Distributed Trust Management: Assignment 2

Deadline: 8 January 2012
How to submit the assignment: – send a pdf file with the solution by email (n.zannone at tue dot nl)
For any question send me an email

Questions

1. Write the policy supporting the following scenario in UCON$_{preA_0preB_0onC_0}$.

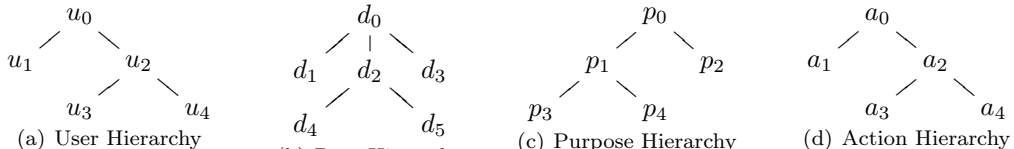
   A doctor can only access medical records of his patient. The doctor is authorized to access medical records during his turn at the hospital. Accesses are authorized only if the patient has given his informed consent. A doctor can access patient records without patient consent only in case of emergency.

2. Define the purpose hierarchy, role hierarchy, and access purpose authorizations in Purpose-based Access Control for the following scenario.

   A bank offers loans to its clients. The process of granting loans consists of checking customer financial credentials and calculating loan price and approving the loan. Any employee in the bank can access customer information for checking customer financial credentials. The price of a loan can be only calculated by manager or by a clerk with at least five years of experience. A loan can be approved only by a senior manager (i.e., a manager with at least three years of experience). However, in the case that no senior managers are present at the bank, the loan can be approved by a clerk with at least five years of experience.

3. Let *pol* be an EPAL policy and the hierarchies in Figure 1 be user hierarchy, data hierarchy, purpose hierarchy and action hierarchy, with

$$pol = \begin{cases} \langle (u_1, d_2, p_0, a_2)(+, true, o_1) \rangle \\ \langle (u_2, d_0, p_1, a_1)(\circ, true, o_2) \rangle \\ \langle (u_2, d_5, p_4, a_0)(-, true, o_3) \rangle \\ \langle (u_1, d_0, p_1, a_2)(+, true, o_4) \rangle \end{cases}$$



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

Figure 1: Hierarchies

   Evaluate the following access requests against *pol*:

   $req_1 = (u_1, d_3, p_1, a_4)$
   $req_2 = (u_3, d_3, p_2, a_3)$
   $req_3 = (u_4, d_2, p_1, a_1)$

4. Given the XACML policy and access request below, determine the access response. Justify the answer. Do the same exercise, in the case the effect of rule R3 is *Permit*.
   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 "Indeterminate".

Access Request

```
<Request>
 <Subject>
   <Attribute
        AttributeId="urn:oasis:names:tc:xacml:2.0:subject:subject-id"
        DataType="http://www.w3.org/2001/XMLSchema#anyURI">
     <AttributeValue>Bob</AttributeValue>
   </Attribute>
   <Attribute
        AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
        DataType="http://www.w3.org/2001/XMLSchema#anyURI">
     <AttributeValue>accountant</AttributeValue>
   </Attribute>
 </Subject>
 <Resource>
   <Attribute
       AttributeId="urn:oasis:names:tc:xacml:2.0:subject:resource-id"
       DataType="http://www.w3.org/2001/XMLSchema#anyURI">
     <AttributeValue>order</AttributeValue>
   </Attribute>
 </Resource>
 <Action>
   <Attribute
       AttributeId="urn:oasis:names:tc:xacml:2.0:subject:action-id"
       DataType="http://www.w3.org/2001/XMLSchema#string">
     <AttributeValue>modify</AttributeValue>
   </Attribute>
 </Action>
 <Environment/>
</Request>
```

Access Control Policy

```
<PolicySet
    xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
    PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides"
    PolicySetId="PS">
  <Target>
    <Resources>
      <Resource>
        <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue
              DataType="http://www.w3.org/2001/XMLSchema#string">order</AttributeValue>
          <ResourceAttributeDesignator
              AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
              DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true" />
        </ResourceMatch>
      </Resource>
    </Resources>
  </Target>
  <Policy
      PolicyId="P1"
      RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable">
    <Target />
    <Rule Effect="Permit" RuleId="R1">
      <Target>
        <Subjects>
          <Subject>
            <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue
                  DataType="http://www.w3.org/2001/XMLSchema#string">manager</AttributeValue>
              <SubjectAttributeDesignator
                  AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                  DataType="http://www.w3.org/2001/XMLSchema#string" />
            </SubjectMatch>
            <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue
                  DataType="http://www.w3.org/2001/XMLSchema#string">accountant</AttributeValue>
              <SubjectAttributeDesignator
                  AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                  DataType="http://www.w3.org/2001/XMLSchema#string" />
            </SubjectMatch>
          </Subject>
        </Subjects>
      </Target>
    </Rule>
    <Rule Effect="Deny" RuleId="R2">
      <Target>
        <Subjects>
          <Subject>
            <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue
                  DataType="http://www.w3.org/2001/XMLSchema#string">manager</AttributeValue>
              <SubjectAttributeDesignator
                  AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
```

```
                DataType="http://www.w3.org/2001/XMLSchema#string" />
          </SubjectMatch>
        </Subject>
        <Subject>
          <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#string">accountant</AttributeValue>
            <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                DataType="http://www.w3.org/2001/XMLSchema#string" />
          </SubjectMatch>
        </Subject>
      </Subjects>
    </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:permit-overrides">
  <Target>
    <Actions>
      <Action>
        <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue
              DataType="http://www.w3.org/2001/XMLSchema#string">modify</AttributeValue>
          <ActionAttributeDesignator
              AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
              DataType="http://www.w3.org/2001/XMLSchema#string" />
        </ActionMatch>
      </Action>
    </Actions>
  </Target>
  <Rule Effect="Deny" RuleId="R3">
    <Target>
      <Subjects>
        <Subject>
          <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#string">accountant</AttributeValue>
            <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                DataType="http://www.w3.org/2001/XMLSchema#string" />
          </SubjectMatch>
          <SubjectMatch
              MatchId="urn:oasis:names:tc:xacml:1.0:function:time-greater-than-or-equal">
            <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#time">17:00:00</AttributeValue>
            <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:1.0:subject:request-time"
                DataType="http://www.w3.org/2001/XMLSchema#time" MustBePresent="true" />
```

```
            </SubjectMatch>
          </Subject>
        </Subjects>
      </Target>
    </Rule>
    <Rule Effect="Deny" RuleId="R4">
      <Target>
        <Subjects>
          <Subject>
            <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue
                  DataType="http://www.w3.org/2001/XMLSchema#string">accountant</AttributeValue>
              <SubjectAttributeDesignator
                  AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                  DataType="http://www.w3.org/2001/XMLSchema#string" />
            </SubjectMatch>
          </Subject>
        </Subjects>
      </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>
```