Information Security COMP 421

Fall 2024 Section B

Assignment 2

Hira Ali

251690180

1) Generate a private and public key

- Private key: openssl genrsa -out myprivatekey.pem 2048
- Public key from the private key: openssl rsa -in myprivatekey.pem -pubout -out mypublickey.pem

```
hira@hira-VirtualBox:~$ mkdir assign2
hira@hira-VirtualBox:~$ cd assign2
hira@hira-VirtualBox:~/assign2$ openssl genrsa -out myprivatekey.pem 2048
hira@hira-VirtualBox:~/assign2$ openssl rsa -in myprivatekey.pem -pubout -out mypublickey,pem
writing RSA key
```

2) Generate a Certificate Signing Request (CSR)

openssl req -new -key myprivatekey.pem -out myrequest.csr

```
hira@hira-VirtualBox:~/assign2$ openssl req -new -key myprivatekey.pem -out myrequest.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:Pakistan
String too long, must be at most 2 bytes long
Country Name (2 letter code) [AU]:pk
State or Province Name (full name) [Some-State]:punjab
Locality Name (eg, city) []:lahore
Organization Name (eg, company) [Internet Widgits Pty Ltd]:fccu
Organizational Unit Name (eg, section) []:uni
Common Name (e.g. server FQDN or YOUR name) []:hira
Email Address []:ahira0888@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:hira123
An optional company name []:fc
```

3) Create a self-signed certificate

openssl x509 -req -days 365 -in myrequest.csr -signkey myprivatekey.pem -out mycertificate.crt

```
hira@hira-VirtualBox:~/assign2$ openssl x509 -req -days 365 -in myrequest.csr -signkey myprivatekey.pem -out
 mycertificate.crt
Certificate request self-signature ok
subject=C = pk, ST = punjab, L = lahore, O = fccu, OU = uni, CN = hira, emailAddress = ahira0888@gmail.com
```

4) Act as a Certification Authority (CA) to issue certificates.

- Create a CA private key: openssl genrsa -out ca_privatekey.pem 2048
- Create a CA certificate: openssl req -x509 -new -nodes -key ca_privatekey.pem -sha256 -days 3650 -out ca_certificate.crt
- Use the CA to sign a CSR and issue a certificate: openssl x509 -req -in myrequest.csr -CA ca_certificate.crt -CAkey ca_privatekey.pem -CAcreateserial -out issued_certificate.crt -days 365 -sha256