Examples of earlier exam questions covering the area of access control.

2013-08-12

Problem 2

In the course book Matt Bishop (05, p251) writes:
Two questions underlie the use of access controls:

1. *Given a subject, what objects can it access, and how?*
2. *Given and object, what subjects can access it, and how?*

Explain the practical significance of these questions, including what this implies for what Bishop calls *abbreviations* of rights and for revocation of rights.

2012-10-31

Problem 2

During the course we have made a clear division between methods for authentication and for access control. However, for some security mechanisms it may not be as clear whether they can be classified and described as authentication mechanisms or access control mechanisms.

Consider the key-cards that are distributed to staff and students at the DSV department to allow access to the building and its rooms.

Characterise the key-card system in terms commonly used to describe authentication methods, and then in terms commonly used to describe an access control mechanism. For each of these viewpoints motivate why the system is best characterised in the terms that you have used.

2012-08-20

Problem 3

Describe and explain how the practical implications of the *own* privilege will differ between Discretionary Access Control (DAC) and Mandatory Access Control (MAC) file systems.

Problem 4

Describe 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 *description*, *relationship to [your chosen related concept]*, and *example.*

- Certificate
- **Capabilities**
- Covert channel
- Common Criteria

2011-12-19

Problem 4

Describe 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 *description*, *relationship to [your chosen related concept]*, and *example.*
Some students may find it helpful to use the pre-printed problem 4 answer sheet for their answer. Those who choose not to should take care to follow the above instructions extra carefully.
Please note that in general a 50% complete answer will be required to obtain a pass mark for this problem

- RSA
- Spacial privacy
- **ACL (Access Control List)**
- Integrity policy

2011-10-25

Problem 2

[N.B. This concept ORCON is not covered in Pfleeger's book, and it therefore would not be part of a question on the IntroSec exam]

The underground (or “subway” if you prefer) system of the Stockholm local public transport network has a physical access control mechanism of barriers, the purpose of which is to prevent unauthorised travellers gaining access to the system. This is physical system (admittedly with some relevant IT elements) which is analogous to access control mechanisms of IT systems.

a) Using this analogy, reason to what extent this system can be viewed as either and Access Control List or a Capability Based system of access control. You may limit your discussion to only describing the case for subjects that are individual students and staff of the University.

Let us now change our perspective so as to instead analyse the tickets that we have to the underground as being the objects of an access control system. These can be plastic cards with RFID chips in them, paper coupons, or mobile phone text message replies. Still limiting the subjects to be individual students and staff, we can assume our subjects to be owner of all three types of ticket. Note how these tickets are to some degree transferable, i.e., the owner is to free to lend them to others to use.

b) Suggest and explain a set of access rights that apply to these subjects and objects and that are designed to uphold the validity of the tickets. Discuss also whether it is more suitable to view this as a DAC, MAC, or ORCON based access control system. Be clear in any analogies that your draw from and/or assumptions that you make about the real life ticketing system.

2009-12-07

Problem 2

A student in higher education might expect to be given space on a file server where files for e.g. working with hand-in assignments can be kept. Suggest and motivate reasons why such a

file-server should apply on the one hand discretionary access control, or on the other hand mandatory access control.