Principles of Data Protection (2IMS25): Exam 1/11/2019

Questions

1. **(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,{Army, Navy})
Major	(MEDIUM,{Army, Navy})
Captain	(MEDIUM,{Navy})
Soldier	(LOW,{Army})

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 compute the cost of the overall defense (i.e., army and navy) units?

   (c) Can the colonel compute the cost of the overall defense (i.e., army and navy) units, after he has changed the cost of navy units?

   (d) Can the major change the cost of navy units, after the soldier has read it?

   (e) Can the captain change the number of army units?

   (f) Can the captain change the number of army units, after he has read the army position?

   (g) Can the soldier compute the position of the overall defense (i.e., army and fleet)?

   Justify your answer.

   Hint:

   - Changing an object requires 'write' rights over the object.
   - Computing requires 'read' rights over the (input) objects.

2. **(1.5 points)** Represent the DAC model using capability lists in UCON.

3. **(2 points)** RT

   (a) Explain (briefly) what trust negotiation is. In particular, mention (1) why it is needed (give a concrete example), and (2) how it could be carried out in RT.

   (b) Consider the following RT_0 policy.

   $A.t \longleftarrow A.t.s$
   $A.t \longleftarrow K.t \cap L.t$

   $K.t \longleftarrow C.$
   $K.t \longleftarrow D.$
   $K.t \longleftarrow E.$

   $L.t \longleftarrow D.$
   $L.t \longleftarrow E.$

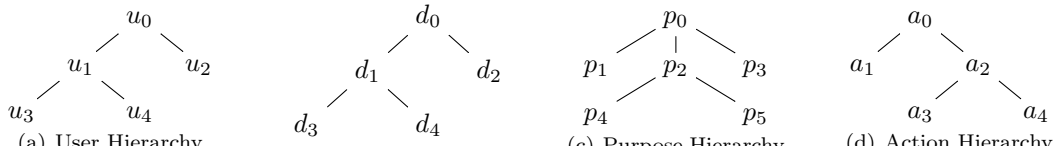
   $D.s \longleftarrow G.$
   $D.s \longleftarrow H.$

   $H.t \longleftarrow W.$
   $H.s \longleftarrow Z.$

   $Z.s \longleftarrow W$

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

4. **(1.5 points)** Let $Voc = (UH, DH, PH, AH, OM)$ be a vocabulary where the user hierarchy UH, data hierarchy DH, purpose hierarchy PH and action hierarchy AH are defined in Figure 1, and $OM = (O, \rightarrow)$ is the obligation model with $O = \{o_1, o_2, o_3, o_4, o_5, o_6\}$ and $\rightarrow = \{o_2 \rightarrow o_3, o_2 \rightarrow o_5, o_3 \rightarrow o_4\}$.



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

Figure 1: Hierarchies

Consider the following EPAL policies defined over Voc:

$$pol_1 = \begin{cases} \langle (u_0, d_1, p_0, a_2)(+, true, \{o_1\}) \rangle \\ \langle (u_1, d_0, p_2, a_2)(-, true, \{o_2\}) \rangle \\ \langle (u_2, d_4, p_4, a_0)(\circ, true, \{o_1\}) \rangle \\ \langle (u_1, d_0, p_1, a_2)(+, true, \{o_5\}) \rangle \\ \text{Default ruling:} - \\ \text{Default obligations:} \{o_4, o_5\} \end{cases}$$

$$pol_2 = \begin{cases} \langle (u_0, d_1, p_0, a_2)(+, true, \{o_1\}) \rangle \\ \langle (u_1, d_0, p_2, a_2)(-, true, \{o_2\}) \rangle \\ \langle (u_2, d_4, p_4, a_0)(\circ, true, \{o_1\}) \rangle \\ \langle (u_3, d_1, p_4, a_3)(+, true, \{o_6\}) \rangle \\ \langle (u_1, d_0, p_1, a_2)(+, true, \{o_5\}) \rangle \\ \text{Default ruling:} - \\ \text{Default obligations:} \{o_2\} \end{cases}$$

$$pol_3 = \begin{cases} \langle (u_0, d_1, p_0, a_2)(+, true, \{o_1\}) \rangle \\ \langle (u_1, d_0, p_2, a_2)(-, true, \{o_3\}) \rangle \\ \langle (u_2, d_4, p_4, a_0)(\circ, true, \{o_1\}) \rangle \\ \langle (u_1, d_0, p_1, a_2)(+, true, \{o_5\}) \rangle \\ \langle (u_0, d_0, p_0, a_0)(-, true, \{o_4, o_5\}) \rangle \\ \text{Default ruling:} + \\ \text{Default obligations:} \{o_4, o_5\} \end{cases}$$

Determine whether:

(a) pol_2 is a refinement of pol_1,

(b) pol_3 is a refinement of pol_1.

