Distributed Trust Management: Assignment 2

Deadline: 6 January 2014
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. **(Usage control)** Write a UCON policy supporting the following scenario.

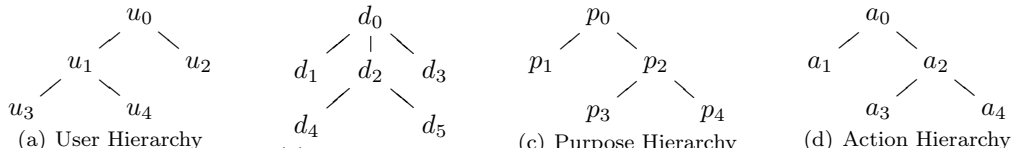
   The university provides a video lecture service which allows users to watch the recordings of the lectures given at the university. The service is freely available within the university network. Remote access to the video lecture service requires registering to the service. Registration has to be done only the first time a service is used. In addition, users have to pay 10$ per lecture (when they access the recordings remotely). However, access to recordings is free of charge for students enrolled at the university.

2. **(Purpose-based Access Control)** An online shop offers customers a number of services. Service provision consists of service selection, delivery and payment. The online shop accepts either bank transfer or credit card for payment. In addition, the online shop provides recommendations about new offers to its customers. A customer decide to buy some services from the online shop, but he does not want to receive recommendations. Also he prefers to pay using credit card.

   - Define the purpose hierarchy for the scenario above.
   - Define the intended purpose associated to the customer's information with respect to the customer's preferences.
   - Can an employee of the online shop access the customer's information for service provision? Justify the answer.

3. **(EPAL)** Let *pol* be an EPAL policy.

$$pol = \begin{cases} \langle (u_0, d_3, p_4, a_1)(-, true, o_1) \rangle \\ \langle (u_1, d_1, p_1, a_1)(+, true, o_2) \rangle \\ \langle (u_4, d_3, p_4, a_3)(-, true, o_3) \rangle \\ \langle (u_0, d_0, p_2, a_2)(\circ, true, o_4) \rangle \\ \langle (u_1, d_2, p_3, a_3)(+, true, o_5) \rangle \end{cases}$$



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

Figure 1: Hierarchies

   Given the user hierarchy, data hierarchy, purpose hierarchy and action hierarchy in Figure 1, evaluate the following access requests against *pol*:

$req_1 = (u_2, d_3, p_1, a_4)$
$req_2 = (u_0, d_1, p_3, a_4)$
$req_3 = (u_1, d_2, p_4, a_2)$
$req_4 = (u_3, d_1, p_3, a_1)$

4. **(XACML)** Given the XACML policy and access request below, determine the access response. Justify the answer.
   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>
 <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">
              Bob
          </AttributeValue>
       </Attribute>
       Attribute IncludeInResult="false"
          AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
              doctor
          </AttributeValue>
  </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">
              medRecord
          </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">
                 medRecord
             </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:first-applicable">
    <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="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">
                  nurse
               </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">
               08:00
            </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="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">
               receptionist
            </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="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">
               doctor
            </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:permit-overrides">
  <Target />
  <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">
                doctor
             </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="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">
                nurse
             </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">
                08:00
             </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>
  <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>
```