Principles of Data Protection: Assignment 1

Deadline: 22 September 2017

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

<table>
<thead>
<tr>
<th></th>
<th>File 1</th>
<th>File 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td>own</td>
<td></td>
</tr>
<tr>
<td>Charlie</td>
<td>own</td>
<td>*read</td>
</tr>
<tr>
<td>David</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

   by executing the sequence of commands $\alpha$ defined as follows:

   1. $CONFER_{exec}(\text{Charlie, Alice, File1})$
   2. $CREATE(\text{Alice, File3})$
   3. $CONFER_{exec}(\text{Alice, Bob, File3})$
   4. $TRANSFER_{exec}(\text{Charlie, David, File2})$
   5. $CONFER_{read}(\text{Bob, Alice, File2})$
   6. $CONFER_{*read}(\text{Bob, Alice, File1})$
   7. $CONFER_{exec}(\text{Bob, Charlie, File2})$
   8. $TRANSFER_{read}(\text{Alice, David, File2})$
   9. $CREATE(\text{Alice, File2})$
   10. $CONFER_{*write}(\text{Alice, Charlie, File2})$

   11. $TRANSFER_{write}(\text{Charlie, David, File2})$
   12. $CONFER_{exec}(\text{Alice, Alice, File3})$
   13. $CREATE(\text{Charlie, File4})$
   14. $TRANSFER_{read}(\text{Alice, David, File1})$
   15. $TRANSFER_{write}(\text{Charlie, David, File4})$
   16. $REVOKE_{read}(\text{Alice, David, File1})$
   17. $REVOKE_{exec}(\text{Alice, Alice, File2})$
   18. $TRANSFER_{write}(\text{Bob, David, File3})$
   19. $REVOKE_{write}(\text{Bob, David, File4})$
   20. $TRANSFER_{read}(\text{Alice, David, File1})$

   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 $\alpha$ leaking access privileges? (Consider only David to be untrusted) 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:

<table>
<thead>
<tr>
<th>Subject</th>
<th>Secrecy Class</th>
<th>Integrity Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Colonel</td>
<td>(SECRET,{Army})</td>
<td>(CRITICAL,{Army})</td>
</tr>
<tr>
<td>Major</td>
<td>(CONFIDENTIAL,{Army,Navy})</td>
<td>(CRITICAL,{})</td>
</tr>
<tr>
<td>Soldier</td>
<td>(UNCLASSIFIED,{})</td>
<td>(NON-CRITICAL,{Army,Navy})</td>
</tr>
<tr>
<td>Object</td>
<td>Secrecy Class</td>
<td>Integrity Class</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Army position</td>
<td>(SECRET, {Army})</td>
<td>(CRITICAL, {Army})</td>
</tr>
<tr>
<td>Fleet position</td>
<td>(SECRET, {Navy})</td>
<td>(CRITICAL, {Navy})</td>
</tr>
<tr>
<td>Number of army units</td>
<td>(CONFIDENTIAL, {Army})</td>
<td>(CRITICAL, {})</td>
</tr>
<tr>
<td>Number of navy units</td>
<td>(CONFIDENTIAL, {Navy})</td>
<td>(CRITICAL, {})</td>
</tr>
<tr>
<td>Cost of army unit</td>
<td>(UNCLASSIFIED, {Army})</td>
<td>(NON-CRITICAL, {})</td>
</tr>
<tr>
<td>Cost of navy unit</td>
<td>(UNCLASSIFIED, {Navy})</td>
<td>(NON-CRITICAL, {})</td>
</tr>
</tbody>
</table>

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

(a) Can the colonel change the position of the fleet?
(b) Can the colonel compute the overall number of defense units? (This requires rights to read the number of army units and the number of navy units)
(c) Can the major read the position of the overall defense units? (This requires rights to read the position of army units and the position of the fleet)
(d) Can the major compute the overall number of defense units? (This requires rights to read the number of army units and the number of navy units)
(e) Can the major change the overall number of defense units? (This requires rights to write the number of army units and the number of navy units)
(f) Can the soldier read the cost of navy 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) Bank employees 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 offer is lower than $10K, the offer should be approved by a manager.
(g) If the amount of the loan offers is equal or greater than $10K, the offer must be approved by two managers.
(h) A bank employee cannot approve loan offers he made or reviewed.

5. Define the Chinese Wall model in the BLP Model.

6. SELinux implements a complex access control system that combines various access models, e.g. Role-Based Access Control and Mandatory Access Control. Describe the access control system used in SELinux highlighting how the various models have been combined/used and the authorization process.