SVS | Exercise 6

Task 1

3 Subjekte möchten über einen unsicheren Kanal mittels a) eines **symmetrischen** und b) eines **asymmetrischen** Verschlüsselungs-verfahrens kommunizieren. Wie kann Vertraulichkeit, Integrität und Authentizität der gegenseitigen Kommunikation hergestellt werden?
Betrachten Sie für den Fall b) zusätzlich die Situation, wenn jeglicher Datenaustausch zwischen diesen 3 Subjekten über andere Wege unmöglich ist

3 subjects want to communicate over an unsecure channel using a) a **symmetric** and b) an **asymmetric** encryption method. How one can establish confidentiality, integrity and authenticity of mutual communication?
For the case b) consider a situation, where no data exchange over other channels among the 3 subjects is possible.

Task 2

1. Welche Informationen werden in den X509 Zertifikaten abgelegt?
2. Was ist ein *Certificate Signing Request (CSR)*?
3. Erzeugen Sie mittels *openssl* ein **selbstsigniertes** X509 Zertifikat:
    a. *openssl genrsa -out server.key 2048*
    b. *openssl req -new -key server.key -out server.csr* (als *Subject Common Name* geben Sie *localhost* an)
    c. *openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt*
    d. Überprüfen: *openssl x509 -in server.crt -noout –text*
4. Starten Sie mittels *openssl* einen fiktiven Webserver auf dem Port 12345 und testen Sie die Seite https://localhost:12345 in Ihrem Browser:
    openssl s_server -accept 12345 -cert server.crt -key server.key -www

Warum bekommt man eine Warnung zu sehen?

1. Which information is stored in X509 certificates?
2. What is a Certificate Signing Request (CSR)?
3. Using openssl create a **self-signed** X509 certificate:
4. Using openssl start a fictitious Web server on port 12345 and test the page https://localhost:12345 in your browser.

Why do you see a warning?

Task 3

1. Erzeugen Sie mittels *openssl* ein Zertifikat für eine fiktive *Certification Authority* (CA) (siehe 2.3)
2. Importieren Sie das CA-Zertifikat in Ihren Browser (Bereich: Zertifizierungsstellen).
3. Erzeugen Sie ein X509 Zertifikat auf den Namen *localhost*, diesmal aber unterschrieben mit dem CA-Schlüssel aus 3.1:

1. Using *openssl* create a certificate for a fictitious certification authority (CA) (see 2.3)
2. Import the CA certificate into your browser (area: certification authorities)
3. Create an X509 certificate on the name *localhost*, but now signed using the CA-key from 3.1:

openssl x509 -req -days 360 -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial -out server.crt

4. Starten Sie den Webserver neu und öffnen Sie dieselbe Seite. Warum wird die Warnung nicht mehr angezeigt?

4. Restart the Web server and open the same page. Why no warning is shown anymore?

Homework

1. Erzeugen Sie ein selbstsigniertes Zertifikat auf Ihren Namen (als *Subject Common Name* z.B. Ihr URZ-Nutzerkürzel angeben).
2. Wandeln Sie das soeben erstellte Zertifikat in das *pkcs12/pfx* Format um.
3. Importieren Sie die pkcs12-Datei in den Zertifikatsspeicher von Ihrem Browser (Bereich: Persönliche Zertifikate).
4. Mittels openssl starten Sie den Webserver und verlangen Sie nach einem Clientzertifikat:

1. Create a self-signed certificate on your name (as *Subject Common Name* put e.g. your URZ account name)
2. Convert the just created certificate into the *pkcs12/pfx* format.
3. Import the pkcs12 file into the certificate store of your browser (area: personal certificates)
4. Using openssl start a web server and request a client certificate:

openssl s_server -accept 12345 -cert server.crt -key server.key -www -Verify 0

5. Öffnen Sie die Seite https://localhost:12345 im Browser und wählen Sie das importierte Zertifikat für die Authentifizierung aus. Wie vertrauenswürdig ist die Information im Subject Common Name-Attribut für den Server?

5. Open the page https://localhost:12345 and select the imported certificate to authenticate. How trustworthy is the information in Subject Common Name attribute for the server?