

SET 3

Date: 05.11.2009

1 Lecture 10: Access Control

Exercise 1

- Give examples of Authentication without Identification.
- Give examples of Authorization without Authentication.

Exercise 2 (Access control lists and capability lists)

Alice can read and write the file f_1 , can read the file f_2 , and can execute the file f_3 . Bob can read f_1 , can read and write f_2 , and cannot access f_3 .

1. Write a set of access control lists for this situation. Which list is associated with which file?
2. Write a set of capability lists for this situation.

Exercise 3 (RBAC)

1. Summarize the main advantages of role-based access control.
2. Draw the access matrix that corresponds to the RBAC model depicted in Figure 1.

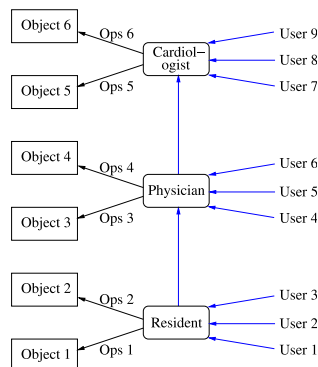


Figure 1: An RBAC Model

Exercise 4 (Examples)

Give some examples from everyday life where the following models for security policies are used:

1. Mandatory access control
2. Discretionary access control

Exercise 5 (Bell-LaPadula)

Given are the security levels TOP SECRET, SECRET, CONFIDENTIAL and UNCLASSIFIED (ordered from highest to lowest) and two categories: Nuclear and Army. We have four subjects:

- the president has a TOP SECRET clearance for Nuclear and Army,
- the colonel has SECRET clearance for Army and Nuclear,
- the major has only CONFIDENTIAL clearance for Army, and
- the soldier has only UNCLASSIFIED clearance for Nuclear.

We also have some objects (documents):

- the army position at security level SECRET,
- the number of army units at security level CONFIDENTIAL,
- the number of nuclear units at security level CONFIDENTIAL,
- the costs of the nuclear program at security level UNCLASSIFIED,
- the costs of the army at security level UNCLASSIFIED, and
- the nuclear code at security level TOP SECRET.

Answer the following questions based on the Bell-LaPadula model:

1. Draw the lattice of classifications.
2. Can the president compute the overall defense costs (army + nuclear)?
3. Can the major compute the total number of nuclear and army units?
4. Can the colonel compute the total number of nuclear and army units?
5. Can the colonel change the army position?
6. Can the major change the nuclear code?
7. Can the soldier change the nuclear code?
8. What problem is raised by question 7?

2 Lecture 11:

Exercise 6

We consider public variables, called low variables denoted by ℓ_i and private ones, called high variables denoted by h_i . Say if there is some leak of information for the following program lines, where the encryption is a deterministic and asymmetric scheme (like RSA), and νl_1 means that you generate a fresh value and assign it to the variable l_1 :

- $\ell_1 := \nu h_2 \cdot h_2 \oplus h_1$?
- $\ell_1 := \nu \ell_2 \cdot \ell_2 \oplus h_1$?
- $\ell_1 := \{h_1\}_l$ and l known?
- $\ell_1 := \{h_1\}_h$ and h is not known?
- $\ell_1 := \{h_1\}_h, \{0\}_h$ and h are known?
- $\ell_1 := \{\nu \ell_2 \cdot \ell_2 \oplus h_1\}_h$ and h known?
- $\ell_1 := \{\nu \ell_2 \cdot \ell_2 \oplus h_1\}_l$ and l known?

3 Lecture 12:

Exercise 7

(15 points) Compute the recoverable set of keys and the pattern of the following expressions:

- $E_1 = \langle \{k_1\}_{k_2}, \{k_2\}_{k_1} \rangle$
- $E_2 = \langle \langle \{k_2, k_4\} \rangle_{k_1}, \{ \{k_1\}_{k_2} \}_{k_4} \rangle, k_4$
- $E_3 = \{ \langle \{k_3, 0\} \rangle_{k_2} \}_{k_1}, \langle \{0\}_{k_3}, k_1 \rangle, k_5$