Principles of Data Protection (2IMS25): Exam 25/1/2019

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 change the cost of army units?

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

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

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

(f) Can the captain change the number of navy units, after the soldier read it?

(g) Can the soldier change the cost of army units, after he read the cost of navy units?

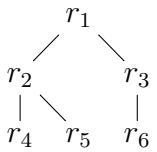
Justify your answer.

Hint:

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

2. **(1.5 points)** The following access matrix has been generate from an RBAC_1 policy with the given hierarchy and where C has role r_4. Give the minimal User-Assignment and Permission-Assignment corresponding to the given Access Matrix such that you do not assign anything that can be already derived otherwise.

	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8
A	×	×	×	×				×
B	×		×			×		
C	×		×		×		×	
D		×		×				×
E	×	×	×		×		×	
F		×						
G	×		×					



Hint: Users might have more than one role.

3. **(2 points)** RT

(a) Consider the following RT_0 policy.

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

$B.u \longleftarrow C$
$B.u \longleftarrow A.r$

$B.t \longleftarrow C.t$

$C.t \longleftarrow C$
$C.t \longleftarrow E$
$C.t \longleftarrow F$
$C.t \longleftarrow G$

$F.t \longleftarrow H$

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

(b) One of the characteristics of Trust Management is that "peers are not continuously available". Explain why this is so, and which impact this has on the language and the semantics of TM.

4. **(1.5 points)** Explain the steps (along with their goals) of the access decision making process in Purpose-based Access Control.

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

(a) Define α over a seven-valued decision set $\mathcal{D}_7$ point-wise (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

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

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. 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">
                Bob
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                employee
            </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">
                financialRecord
            </AttributeValue>
            <AttributeDesignator
                MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                AttributeId="urn:oasis:names:tc:xacml:1.0: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-unless-deny">
      <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">
                   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="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>
          </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">
             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: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="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">
              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>
    <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>
          </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:first-applicable">
  <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="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 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">
                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: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">
             manager
          </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">
             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: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>
    <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>
```