Autor: Ruxandra F. Olimid
Departamentul de Informatică, Universitatea din București

- Laboratorul 12 -
Semnături și certificate digitale

Disclaimer: Pe parcursul acestui curs/laborator vi se vor prezenta diverse noțiuni de securitate informatică, cu scopul de a învăța cum să securizați sistemele. Toate noțiunile și exercițiile sunt prezentate în scop didactic, chiar dacă uneori se presupune să gândiți ca un adversar. Nu folosiți aceste tehnici în scopuri malițioase! Acestea pot avea consecințe legale în cazul comiterii unor infracțiuni, pentru care **deveniți pe deplin răspunzători**!

1. Noțiuni introductive


Reamintiți-vă despre *semnături* și *certificate digitale* [1,2].


Următoarele întrebări se referă la certificatul digital al site-ului facultății [3]:

a) Cine a emis certificatul digital?
b) Care este validitatea certificatului?
c) Pe câți biți este definită cheia publică?
d) Care este valoarea exponenților de criptare din certificat și din certificatele care îl atestă în lanț? Ce observați? Are aceasta impact asupra securității?

2. Generarea cheilor folosind Putty


Folosiți *Putty* [4] pentru generarea cheilor SSH:

a) Descărcați *puttygen.exe* [4].
b) Generați o pereche de chei cheie publică - cheie privată RSA pe 2048 de biți. Apăsați *Generate*.
c) Adaugati *PassPhrase*. La ce folosește aceasta?
d) Exportați cheia publică în fișierul *publick_key.pub*, cheia secretă în fișierul *private_key.ppk*. Pentru aceasta, folositi *Save public key*, respectiv *Save private key*.
e) Exportați cheia în format *openssh*. Pentru aceasta, accesați *Conversions* și *Export OpenSSH key*.
f) Deschideți și vedeți ce conțin toate fișierele generate.

3. Generarea certificatelor cu OpenSSL

Răspundeți la următoarele cerințe folosind *OpenSSL* [5]:

a) Generați o cheie RSA. Revedeți laboratorul de criptare asimetrică dacă nu vă mai amintiți cum realizați acest lucru.

b) Folosiți cheia generată anterior într-un certificat *self-signed*, valabil 120 de zile, stocat ca *ca.crt.* Folosiți următoarele informații:

Country: RO
Provincie: Muntenia
Localitate: Bucuresti
Numele organizatiei: CA_SSI
Numele unitatii:CA_SSI_Lab
Common Name: CA_numele vostru (e.g.: CA_Andrei)
E-mail: test@test.ro

Pentru aceasta, folositi comanda

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

c) Citiți despre standardul *X.509* [6]. Vizualizați certificatul digital creat:

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

d) Folosiți acest certificat al CA ca să semnați/emiteți un alt certificat al unei entitati subordonate SUB_SLA. Folositi urmatoarele informatii:

Country: RO
Provincie: Muntenia
Localitate: Bucuresti
Numele organizatiei: SUB_SSI
Numele unitatii:SUB_SSI_Lab
Common Name: SUB_numele vostru (e.g.: CA_Andrei)
E-mail: test_sub@test.ro

Pentru aceasta, mai întâi generați o noua cheie a entității SUB_SSI pe 2048 de biți in fișierul *sub.key*.

e) Inițiați un *Certificate Signing Request (CSR) sub.csr*:

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

f) Creați apoi un certificat pentru SUB_SSI *sub.crt* semnat de autoritatea CA, valabil pentru 60 de zile, cu numărul serial 02:

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

g) Vizualizați certificatul digital creat:

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

h) Transformați acest certificat digital in *PKCS#12*:

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

i) Verificați conținutul fișierului *sub.p12* folosind:

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

Referințe bibliografice

1. Kryszczuk, K., & Richiardi, J. (2014). *Springer Encyclopedia of Cryptography and Security*. Accesibil la: https://www.researchgate.net/publication/230674947_Springer_Encyclopedia_of_Cryptography_and_Security Ultima accesare: septembrie 2021.
2. Itfreetraining. *What are certificates?* Accesibil la: https://www.youtube.com/watch?v=LRMBZhdFjDI&ab_channel=itfreetraining Ultima accesare: decembrie 2021.
3. Facultatea de Matematică și Informatică. Universitatea din București. Accesibil la: https://fmi.unibuc.ro/ Ultima accesare: decembrie 2021.
4. Putty. Accesibil la: https://www.chiark.greenend.org.uk/~sgtatham/putty/ Ultima accesare: decembrie 2021
5. OpenSSL. Accesibil la: https://www.openssl.org/ Ultima accesare: decembrie 2021.
6. Technopedia. X.509 Certificate. Accesibil la: https://www.techopedia.com/definition/29751/x509-certificate Ultima accesare: decembrie 2021.