Principles of Data Protection: Assignment 2

Deadline: 16 October 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 **Note:** The assignment should be done individually.

Questions

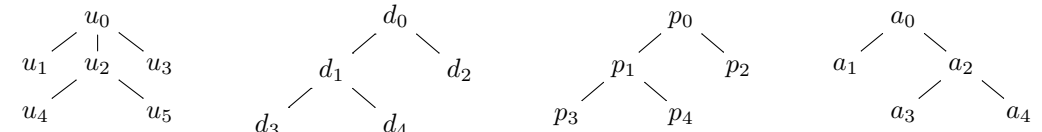
1. **(Usage control)** Discuss the UCON model needed to specify a policy supporting the following scenario, and write the UCON policy in the identified model.

   Doctors can access medical records to provide medical treatment to patients. However, access is authorized only during their turn at the hospital. Moreover, doctors can only access medical records of the patients they treat and only if the patient has given their informed consent. A doctor can only access medical records without patient consent only in case of emergency.

2. **(Purpose-based Access Control)** A bank offers loans to its clients. The loan process consists of three steps, namely checking customer financial credentials, calculating the loan price and approving the loan offer. Any bank employee with at least three year experience at the bank can access customer information for checking customer financial credentials. The price of a loan can be only computed by a manager or by a clerk with at least five year experience. A loan offer can be approved only by a senior manager (i.e., a manager with at least five year experience). However, in the case no senior managers are present at the bank, a loan offer can be approved by a clerk with at least ten year experience.

   - Define the purpose hierarchy and role hierarchy along with role attributes for the scenario above.
   - Define the access purpose authorizations for the scenario.
   - Determine whether a clerk with ten year experience can request access to customer information in order to execute the loan process (Assume a senior manager is present in the bank). Justify the answer.

3. **(EPAL)** 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:

$$pol_1 = \begin{cases} \langle (u_1, d_2, p_0, a_2)(+, true, \{o_1, o_3\}) \rangle \\ \langle (u_2, d_0, p_1, a_1)(\circ, true, \{o_3\}) \rangle \\ \langle (u_1, d_4, p_3, a_0)(-, true, \{o_1, o_2\}) \rangle \\ \langle (u_3, d_0, p_1, a_2)(+, true, \{o_4\}) \rangle \\ \text{Default ruling:} - \\ \text{Default obligations:} \{o_1, o_5\} \end{cases}$$

$$pol_2 = \begin{cases} \langle (u_1, d_2, p_0, a_2)(+, true, \{o_1\}) \rangle \\ \langle (u_2, d_0, p_1, a_1)(\circ, true, \{o_3\}) \rangle \\ \langle (u_1, d_4, p_3, a_0)(-, true, \{o_1, o_3\}) \rangle \\ \langle (u_3, d_0, p_1, a_2)(+, true, \{o_4\}) \rangle \\ \langle (u_2, d_0, p_1, a_0)(-, true, \{o_1, o_5\}) \rangle \\ \text{Default ruling:} + \\ \text{Default obligations:} \{o_2, o_4\} \end{cases}$$

Determine whether

(a) pol_2 is a refinement of pol_1,

(b) pol_1 is a refinement of pol_2.

Justify your answer.

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">
                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">
                radiologist
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                physician
            </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">
```

```
            MedicalRecord
         </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: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">
                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>
  <Policy PolicyId="P1"
      RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-unless-deny">
    <Target>
       <AnyOf>
          <AllOf>
           <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                MedicalRecord
            </AttributeValue>
            <AttributeDesignator
                MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:1.0:attribute-category:resource"
                AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-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">
                  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">
             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="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">
             physician
          </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">
             physician
          </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">
             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>
         </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="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">
                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>
       </AllOf>
       <AllOf>
         <Match
             MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                physician
             </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="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">
                radiologist
            </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">
               9:00
            </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="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">
               physician
            </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">
               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>
      </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>
```