Justify your answer.

5. **(1.5 points)** Consider an operator α defined over the three-valued decision set $\mathcal{D}_3 = \{1, 0, \bot\}$ defined as follows:

α	1	0	$\bot$
1	1	1	$\bot$
0	1	0	0
$\bot$	$\bot$	0	$\bot$

(a) Define α over the seven-valued decision set $\mathcal{D}_7$ in point-wise way (Recall $\mathcal{D}_7 = \wp(\mathcal{D}_3) \setminus \emptyset$).

(b) Explain when a decision reduction is safe with respect to an operator.

(c) Let $\mathcal{D}_6 = \{P, D, NA, I(P), I(D), I(PD)\}$ be a six-valued decision set and $\rho_{76} : \mathcal{D}_7 \to \mathcal{D}_6$ a decision reduction that maps a decision in $\mathcal{D}_7$ to a decision in $\mathcal{D}_6$ such that:

$$\rho_{76}(d) = \begin{cases} P & \text{if } d = 1 \qquad I(P) \quad \text{if } d = \{1, \perp\} \\ D & \text{if } d = 0 \qquad I(D) \quad \text{if } d = \{0, \perp\} \\ NA & \text{if } d = \perp \qquad I(PD) \quad \text{if } d = \{1, 0\} \vee d = \{1, 0, \perp\} \end{cases}$$

Determine whether ρ_{76} is safe with respect to the operator α defined over $\mathcal{D}_7$.

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. Recall that rule evaluation and some combining algorithms are defined over the extended Indeterminate set ("Indeterminate(P)", "Indeterminate(D)", "Indeterminate(PD)"). Decisions in the extended Indeterminate set indicate the potential decision(s) (Permit or Deny) that would have returned if an error have not occurred in the evaluation.

Access Request

```
  <Request>
    <Attributes
         Category="urn:oasis:names:tc:xacml:1.0: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:2.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                doctor
            </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:resource-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                PatientRecord
            </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:2.0:policy:schema:os"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  PolicyCombiningAlgId="urn:oasis:names:tc:xacml:3.0:policy-combining-algorithm:deny-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">
               PatientRecord
           </AttributeValue>
           <AttributeDesignator
               MustBePresent="false"
               Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
               AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-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: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">
                radiology
             </AttributeValue>
             <AttributeDesignator MustBePresent="true"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:department"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </Match>
        </AllOf>
      </AnyOf>
    </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">
                   doctor
               </AttributeValue>
               <AttributeDesignator MustBePresent="false"
                   Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                   AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute: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="false"
                Category="urn:oasis:names:tc:xacml:1.0:subject-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="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">
                nurse
            </AttributeValue>
            <AttributeDesignator MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute: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="01" />
    <Obligation FulfillOn="Deny" ObligationId="02" />
  </Obligations>
</Policy>
<Policy PolicyId="P2"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:permit-overrides">
  <Target />
  <Rule Effect="Permit" RuleId="R3">
    <Target>
      <AnyOf>
        <AllOf>
          <Match
```

```
            MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
                15:00
            </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:authentication-time"
                DataType="http://www.w3.org/2001/XMLSchema#time"/>
         </Match>
         <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                doctor
            </AttributeValue>
            <AttributeDesignator MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute:role"
                DataType="http://www.w3.org/2001/XMLSchema#string"/>
         </Match>
       </AllOf>
     </AnyOf>
   </Target>
</Rule>
<Rule Effect="Deny" 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">
                doctor
            </AttributeValue>
            <AttributeDesignator MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute: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="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">
                  doctor
               </AttributeValue>
               <AttributeDesignator MustBePresent="false"
                  Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                  AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute: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="false"
                  Category="urn:oasis:names:tc:xacml:1.0:subject-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>
    <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>
```