Written Exam for IntroSec

2021-01-13 2pm – 6pm (4 hours)

Problem 1

Passwords are still often used. Name and explain security problems when relying on passwords, and problems when people have to use passwords (considering the following two scenarios). Explain how to mitigate the problems caused by passwords and whether the mitigations will introduce other problems (Note that the mitigations are not limited to using passwords).

a) A bank where you log in with your Swedish ID ("social security number") and a password you chose yourself.

b) A web-page where you can check your mobile phone surf usage/balance, and perform simple tasks, that comes with a password generated by the provider. This password cannot be changed by the user.

Problem 2

UrStudent is a software development company based in Stockholm. The company provides software to universities both in Sweden and across Europe that supports activities of students and teachers, including registration of marks, dashboard of individual student's marks and others. The company, to be compliant with GDPR, has started a process of implementing Privacy by Design (PbD) into their software development process. Focus on at least 5 principles of PbD and discuss what implications the integration of PbD will have in their software development process. Provide specific examples to support your discussion.

Problem 3

The ACL - Access Control List is popular as an access control method. However, it is not without problems. Imagine a scenario where you have 1000 users and 1 000 000 different objects (mostly files, but also some other resources). Furthermore, you have two different scenarios where in a) you have centralised control over all the subjects/users and objects, and in b) you have centralised control of whom the subjects are, but control of access rights is distributed over many different people and organisations. In all cases the access control method is the classic ACL without any wildcards.

What are the advantages and problems facing the organisation using this policy in the above case a) and b)? Does the policy work well in either case a) or in case b) (explain)?

Problem 4

Define each of the following IT security related terms. Also, for each of these terms further illustrate the concept by choosing a closely connected IT security concept and explaining the relationship between the concepts. Furthermore, give an example of an application of these tools/threats/concepts. Give concrete examples wherever possible. Structure each of your answers with headings definition, relationship to [your chosen related concept], and example. Your answers to each part should contribute to evidence of your deep understanding of the concept. Related concepts and examples should be chosen and explained with care to maximise the depth of your answers.

Please note that in general a 50% complete answer will be required to obtain a pass mark for this problem

- Signature-based intrusion detection
- Asymmetric cryptosystems
- Integrity check
- Trojan horse

If it helps you, you may like to paste the following into your editor to help you structure your answer:

- Signature-based intrusion detection
    - Definition
    - Relationship to [replace this with your chosen related concept]
    - Example.
- Asymmetric cryptosystems
    - Definition
    - Relationship to [replace this with your chosen related concept]
    - Example.
- Integrity check
    - Definition
    - Relationship to [replace this with your chosen related concept]
    - Example.
- Trojan horse
    - Definition
    - Relationship to [replace this with your chosen related concept]
    - Example.

Problem 5

Demonstrate how two different consequence-based principles of ethical reasoning can be applied to a difficult cybersecurity decision situation of your choice (create and describe your own case/situation). Describe the following issues:

What are the principles called? What do they mean? How can these be applied to your decision situation? Is the outcome of the decision likely to be the same regardless of which principle is applied? Do you at all times prefer one principle over the other (motivate)?