MIEIC Segurança em Sistemas Informáticos (Computer Security) – 2019/20 FEUP

Exam without consultation of documentation (*closed-book* exam) **Normal Exam**
Duration: 1,5 hours **26.June.2020**
Weight in course final grade: 50%

You may answer in English or in Portuguese.

1. [1 pt]

The risks of too much complexity are stressed over and over again by scientists and academics that work on computer security. Consider the quote[*] "*Complexity is the enemy of security. The more you have to depend on, the less likely it is that you can understand it well enough to exclude vulnerabilities*.»
Besides the introduction of unsuspected vulnerabilities in the systems' design, give an additional risk to security raised by complexity.

2. [1 pt]

Suppose you want to transmit to a partner a confidential long document. You share with your partner a cryptographic key *K*, adequate to be used with a specific cryptographic algorithm.
Present:

a) a technique for preparing the document for the transmission – sketch an elucidating picture;

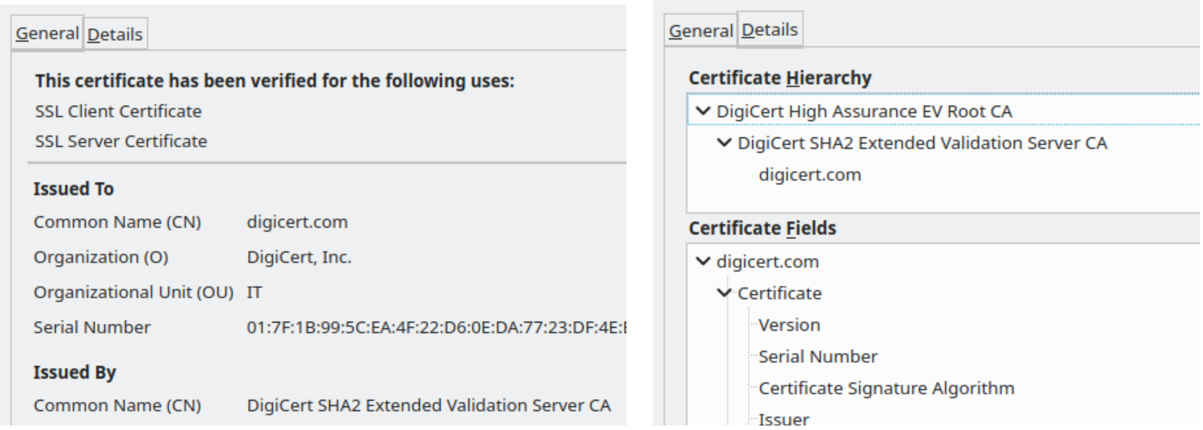
b) an advantage and a disadvantage of the scheme you have proposed.

3. [1 pt]

Say what is meant by MAC, Message Authentication Code, and explain how a *keyed* hash technique can be used to obtain and use it.

4. [1 pt]

Consider the nearby picture, which has two partial snapshots of the information offered by Firefox of a digital certificate it received upon accessing the website `digicert.com`.[**]



This certificate has been verified for the following uses:
SSL Client Certificate
SSL Server Certificate

Issued To

Common Name (CN)	digicert.com
Organization (O)	DigiCert, Inc.
Organizational Unit (OU)	IT
Serial Number	01:7F:1B:99:5C:EA:4F:22:D6:0E:DA:77:23:DF:4E:

Issued By

Common Name (CN)	DigiCert SHA2 Extended Validation Server CA

Certificate Hierarchy
- DigiCert High Assurance EV Root CA
  - DigiCert SHA2 Extended Validation Server CA
    - digicert.com

Certificate Fields
- digicert.com
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer

a) Identify the 4 essential pieces of information that must be present in a digital certificate. From what you can see in the nearby pictures, present values for those essential items. (Note: probably, you will not be able to present all those values! ;-))

b) What is the most crucial information you need in order to validate the shown certificate of `digicert.com`?

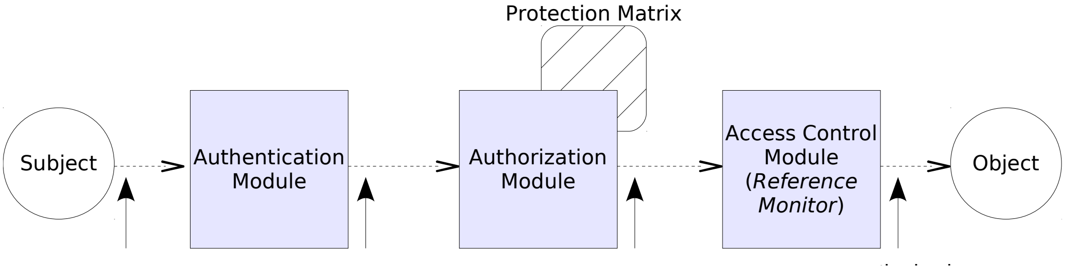
c) From the certificate hierarchy presented in the rightmost snapshot you can see that the same company (Digicert, Inc), which, by the way, is a Certificate Authority, uses an "intermediate" certifying entity for issuing its "low-level" `digicert.com`'s certificate. Why is it so?

[*] Jonathan Millen, computer scientist: "*On covert channel communication*", `https://intelligence.org/2014/04/12/jonathan-millen/`.

[**] Actually, it receives a chain of 2 certificates, each pertaining to each of the lowest presented entities in the Certificate Hierarchy shown in the rightmost picture. The certificate of the first presented entity in the hierarchy is supposed to be already installed in the browser.

5. [1 pt]

The nearby picture represents the system modules academically recommended for regulating a user's access to a computer resource.



Explain:

a) what does the “authentication” operation consist of;

b) what is gained, security-wise, by the shown scheme of separated modules (for authentication, authorization and access control).

6. [1.7 pt]

In a distributed system with centralized authentication the login operation is done by collecting the user data in the local system, but relying on a central authentication service to perform the operation. This central system stores the information needed to perform it.

a) If the authentication factor is a password, state some recommended precautions for forming the users’ passwords and storing them.

b) Describe a mechanism to securely perform the authentication in the remote system, considering network eavesdropping and replay.

c) Can authentication be based on asymmetric cryptography? Explain.

7. [1.5 pt]

Some obscure vulnerabilities are present on a program when a race condition is not protected enough (aka a TOCTTOU).

a) Explain, using an example, how they can be exploited.

b) Describe and explain two possible ways (in different situations) to stop those exploitations.

8. [1.8 pt]

The OAuth authorization protocol uses authorization codes and access tokens.

a) What is the difference between them, the purpose of each one, and the reason for using both?

b) Access codes can be opaque (just a value) or structured (in the format of a JWT). Describe how each form is verified by the resource server.

c) What is the OpenID Connect protocol? How is it used in conjunction with OAuth?

APM/JMC