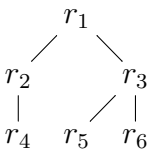
Principles of Data Protection (2IMS25): Exam 24/1/2020

Questions

1. **(1.5 points)** Explain the safety problem in Harrison-Ruzzo-Ullman model. State under which condition(s) the safety problem is decidable.

2. **(1.5 points)** The following access matrix has been generate from an RBAC_1 policy with the given hierarchy and where A has role r_6. 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) In Trust Management, one of most important requirements is that "attributes must have a precise semantics". Explain shortly (a) what this means, (b) why this is so important, and (c) give an example in which things go "wrong" due to the imprecision of the semantics.

   (b) Consider the following RT_0 policy.

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

   $K.t \longleftarrow A.t$

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

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

   $H.t \longleftarrow W$

   $H.s \longleftarrow Z$

   $Z.s \longleftarrow U$

   $Z.t \longleftarrow R$

   - 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)** Represent the Biba model with low-watermark for objects in UCON_{ABC}.

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/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:attribute-category:subject">
    <Attribute IncludeInResult="false"
      AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
         Charlie
      </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">
         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:function:string">
          <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:2.0: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">
               clerk
            </AttributeValue>
            <AttributeDesignator
              MustBePresent="true"
              Category="urn:oasis:names:tc:xacml:3.0:attribute-category: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 Effect="Permit" 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:3.0:attribute-category: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">
             9:00
          </AttributeValue>
          <AttributeDesignator
            MustBePresent="true"
            Category="urn:oasis:names:tc:xacml:3.0: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">
             clerk
          </AttributeValue>
          <AttributeDesignator
            MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category: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">
             9:00
          </AttributeValue>
          <AttributeDesignator
            MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:3.0: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: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">
           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="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:3.0:attribute-category:subject"
            AttributeId="urn:oasis:names:tc:xacml:2.0:example:attribute: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">
             accountant
          </AttributeValue>
          <AttributeDesignator
            MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category: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">
             manager
          </AttributeValue>
          <AttributeDesignator
            MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category: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">
             accountant
          </AttributeValue>
          <AttributeDesignator
            MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category: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="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">
            clerk
          </AttributeValue>
          <AttributeDesignator
            MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category: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">
               9:00
            </AttributeValue>
            <AttributeDesignator
              MustBePresent="true"
              Category="urn:oasis:names:tc:xacml:3.0: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>
```