

Principles of Data Protection (2IMS25): Exam 30/10/2017

Questions

- (1.5 points)** Explain the safety problem in Harrison-Ruzzo-Ullman model. State under which condition(s) the safety problem is decidable.
- (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})
Captain	(MEDIUM, {Army, Navy})
Soldier	(LOW, {Army, 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:

- Draw the lattice of classifications.
- Can the colonel change the number of navy units?
- Can the colonel change the number of navy units, after he read the cost of navy units?
- Can the major change the number of army units, after the colonel read it?
- Can the major change the cost of army units, after he read the fleet position?
- Can the captain compute the cost of the overall defense (i.e., army and navy) units?
- Can the soldier read the number of navy units, after he modified it?

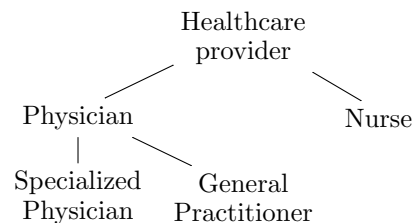
Justify your answer.

Hint:

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

- (1.5 points)** The following Access Matrix has been generate from an RBAC₁ policy with the given hierarchy and where Bob has role “Physician”. 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.

	Prescription	Medical History	Scan
Alice	read, write	read	read, insert
Bob	read	read	read
Charlie	read	write	
David	read	read	read, insert
Eve	read, write	read	read
Frank	read, write	read, write	read
Gill	read	read, write	read, insert



Hint: Users might have more than one role.

4. (2 points) RT

(a) Consider the following RT_0 policy:

$A.s \leftarrow A.t.u$

$A.t \leftarrow B.s$

$B.s \leftarrow B.t.u$

$B.t \leftarrow C.r$

$C.r \leftarrow A$

$C.r \leftarrow B$

$C.u \leftarrow J$

$B.u \leftarrow A$

$B.u \leftarrow D$

$B.u \leftarrow E$

$A.u \leftarrow A$

$D.u \leftarrow F$

$D.u \leftarrow G$

- Find all principals populating $A.s$ and $B.s$ (which means, compute $\llbracket A.s \rrbracket$ and $\llbracket B.s \rrbracket$).
- 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) Explain what is "attribute-based delegation", devise a situation in which it is useful and write an RT_0 policy describing the situation.

5. (1.5 points) Explain the steps (along with their goals) of the access decision making process in Purpose-based Access Control.

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/PolicySet 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: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">
        clerk
      </AttributeValue>
    </Attribute>
    <Attribute IncludeInResult="false"
      AttributeId="urn:oasis:names:tc:xacml:2.0: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:resource-id">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
        FinacialRecord
      </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">
        read
      </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">
              FinacialRecord
            </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:deny-overrides">
    <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">
                  manager
                </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">
                  15:00
                </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>
          <AllOf>
            <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                  clerk
                </AttributeValue>
              </Match>
            </AllOf>
          </AnyOf>
        </Target>
      <RuleEffect>Deny
    </Rule>
  </Policy>
</PolicySet>

```

```

    </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">
      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>
</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">
            accountant
          </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="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="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>
  <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:2.0:example:attribute: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 />
  <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">
              clerk
            </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">
              15:00
            </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>
        </AnyOf>
      </Target>
    </Rule>
  </Policy>

```

```

    </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">
              accountant
            </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>
    <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>

```