Principles of Data Protection: Assignment 1

Deadline: 18 September 2015
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. Let $R = \{own, read, write, exec\}$ be the set of rights. Assume a protection system with the following commands:

   command create(s, o)
     create object o
     enter own *into* $A[s, o]$
   end

   command assign_own_right(s, o, r)
     if own in $A[s, o]$
     then *enter r into* $A[s, o]$
   end

   command assign_right(s_1, s_2, o, r)
     if own in $A[s_1, o]$ and
       $r \neq$ write
     then *enter r into* $A[s_2, o]$
   end

   command transfer_right(s_1, s_2, o, r)
     if r in $A[s_1, o]$ and
       own not in $A[s_1, o]$
     then *enter r into* $A[s_2, o]$
         delete r into $A[s_1, o]$
   end

   Users should not be able to modify (write) documents created by other users. Is the system secure? Justify the answer.

3. Let SECRET, CONFIDENTIAL and UNCLASSIFIED be the secrecy levels (ordered from highest to lowest), CRITICAL and NON-CRITICAL the integrity levels (ordered from highest to lowest) and Navy and Army two categories. Consider the following subjects and objects along with their secrecy classes:

Subject	Secrecy Class	Integrity Class
Colonel	(SECRET,{Army})	(CRITICAL,{Army})
Major	(CONFIDENTIAL,{Army,Navy})	(CRITICAL,{})
Soldier	(UNCLASSIFIED,{})	(NON-CRITICAL,{Army,Navy})

Object	Secrecy Class	Integrity Class
Army position	(SECRET,{Army})	(CRITICAL,{Army})
Fleet position	(SECRET,{Navy})	(CRITICAL,{Navy})
Number of army units	(CONFIDENTIAL,{Army})	(CRITICAL,{})
Number of navy units	(CONFIDENTIAL,{Navy})	(CRITICAL,{})
Cost of army unit	(UNCLASSIFIED,{Army})	(NON-CRITICAL,{})
Cost of navy unit	(UNCLASSIFIED,{Navy})	(NON-CRITICAL,{})

Answer the following questions based on the combination of the BLP model and the Biba model:

(a) Can the colonel compute the overall number of defense units (This requires access to the number of army units and the number of navy units)?

(b) Can the colonel update the position of navy units?

(c) Can the major change the overall costs of army units (This requires access to the number of army units and cost of army units)?

(d) Can the major read the position of navy units?

(e) Can the soldier compute the overall number of defense units (This requires access to the number of army units and the number of navy units)?

(f) Can the soldier read the position of army units?

Justify the answers.

4. Define a RBAC$_3$ system to regulate permissions within a bank branch. The system should implement the following requirements:

(a) A bank employee can be a clerk, a manager or the head of the bank branch.

(b) A bank branch can have only one head.

(c) The head of the bank branch is a manager.

(d) Clerks can make loan offers to customers.

(e) Loan offers should be reviewed by a different clerk or a manager before they can be approved.

(f) If the amount of the loan offers is lower than $15K, the offer should be approved by a manager.

(g) If the amount of the loan offers is equal or greater than $15K, the offer must be approved by two managers.

(h) A bank employee cannot approve loan offers he made or reviewed.

5. Differentiate between static separation of duty (SSD) and dynamic separation of duty (DSD). Suppose we have $(\{r_1, r_2, r_3, r_4\}, 3) \in SMER$ and $(\{r_1, r_2, r_3, r_4\}, 3) \in DMER$. What are the implications of having both these constraints enforced simultaneously.

6. Describe the access control system used in FreeBSD.