Wroclaw

Secure Systems and Networks

Laboratory No. 4

Wiktor Lagiewka 219226

- **Create CA**

I used script *CA.pl* from `/usr/lib/ssl/misc/`. Firstly I edited file with default configuration `openssl.cnf` to set own default parameters. Then I created new CA by command `./CA.pl -newca`.

- **Create certificate request**

I used above script and typed *./CA -newreq* to create certificate then *./CA - sign to sign it.*

- **Configure Apache server to use it**

Firstly I installed Apache2 and start it to make sure it works *systemctl start apache2.* Then I configured Apache2 to use SSl:

(1) Activated the SSL Module by `a2enmod ssl` then restarted the Apache `service apache2 restart.`

(2) Created new directory `/etc/apache2/ssl` and placed there key and certificate which I generated in previous step.

(3) Edited file `/etc/apache2/sites-available/default-ssl.conf` and changed entries
SSLCertificateFile and *SSLCertificateFile* to actual path to key and certificate in *apache2/ssl*.

(4) Enabled SSL Virtual Host by command `a2ensite default-ssl.conf` and restarted Apache.

Now I can reach https://localhost/ but browser gives a warning that cannot verify the identity of server – because it has not been signed by certificate authority that it trusts. (to bypass this I added exception).

- **client certificates**

To do this task I simply used `./CA.pl -newreq` to create new certificate request, then `./CA.pl -sign` to sign this certificate and lastly `./CA.pl -pkcs12` to create it in PKCS12 format to be able to import it to the browser. Passwords are *client1* and *client2*.

- **Configure Apache to recognize client certs**

To configure the Apache to do this task I copied CA certificate to `/etc/apache2/ssl` and added a line to `default-ssl.conf`.