Principles of Data Protection: Assignment 1

Deadline: 23 September 2016

How to submit the assignment:
– by email (n.zannone at tue dot nl)

For any question send me an email

Note: The assignment should be done individually.

Questions

1. Search in the news an article about privacy violations. Describe briefly the reported incident and discuss its privacy implications (at most one page). The reference (or url) to the article should be given. **Note:** The article should be at most six months old.

2. Recall the HRU model.

   (a) Compute the access matrix that results from the following initial state

	File 1	File 2
Alice		
Bob		own
Charlie	own	*read
David		

   by executing the sequence of commands α defined as follows:

1 $CREATE(Alice, File3)$
2 $CONFER_{*read}(Alice, Bob, File3)$
3 $CONFER_{*exec}(Bob, Alice, File2)$
4 $TRANSFER_{exec}(Alice, Charlie, File3)$
5 $CONFER_{read}(Bob, Alice, File2)$
6 $CONFER_{*read}(Bob, Alice, File1)$
7 $TRANSFER_{exec}(Alice, Bob, File2)$
8 $CONFER_{*read}(Alice, David, File2)$
9 $CREATE(Alice, File1)$
10 $CONFER_{*read}(Alice, Bob, File1)$
11 $CREATE(Bob, File4)$
12 $CONFER_{*exec}(Alice, Alice, File3)$
13 $TRANSFER_{read}(Charlie, David, File1)$
14 $TRANSFER_{read}(Alice, David, File1)$
15 $TRANSFER_{write}(Bob, David, File4)$
16 $REVOKE_{read}(Alice, David, File1)$
17 $REVOKE_{exec}(Alice, Alice, File2)$
18 $TRANSFER_{write}(Bob, David, File3)$
19 $REVOKE_{write}(Bob, David, File4)$
20 $TRANSFER_{exec}(Alice, David, File2)$

   Hints:

   - Command $CONFER_{*read}$ is equal to $CONFER_{read}$ but grants $*read$ instead of $read$. Similar principle applies to $CONFER_{*write}$ and $CONFER_{*exec}$.
   - Command $REVOKE_{read}$ removes both $read$ and $*read$. Similar principle applies to $REVOKE_{exec}$ and $REVOKE_{write}$.

   (b) Is α leaking access privileges? (Consider only David to be untrusted) Justify the answer.

3. Let HIGH, MEDIUM and LOW be integrity levels (ordered from the highest to the lowest). Let Navy and Army be two categories. Consider the following subjects and objects along with their integrity classes:

Subject	**Integrity**
Colonel	(HIGH,{Navy})
Major	(MEDIUM,{Army,Navy})
Captain	(MEDIUM,{Army})
Lieutenant	(LOW,{Navy})

Object	**Integrity**
Army position	(HIGH,{Army})
Fleet position	(HIGH,{Navy})
Number of army units	(MEDIUM,{Army})
Number of navy units	(MEDIUM,{Navy})
Cost of army units	(LOW,{Army})
Cost of navy units	(LOW,{Navy})

Answer the following questions based on the Biba model with low-watermark for subjects:

(a) Draw the lattice of classifications.

(b) Can the major change the army position?

(c) Can the major change the number of army units, after he read the cost of army unit?

(d) Can the lieutenant read the number of army units, after the major changed it?

(e) Can the colonel change the cost of navy units, after he read the fleet position?

(f) Can the colonel change the fleet position, after the lieutenant read it?

(g) Can the captain read the number of navy units?

Justify your answer.

Hint: Changing an object requires 'write' access to the object.

4. Define an RBAC$_3$ system to regulate a conference submission system implementing the following requirements:

   (a) An author can submit one or more papers to the conference.

   (b) An author can view its submission(s).

   (c) An author can update its submission(s).

   (d) A conference has a Program Committee (PC).

   (e) There is at least one PC chair, who is a PC member.

   (f) A PC member can view any submission.

   (g) Only the PC chair can assign papers to PC members.

   (h) A PC member can assign its papers to external reviewers.

   (i) A paper can be reviewed by a PC member.

   (j) A paper can be reviewed by an external reviewer.

   (k) Each paper should be reviewed by at least three reviewers (PC members or external reviewer).

   (l) An authors may (or may not) be a PC member.

   (m) However, authors cannot review their own papers.

   (n) The decision about the acceptance of a paper is made by the PC chair(s).

5. A consulting firm provides professional advice to organizations. Among its clients, the firm has two banks, A and B, and an insurance company C. Suppose that a consultant of the firm is assigned to A, another consultant is assigned to B and both consultants are assigned to C.

   - Explain the possible security breach that can occur if only the simple property of the Chinese wall model is enforced.
   - Show how the leak could be prevented by taking into account (and enforcing) the *-policy.

6. Describe the Take-grant access control model. Discuss the main differences between the Take-grant model and the HRU model.