Principles of Data Protection: Assignment 2

Deadline: 20 October 2016
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.

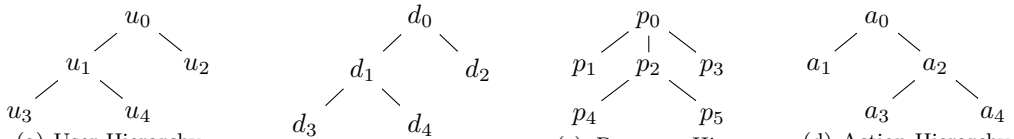
   A content provider offers an on-demand media streaming service. To access the service, users should subscribe to the service. The provider allows two types of subscription: Basic and Gold. Depending on the type of subscription, users can simultaneously connect a different number of devices to the provider's library of online content. In particular, the Basic subscription allows a user to connect one device whereas the Gold subscription allows a user to connect up to five devices. The service is offered only within the Netherlands.

   Hint: Model the subscription to the service using obligations.

2. **(Purpose-based Access Control)** The medical staff of a hospital (i.e., doctors and nurses) can read patients' medical records for providing medical treatment. A doctor can treat a patient if he has worked at least two years in the hospital or he has at least five years of experience. A nurse can only access medical records of those patients in his/her department. Administrative staff can access patient information for billing purposes. In addition, receptionists (who are part of the administrative staff) can access patients' demographic information and doctors' schedule for managing appointments. Administrative staff can only access patients' information within the hospital network.

   - Define the purpose hierarchy and role hierarchy along with role and system attributes for the scenario above.
   - Define the access purpose authorizations for the scenario.
   - Determine whether a receptionist with ten year experience can request access to the medical record of a patient in order to make an appointment (Assume the receptionist is within the hospital network). Justify the answer.

3. **(EPAL)** Let $Voc = (UH, DH, PH, AH, OM)$ be a vocabulary where the user hierarchy UH, data hierarchy DH, purpose hierarchy PH and action hierarchy AH are defined in Figure 1, and $OM = (O, \rightarrow)$ is the obligation model with $O = \{o_1, o_2, o_3, o_4, o_5, o_6\}$ and $\rightarrow = \{o_2 \rightarrow o_3, o_2 \rightarrow o_5, o_3 \rightarrow o_4\}$.



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

Figure 1: Hierarchies

Consider the following EPAL policies defined over Voc:

$$pol_1 = \begin{cases} \langle (u_0, d_1, p_0, a_2)(+, true, \{o_1\}) \rangle \\ \langle (u_1, d_0, p_2, a_2)(-, true, \{o_2\}) \rangle \\ \langle (u_2, d_4, p_4, a_0)(\circ, true, \{o_1\}) \rangle \\ \langle (u_1, d_0, p_1, a_2)(+, true, \{o_5\}) \rangle \\ \text{Default ruling:} - \\ \text{Default obligations:} \{o_4, o_5\} \end{cases}$$

$$pol_2 = \begin{cases} \langle (u_0, d_1, p_0, a_2)(+, true, \{o_1\}) \rangle \\ \langle (u_1, d_0, p_2, a_2)(-, true, \{o_2\}) \rangle \\ \langle (u_2, d_4, p_4, a_0)(\circ, true, \{o_1\}) \rangle \\ \langle (u_3, d_1, p_4, a_3)(+, true, \{o_6\}) \rangle \\ \langle (u_1, d_0, p_1, a_2)(+, true, \{o_5\}) \rangle \\ \text{Default ruling:} - \\ \text{Default obligations:} \{o_2\} \end{cases}$$

$$pol_3 = \begin{cases} \langle (u_0, d_1, p_0, a_2)(+, true, \{o_1\}) \rangle \\ \langle (u_1, d_0, p_2, a_2)(-, true, \{o_3\}) \rangle \\ \langle (u_2, d_4, p_4, a_0)(\circ, true, \{o_1\}) \rangle \\ \langle (u_1, d_0, p_1, a_2)(+, true, \{o_5\}) \rangle \\ \langle (u_0, d_0, p_0, a_0)(-, true, \{o_4, o_5\}) \rangle \\ \text{Default ruling:} + \\ \text{Default obligations:} \{o_4, o_5\} \end{cases}$$

Determine whether:

(a) pol_2 is a refinement of pol_1,

(b) pol_3 is a refinement of pol_1.

Justify your answer.

4. **(XACML)** Given the XACML policy and access request below, determine the access response.

   Hint: If an attribute is missing (i.e., it is not provided in the request), 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:attribute-category: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:2.0:subject:role">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
        clerk
      </AttributeValue>
    </Attribute>
    <Attribute IncludeInResult="false"
      AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
        accountant
      </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">
        finacialRecord
      </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">
        write
      </AttributeValue>
    </Attribute>
  </Attributes>
</Request>
```

```
<PolicySet PolicySetId="PS"
  xmlns="urn:oasis:names:tc:xacml:3.0:policy:schema:os"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  PolicyCombiningAlgId="urn:oasis:names:tc:xacml:3.0: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">
            finacialRecord
          </AttributeValue>
          <AttributeDesignator
            MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:3.0: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>
  <Policy PolicyId="P1"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:2.0:rule-combining-algorithm:first-applicable">
    <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="true"
              Category="urn:oasis:names:tc:xacml:3.0:attribute-category: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 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:3.0:attribute-category: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:3.0: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">
              clerk
            </AttributeValue>
            <AttributeDesignator
              MustBePresent="false"
              Category="urn:oasis:names:tc:xacml:3.0:attribute-category: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="false"
              Category="urn:oasis:names:tc:xacml:3.0: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="01" />
    <Obligation FulfillOn="Deny" ObligationId="02" />
  </Obligations>
</Policy>
<Policy PolicyId="P2"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-overrides">
  <Target>
```

```
  <AnyOf>
    <AllOf>
      <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="true"
          Category="urn:oasis:names:tc:xacml:3.0: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="Pemit" 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:3.0:attribute-category: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:3.0:attribute-category: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="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:3.0:attribute-category: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:3.0:attribute-category: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">
            clerk
          </AttributeValue>
          <AttributeDesignator
            MustBePresent="false"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category: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:3.0: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>
```