Principles of Data Protection: Assignment 2

Deadline: 5 January 2015
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)** Discuss the UCON model needed to specify a policy supporting the following scenario, and write the UCON policy in the identified model.

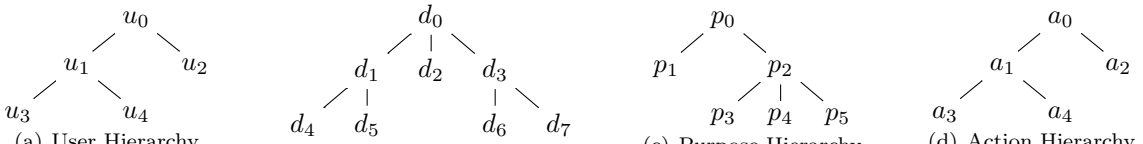
   A digital library offers access to a collection of articles to users affiliated with institutions that have subscribed to the digital library. In order to access the articles in the digital library, users affiliated with a subscribed institution have to authenticate using their institution credentials or to connect to the digital library using their institution's network. The digital library makes some information about the articles like authors, title and abstract, publicly available.

2. **(Purpose-based Access Control)** An online shop offers customers a number of services for which access to customers' information is required. The shop allows customers to buy products. The purchase process includes the verification of the payment and the delivery of the purchased products. The verification of the payment can be performed by employees in the financial department, who had worked at least three years in the financial department or have at least five years of experience as accountants. The delivery of the purchased products can be carried out by employees in the warehouse. In particular, this task can be performed by a manager or by a warehouse worker who has a certification to handle customer personal information. In addition, the purchase process includes an accountability step to determine whether the process has been executed properly. This accountability step can be performed by a manager in the financial department, who has at least 10 years of experience as an accountant. Moreover, the online shop provides recommendations about new products based on the customer preferences. Only employees with at least three years at the shop can access customers' information to provide recommendations.

   - Define purpose hierarchy and role hierarchy along with role attributes for the scenario above.
   - Define the access purpose authorizations for the scenario.
   - Determine whether an employee in the financial department and with ten years at the shop can request access to customer information for performing the purchase process. Justify the answer.

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

$$pol = \begin{cases} \langle (u_2, d_2, p_4, a_2)(-, true, \{o_1, o_2\}) \rangle \\ \langle (u_1, d_0, p_2, a_0)(\circ, true, \{o_3\}) \rangle \\ \langle (u_1, d_1, p_0, a_1)(+, true, \{o_2\}) \rangle \\ \langle (u_4, d_3, p_4, a_3)(-, true, \{o_3\}) \rangle \\ \langle (u_0, d_0, p_2, a_2)(\circ, true, \{o_4\}) \rangle \\ \langle (u_1, d_2, p_3, a_0)(+, true, \{o_5\}) \rangle \\ \text{Default ruling:} + \\ \text{Default obligations:} \{o_2, o_6\} \end{cases}$$



(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*:

$req_1 = (u_1, d_3, p_1, a_4)$
$req_2 = (u_0, d_2, p_4, a_0)$
$req_3 = (u_1, d_4, p_5, a_2)$
$req_4 = (u_3, d_7, p_3, a_1)$

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">
               Charlie
           </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 IncludeInResult="false"
           AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role">
           <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
               clerk
           </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">
               loan offer
           </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">
              make
          </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:only-one-applicable">
  <Target>
       <AnyOf>
          <AllOf>
           <Match
             MatchId="urn:oasis:names:tc:xacml:1.0:function:function:string">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 loan offer
             </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:3.0:rule-combining-algorithm:deny-unless-permit">
    <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">
                 make
             </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">
                  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">
               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="Permit" 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: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">
               09:00
            </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="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>
        </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">
                 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">
                 09:00
              </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="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: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">
                  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="03" />
      <Obligation FulfillOn="Deny" ObligationId="04" />
    </Obligations>
  </Policy>
  <Obligations>
    <Obligation FulfillOn="Permit" ObligationId="05" />
    <Obligation FulfillOn="Deny" ObligationId="06" />
  </Obligations>
</PolicySet>
```