Principles of Data Protection (2IMS25): Exam 26/10/2015

Questions

1. **(2 points)** Explain the safety problem in Harrison-Ruzzo-Ullman model. State under which condition(s) the safety problem is decidable.

2. **(2 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**
President	(HIGH,{Navy,Army})
Colonel	(MEDIUM,{Navy})
Major	(LOW,{Army,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 president change the cost of army units?

   (c) Can the president change the number of navy units, after the major read it?

   (d) Can the president change the position of army units, after he read the cost of navy unit?

   (e) Can the colonel change the number of navy units, after the president changed it?

   (f) Can the colonel read the number of army units?

   (g) Can the soldier change the army position?

   Justify your answer.

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

3. **(2 points)** Consider the following RT_0 policy.

   $A.t \longleftarrow B.t$
   $B.t \longleftarrow A.t$

   $C.t \longleftarrow C.r$
   $C.r \longleftarrow C.s$
   $C.r \longleftarrow Alice$
   $C.u \longleftarrow Bob$
   $C.s \longleftarrow Charlie$

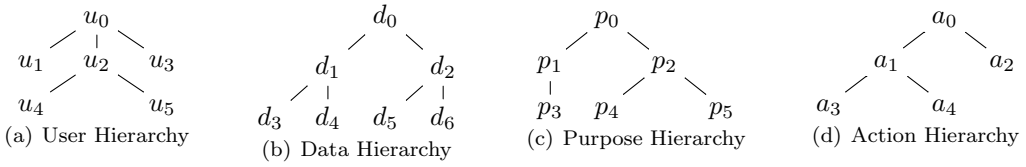
   $D.t \longleftarrow D.r.s$
   $D.t \longleftarrow C$
   $D.r \longleftarrow C$

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

4. **(1.5 points)** Explain the access decision making (i.e., purpose compliance and access purpose verification) in Purpose-based Access Control.

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.

$$pol = \begin{cases} \langle (u_2, d_1, p_0, a_1)(+, true, o_1) \rangle \\ \langle (u_0, d_2, p_2, a_0)(\circ, true, o_2) \rangle \\ \langle (u_4, d_0, p_4, a_4)(-, true, o_3) \rangle \\ \langle (u_2, d_2, p_0, a_1)(\circ, true, o_4) \rangle \\ \langle (u_0, d_0, p_5, a_1)(+, true, o_5) \rangle \\ \text{Default ruling:} + \\ \text{Default obligations:} \{o_6\} \end{cases}$$



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

Figure 1: Hierarchies

Evaluate the following access requests against *pol*:

$req_1 = (u_3, d_5, p_5, a_3)$
$req_2 = (u_2, d_4, p_1, a_0)$
$req_3 = (u_6, d_2, p_3, a_2)$
$req_4 = (u_4, d_3, p_2, a_3)$

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">
                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">
                accountant
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                manager
            </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:2.0:policy:schema:os"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-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:1.0:attribute-category:resourse"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:resourse:resourse-id"
                 DataType="http://www.w3.org/2001/XMLSchema#string"/>
           </Match>
          </AllOf>
        </AnyOf>
  </Target>
  <Policy PolicyId="P1"
      RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0: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">
                 manager
             </AttributeValue>
             <AttributeDesignator
                 MustBePresent="false"
                 Category="urn:oasis:names:tc:xacml:1.0: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: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>
            <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="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: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="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">
                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>
       </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: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:1.0: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>
       </AllOf>
     </AnyOf>
```

```
      <AnyOf>
        <AllOf>
          <Match
              MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">
                 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:authentication-time"
                  DataType="http://www.w3.org/2001/XMLSchema#time"/>
          </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: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>
       </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>
```