SCS2311 - Cryptography and Information Security

University of Colombo, School of Computing

Lab 8: OpenSSL CA Server

Practical Environment

Please use your Ubuntu environment (Laptop or VM) to work on this practical. In Ubuntu (Linux) OpenSSL is preinstalled. You have to download CAServer.zip file and unzip it. In order to generate SSL certificates, scripts are given in the CAServer.zip file.

1. **First you need to install a Certification Authority (CA). Execute createCA.sh script, it will create your own CA.**
   Your CA server's public key file is **cacert.pem**. It is in the sslCA directory. This public key has to be configured as trusted certificate in your applications.

2. **Then execute createHostCert.sh script to generate public private key pair and public key certificate for a Web Server.**
   Your private keyfile is **hostkey.pem** and certificate file is **hostcert.pem**. You can point these files by editing the the web server configuration (For Appache - htttpd-ssl.conf file).

3. **In order to generate a key pair and certificate to a person, execute createUserCert.sh. It will create your personal certificate.**
   Your private key and certificates are packed into **usr.pfx** file. You can import it to your browser, e-mail or any other application.

4. **Import your keys and certificate file (usr.pfx) into a Firefox browser.**

5. **Finally, view and observer the attributes of newly generated public key certificate, capture the screen short of it and upload it to the LMS.**

+++ end +++