Distributed Trust Management: Exam 29/1/2014

Questions

1. **(1.5 points)** The Take-grant model is an access control model based on rules which describe changes in the access rights that subjects have over objects. These rules are:

   - *Take* rule allows a subject to take a right on an object from another subject.
   - *Grant* rule allows a subject to grant a right he has to another subject.
   - *Create* rule allows a subject to create a new object.
   - *Remove* rule allows a subject to remove a right it has on an object.

   Define an authorization system in Harrison-Ruzzo-Ullman model which simulates the Take-grant model. In particular, use the primitive operations provided by the Harrison-Ruzzo-Ullman model to define commands corresponding to the rules in the Take-grant model.

2. **(1 point)** Let TOP SECRET, SECRET, CONFIDENTIAL and UNCLASSIFIED be secrecy levels (ordered from the highest to the lowest). Let CRITICAL and NON CRITICAL 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 secrecy and integrity classes:

Subject	**Secrecy**	**Integrity**
President	(TOP SECRET,{Navy,Army})	(CRITICAL,{Navy,Army})
Colonel	(SECRET,{Army})	(NON CRITICAL,{Navy,Army})
Major	(CONFIDENTIAL,{Navy})	(NON CRITICAL,{Navy})
Soldier	(UNCLASSIFIED,{})	(NON CRITICAL,{Army})

Object	**Secrecy**	**Integrity**
Army position	(SECRET,{Army})	(CRITICAL,{Army})
Fleet position	(SECRET,{Navy})	(CRITICAL,{Navy})
Number of army units	(CONFIDENTIAL,{Army})	(CRITICAL,{Army})
Number of navy units	(CONFIDENTIAL,{Navy})	(CRITICAL,{Navy})
Cost of army units	(UNCLASSIFIED,{Army})	(NON CRITICAL,{Army})
Cost of navy units	(UNCLASSIFIED,{Navy})	(NON CRITICAL,{Navy})

   Answer the following questions based on the combination of the Bell-LaPadula model and Biba model:

   (a) Can the president compute the overall number of army and navy units?

   (b) Can the colonel compute the overall cost of army units?

   (c) Can the major modify the number of navy units?

   (d) Can the soldier change the army position?

   (e) Can the soldier change the fleet position?

   Justify your answer.

3. **(1.5 points)** Recall the definition of the RT_0 grammar. Consider the following RT_0 policy:

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

   $B.t \longleftarrow A$
   $B.t \longleftarrow B$
   $B.t \longleftarrow C$
   $B.t \longleftarrow D$

   $B.u \longleftarrow C$
   $B.u \longleftarrow D$

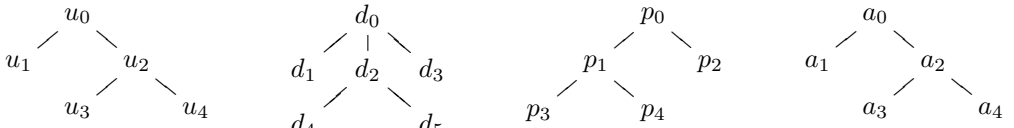
$B.u \longleftarrow E$

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

$C.t \longleftarrow F$

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

4. **(1.5 points)** Trust Negotiation.
   - Explain what is the reason why in some cases some form of trust negotiation is needed. Give an example.
   - Conceive and illustrate a practical example of trust negotiation.
5. **(1.5 points)** Represent the Biba model with low-water mark for subjects in the UCON model.
6. **(1.5 points)** Let the hierarchies in Figure 1 be user hierarchy, data hierarchy, purpose hierarchy and action hierarchy. Let $(O, \rightarrow)$ an obligation model with $O = \{o_1, o_2, o_3, o_4, o_5\}$ and $\rightarrow = \{o_1 \rightarrow o_2, o_1 \rightarrow o_3, o_4 \rightarrow o_5\}$.



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

Figure 1: Hierarchies

Consider the following EPAL policies:

$$pol_1 = \begin{cases} \langle (u_1, d_2, p_0, a_2)(+, true, \{o_1, o_4\}) \rangle \\ \langle (u_2, d_0, p_1, a_1)(\circ, true, \{o_4\}) \rangle \\ \langle (u_2, d_5, p_4, a_0)(-, true, \{o_1\}) \rangle \\ \langle (u_1, d_0, p_1, a_2)(+, true, \{o_5\}) \rangle \\ \text{Default ruling:}+ \\ \text{Default obligations:}\{o_2, o_4\} \end{cases}$$

$$pol_2 = \begin{cases} \langle (u_1, d_2, p_0, a_2)(+, true, \{o_2, o_4\}) \rangle \\ \langle (u_2, d_0, p_1, a_1)(\circ, true, \{o_4\}) \rangle \\ \langle (u_2, d_5, p_4, a_0)(-, true, \{o_1\}) \rangle \\ \langle (u_1, d_0, p_1, a_2)(+, true, \{o_5\}) \rangle \\ \langle (u_1, d_2, p_3, a_4)(+, true, \{o_1, o_4\}) \rangle \\ \text{Default ruling:}+ \\ \text{Default obligations:}\{o_2, o_4\} \end{cases}$$

$$pol_3 = \begin{cases} \langle (u_1, d_2, p_0, a_2)(+, true, \{o_1, o_4\}) \rangle \\ \langle (u_2, d_0, p_1, a_1)(\circ, true, \{o_4\}) \rangle \\ \langle (u_2, d_5, p_4, a_0)(-, true, \{o_1\}) \rangle \\ \langle (u_0, d_0, p_1, a_0)(+, true, \{o_1, o_4\}) \rangle \\ \langle (u_1, d_0, p_1, a_2)(+, true, \{o_5\}) \rangle \\ \langle (u_4, d_3, p_2, a_3)(-, true, \{o_3, o_4\}) \rangle \\ \text{Default ruling:}+ \\ \text{Default obligations:}\{o_2, o_4\} \end{cases}$$

Determine whether

(a) pol_2 is a refinement of pol_1,

(b) pol_3 is a refinement of pol_1.

Justify your answer.

7. **(1.5 points)** Given the XACML policy and access request below, determine the access response. **Hint:** If an attribute from the request context does not match the target of the Rule/Policy/PolicySet, then the attribute is considered missing. If the attribute is missing, 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">
                Alice
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                manager
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                clerk
            </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:esource-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">
                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:1.0: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">
                 financialRecord
             </AttributeValue>
             <AttributeDesignator
                 MustBePresent="false"
                 Category="urn:oasis:names:tc:xacml:1.0: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:1.0:rule-combining-algorithm:permit-overrides">
    <Target>
      <Target>
        <AnyOf>
          <AllOf>
           <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: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="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">
                  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">
               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>
      <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: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>
       </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">
               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">
```

```
                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="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: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: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="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">
               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">
               8:00
            </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">
               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>
    </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>
```