for the root Certificate Authority(CA) using openssl library. You are supposed to generate a certificate and CA's private key file.
2. Issue a digitally signed certificate for the company called **shophere.com** using its private and public key. List the differences between the process of issuing certificate for **shophere.com** and issuing self-signed certificate for the root CA. Submit a copy of encoded key file in readable form.
3. Setup a webserver for **shophere.com** using the certificate generated by CA in the previous question. Access the domain through web browser and note down the response. Explain how to resolve the issue if any. What will happen if we modify the server certificate or server key file ?
4. Implement a secure TCP client and server communication to access **shophere.com** using openssl TLS/SSL connection. To achieve secure communication, the following conditions should be verified.
    a. Client should verify the effective date of server's certificate
    b. Is the certificate belong to the server?
    c. Is the certificate issued by an authorized CA?
    d. Check whether the server is not a spoofed one.

Note:

Change openssl.conf file to create your own certificates for CA and the server if needed.

Submission

- Write your observations in detail on each question in the report.
- Final submission should contain a report along with supporting documents.