Principles of Data Protection (2IMS25): Exam 23/1/2017

Questions

1. **(1.5 points)** Consider a protection system with the following commands:

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

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

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

   command transfer_rights(s_1, s_2, o, r)
   if exec into $A[s_1, o]$ and
   then enter r into $A[s_2, o]$ **end**.

   (Right own cannot be conferred and/or transfered.)

   Suppose Bob wants to share some documents with other users. Users should be able to read those documents, but they cannot modify them (consider right write for modification). Is the system secure? Justify the answer.

2. **(1.5 points)** 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 colonel change the cost of army units?
   (c) Can the colonel change the cost of army units, after he read the number of navy units?
   (d) Can the major read the cost of navy units?
   (e) Can the captain change the number of army units, after the lieutenant read it?
   (f) Can the captain change the number of army units, after he read the fleet position?
   (g) Can the lieutenant read the number of navy units, after the colonel changed it?

   Justify your answer.

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

3. **(1.5 points)** Chinese Wall

   (a) Explain the goal of the Chinese Wall model and describe the main concepts and properties of the model.

   (b) Explain the main differences between the Chinese Wall model and the Bell-LaPadula model.

4. **(2 points)** RT

   (a) Consider the following RT_0 policy.

   $A.s \longleftarrow A.t.u$
   $A.t \longleftarrow B.s$

   $B.s \longleftarrow B.t.u$

   $B.s \longleftarrow D$

   $B.t \longleftarrow C$

   $C.t \longleftarrow A$

   $C.u \longleftarrow J$

   $C.u \longleftarrow K$

   $J.u \longleftarrow P$

   $J.u \longleftarrow Q$

   - Find all principals populating $A.s$ and $B.s$ (which means, compute $[\![A.s]\!]$ and $[\![B.s]\!]$).
   - Write down the graph generated by the top-down algorithm when computing the semantics of $A.s$. (the top-down algorithm is also known as the "backward algorithm").

   (b) Consider the situation in which you have a company CORP1 with the following (self-explanatory) policy in RT

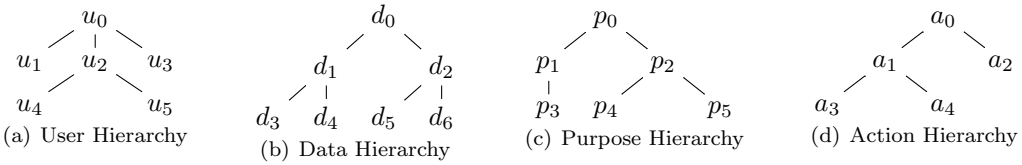
```
CORP1.president <- Sam

CORP1.vicepresident <- Tom
CORP1.vicepresident <- Jane

CORP1.highmanager <- CORP1.vicepresident
CORP1.highmanager <- CORP1.director

CORP1.manager <- Anton
CORP1.manager <- Cliff
CORP1.manager <- John
CORP1.manager <- . . .
CORP1.manager <- CORP1.highmanager
```

   Now, here it would be nice to be able to define an additional role `CORP1.lowmanager` that is populate by all managers that are *not* "highmanager" (that is, that are not members of `CORP1.highmanager`).

   - Explain why in this situation (i.e., given the above policy) it is not "possible" to write an RT role `CORP1.lowmanager` without changing the definition of `CORP1.manager` (technically, it is actually possible, but the resulting policy is suboptimal, or ugly, to say the least).
   - Modify the above policy (by redefining `CORP1.manager`) in order to accommodate the definition of `CORP1.lowmanager`.

5. **(1.5 points)** Let *pol* be an EPAL policy and the hierarchies in Figure 1 the user hierarchy, data hierarchy, purpose hierarchy and action hierarchy.

$$pol = \begin{cases} \langle (u_1, d_2, p_2, a_1)(\circ, true, o_1) \rangle \\ \langle (u_2, d_0, p_1, a_2)(+, true, o_2) \rangle \\ \langle (u_4, d_2, p_4, a_2)(-, true, o_3) \rangle \\ \langle (u_0, d_1, p_0, a_1)(\circ, true, o_4) \rangle \\ \langle (u_1, d_0, p_2, a_0)(+, true, o_5) \rangle \\ \text{Default ruling:} - \\ \text{Default obligations:} \{o_6\} \end{cases}$$



(a) User Hierarchy (b) Data Hierarchy (c) Purpose Hierarchy (d) Action Hierarchy

Figure 1: Hierarchies

Evaluate the following access requests against *pol*:

$req_1 = (u_2, d_2, p_3, a_2)$
$req_2 = (u_1, d_6, p_5, a_4)$
$req_3 = (u_2, d_0, p_2, a_2)$
$req_4 = (u_0, d_4, p_5, a_3)$

6. **(2 points)** Given the XACML policy and access request below, determine the access response.
Hint: If an attribute is missing (i.e., it is not provided in the request), then MustBePresent governs the applicability of the Rule/Policy/PolicySet.

   - If MustBePresent is "False" (default value), then a missing attribute results in an empty bag. (i.e., the Rule/Policy/PolicysSet is "Not Applicable")
   - If MustBePresent is "True", then a missing attribute results in an error. Some combining algorithms are defined in terms of an extended set of "Indeterminate" values ("Indeterminate(P)", "Indeterminate(D)", "Indeterminate(PD)"). The extended set associated with the "Indeterminate" contains the potential effect values which could have occurred if there would not have been an error causing the "Indeterminate".

