Author: Ruxandra F. Olimid
Computer Science Department, University of Bucharest

- Laboratory Assignemnt -
Digital Signatures and Digital Certificates

Disclaimer: During this course/lab you will be introduced to various notions of computer security, with the aim of learning how to secure systems. All notions and exercises are presented for didactic purposes, even if sometimes you are supposed to think like an adversary. Do not use these techniques for malicious purposes! They may have legal consequences in the event of committing crimes, for which you become fully responsible!

1. *Basic Concepts*

Recall *digital signatures* and *digital certificates* [1,2].

The following questions refer to the digital certificate of the faculty website [3]:
a) Who issued the digital certificate?
b) What is the validity of the certificate?
c) How many bits is the public key defined in?
d) What is the value of the encryption exponents in the certificate and in the certificates that attest it in the chain? What do you notice? Does this impact security?

2. *Key Generation using Putty*

Use *Putty* [4] to generate SSH keys:
a) Download *puttygen.exe* [4].
b) Generate a 2048-bit RSA public key - private key pair. Press *Generate*.
c) Add *PassPhrase*. What is this for?
d) Export the public key to the *public_key.pub* file, the private key to the *private_key.ppk* file. To do this, use *Save public key*, respectively *Save private key*.
e) Export the key in *openssh* format. To do this, go to *Conversions* and *Export OpenSSH key*.
f) Open and see what all the generated files contain.

3. *Digital Certificate Generation using OpenSSL*

Answer the following questions using *OpenSSL* [5]:
a) Generate an RSA key.
b) Use the previously generated key in a *self-signed* certificate, valid for 120 days, stored as *ca.crt.* Use the following information:

Country: RO
Province: Muntenia
City: Bucuresti
Organization: CA_SSI
Department:CA_SSI_Lab
Common Name: CA_numele vostru (e.g.: CA_Andrei)
E-mail: test@test.ro

For this, use the next command:

```
openssl req -new -x509 - days <days> -key <key> -out ca.crt
```

a) Read about *X.509* [6]. Have a look at the digital certificated that was created:

```
openssl x509 -text -noout -in ca.crt
```

b) Use this CA certificate to sign/issue another certificate of a subordinate entity SUB_SLA. Use the following information:

Country: RO
Province: Muntenia
City: Bucuresti
Organization: SUB_SSI
Department:SUB_SSI_Lab
Common Name: SUB_numele vostru (e.g.: CA_Andrei)
E-mail: test_sub@test.ro

To do this, first generate a new 2048-bit SUB_SSI entity key in the *sub.key file*.

c) Initiate a *Certificate Signing Request (CSR) sub.csr*:

```
openssl req -new -key sub.key -out sub.csr
```

d) Then create a certificate for SUB_SSI sub.crt signed by the CA authority, valid for 60 days, with serial number 02:

```
openssl x509 -req -days <days> -in sub.csr -CA <ceritificat_CA> -
CAkey <ca_key> -set_serial <serial_no> -out sub.crt
```

e) View the created digital certificate:

```
openssl x509 -text -noout -in sub.crt
```

f) Transform this certificate to *PKCS#12*:

```
openssl pkcs12 -export -out sub.p12 -inkey sub.key -in sub.crt -
chain -CAfile ca.crt
```

g) Verify the content of *sub.p12* by using:

```
openssl pkcs12 -info -in sub.p12
```

References

1. Kryszczuk, K., & Richiardi, J. (2014). *Springer Encyclopedia of Cryptography and Security*. Available at: https://www.researchgate.net/publication/230674947_Springer_Encyclopedia_of_Cryptography_and_Security
2. Itfreetraining. *What are certificates?* Available at: https://www.youtube.com/watch?v=LRMBZhdFjDI&ab_channel=itfreetraining
3. Facultatea de Matematică și Informatică. Universitatea din București. Available at: https://fmi.unibuc.ro/
4. Putty. Available at: https://www.chiark.greenend.org.uk/~sgtatham/putty/
5. OpenSSL. Available at: https://www.openssl.org/
6. Technopedia. X.509 Certificate. Available at: https://www.techopedia.com/definition/29751/x509-certificate