Secure and Dependable Systems
Jacobs University Bremen
Dr. Jürgen Schönwälder

Course: CO21-320203
Date: 2020-04-02
Due: 2020-04-16

SADS 2020 Problem Sheet #7

Problem 7.1: *X.509 certificates* (1+1+1+1+1 = 5 points)

The `openssl` command can be used to create and manipulate X.509 certificates.

a) Write instruction on how to generate a RSA public/private key pair. What key size did you use? Extract the public key into a separate file.

b) Write instruction on how to generate a Certificate Signing Request (CSR) for the RSA public/private key pair created in the previous step. Use the apropriate `openssl` to show the content of the CSR you have generated.

c) In order to sign certificates, you need to setup a Certificate Authority (CA). Explain the process to create a CA. Hint: Take a look at the Debian/Ubuntu Perl script `/usr/lib/ssl/misc/CA.pl` and its `-newca` option.

d) Write instruction on how to sign a CSR with your CA.

e) Create an X.509 certificate and a CA. Get your certificate signed by one of your classmates and help your classmates by signing their X.509 certificates. Upload your certificate to Moodle.

Problem 7.2: *X.509 certificate validation* (1+1 = 2 points)

a) Inspect the certificate presented by the web site `https://cnds.jacobs-university.de/`. What is the validity period of the certificate? What is the validity of the certificates in the certificate chain?

b) The Online Certificate Status Protocol (OCSP) can be used to test the revocation status of a certificate. In order to make the valication check efficient, TLS servers can use OCSP stapling. Briefly explain how OCSP stapling works.

Do the sites `https://cnds.jacobs-university.de/` and `https://beadg.de/` support OCSP stapling? Explain how this can be determined.

Problem 7.3: *diffie hellman key exchanges* (1+2 = 3 points)

Alice and Bob agree on using the prime number $p = 191$ and the primitive root $g = 42$. Alice randomly chooses the value $a = 27$.

a) Which value does Alice send to Bob?

b) After the key exchange, Alice has the key $k = 178$. Which value did Bob choose and which value did Bob send to Alice?