Access Request

```
  <Request>
   <Attributes
         Category="urn:oasis:names:tc:xacml:3.0:subject-category:access-subject">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                Alice
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                manager
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                accountant
            </AttributeValue>
         </Attribute>
    </Attributes>
    <Attributes
         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                financialRecord
            </AttributeValue>
         </Attribute>
    </Attributes>
    <Attributes
         Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action">
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                write
            </AttributeValue>
         </Attribute>
    </Attributes>
  </Request>
```

```
<PolicySet PolicySetId="PS"
    xmlns="urn:oasis:names:tc:xacml:3.0:policy:schema:os"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    PolicyCombiningAlgId="urn:oasis:names:tc:xacml:3.0:policy-combining-algorithm:permit-overrides">
  <Target>
       <AnyOf>
          <AllOf>
           <Match
             MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 write
             </AttributeValue>
             <AttributeDesignator
                 MustBePresent="false"
                 Category="urn:oasis:names:tc:xacml:1.0:attribute-category:action"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:action-id"
                 DataType="http://www.w3.org/2001/XMLSchema#string"/>
           </Match>
          </AllOf>
        </AnyOf>
  </Target>
  <Policy PolicyId="P1"
      RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:first-applicable">
    <Target />
    <Rule Effect="Deny" RuleId="R1">
      <Target>
       <AnyOf>
         <AllOf>
           <Match
               MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                  employee
               </AttributeValue>
               <AttributeDesignator MustBePresent="false"
                   Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                   AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role"
                   DataType="http://www.w3.org/2001/XMLSchema#string"/>
           </Match>
           <Match
               MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
                  14:00
               </AttributeValue>
               <AttributeDesignator MustBePresent="true"
                   Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                   AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                   DataType="http://www.w3.org/2001/XMLSchema#time"/>
           </Match>
         </AllOf>
        </AnyOf>
      </Target>
    </Rule>
```

```
<Rule Effect="Deny" RuleId="R2">
  <Target>
   <AnyOf>
     <AllOf>
       <Match
           MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              manager
           </AttributeValue>
           <AttributeDesignator MustBePresent="false"
               Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
               AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role"
               DataType="http://www.w3.org/2001/XMLSchema#string"/>
       </Match>
       <Match
           MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
              14:00
           </AttributeValue>
           <AttributeDesignator MustBePresent="true"
               Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
               AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
               DataType="http://www.w3.org/2001/XMLSchema#time"/>
       </Match>
     </AllOf>
    </AnyOf>
  </Target>
</Rule>
<Rule Effect="Permit" RuleId="R3">
  <Target>
   <AnyOf>
     <AllOf>
       <Match
           MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              employee
           </AttributeValue>
           <AttributeDesignator MustBePresent="false"
               Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
               AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role"
               DataType="http://www.w3.org/2001/XMLSchema#string"/>
       </Match>
     </AllOf>
     <AllOf>
       <Match
           MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              manager
           </AttributeValue>
           <AttributeDesignator MustBePresent="false"
              Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
              AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
```

```
        </Match>
       </AllOf>
      </AnyOf>
    </Target>
  </Rule>
  <Obligations>
    <Obligation FulfillOn="Permit" ObligationId="01" />
    <Obligation FulfillOn="Deny" ObligationId="02" />
  </Obligations>
</Policy>
<Policy PolicyId="P2"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-overrides">
  <Target />
  <Rule Effect="Permit" RuleId="R4">
    <Target>
     <AnyOf>
       <AllOf>
         <Match
             MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                manager
             </AttributeValue>
             <AttributeDesignator MustBePresent="false"
                 Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role"
                 DataType="http://www.w3.org/2001/XMLSchema#string"/>
         </Match>
         <Match
             MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                read
             </AttributeValue>
             <AttributeDesignator MustBePresent="true"
                 Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                 DataType="http://www.w3.org/2001/XMLSchema#string"/>
         </Match>
       </AllOf>
       <AllOf>
         <Match
             MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                employee
             </AttributeValue>
             <AttributeDesignator MustBePresent="true"
                 Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role"
                 DataType="http://www.w3.org/2001/XMLSchema#string"/>
         </Match>
         <Match
             MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                write
```

```
                </AttributeValue>
                <AttributeDesignator MustBePresent="true"
                    Category="urn:oasis:names:tc:xacml:3.0:attribute-category:action"
                    AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                    DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </Match>
          </AllOf>
        </AnyOf>
      </Target>
    </Rule>
    <Rule Effect="Permit" RuleId="R5">
      <Target>
       <AnyOf>
         <AllOf>
           <Match
               MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                  accountant
               </AttributeValue>
               <AttributeDesignator MustBePresent="false"
                   Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                   AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role"
                   DataType="http://www.w3.org/2001/XMLSchema#string"/>
           </Match>
           <Match
               MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
               <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
                  14:00
               </AttributeValue>
               <AttributeDesignator MustBePresent="true"
                  Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                  AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                  DataType="http://www.w3.org/2001/XMLSchema#time"/>
           </Match>
         </AllOf>
        </AnyOf>
      </Target>
    </Rule>
    <Obligations>
      <Obligation FulfillOn="Permit" ObligationId="03" />
      <Obligation FulfillOn="Deny" ObligationId="04" />
    </Obligations>
  </Policy>
  <Obligations>
    <Obligation FulfillOn="Permit" ObligationId="05" />
    <Obligation FulfillOn="Deny" ObligationId="06" />
  </Obligations>
</PolicySet>
```