Principles of Data Protection (2IS27): Exam 28/1/2015

Questions

1. **(1.5 points)** Recall the HUR model.

   (a) Compute the access matrix that results from the following initial state

	Process 1	File 1	File 2
Alice			
Bob	own		own
Charlie		own	
David			
Process1		read	

   by executing the sequence of commands α defined as follows:

1	$CREATE(Alice, Process2)$	11	$CREATE(Alice, File3)$
2	$CONFER_{*read}(Alice, Process2, File1)$	12	$CONFER_{*write}(Alice, Bob, File3)$
3	$CONFER_{exec}(Alice, Charlie, Process2)$	13	$TRANSFER_{read}(Alice, David, File1)$
4	$CONFER_{exec}(Alice, Charlie, Process1)$	14	$TRANSFER_{write}(Alice, David, File1)$
5	$CONFER_{read}(Bob, Charlie, File2)$	15	$TRANSFER_{write}(Bob, Process1, File3)$
6	$CONFER_{*read}(Bob, Alice, File1)$	16	$REVOKE_{exec}(Alice, Charlie, Process2)$
7	$TRANSFER_{read}(Process1, David, File1)$	17	$REVOKE_{write}(Bob, Bob, File3)$
8	$CONFER_{*read}(Alice, David, File2)$	18	$TRANSFER_{write}(Bob, David, File3)$
9	$REVOKE_{read}(Charlie, David, File1)$	19	$REVOKE_{exec}(Alice, Charlie, Process1)$
10	$REVOKE_{read}(Charlie, Alice, File1)$	20	$CONFER_{exec}(Process1, Charlie, Process1)$

   Hints:

   - Treat processes as subjects.
   - Command $CONFER_{*read}$ is equal to $CONFER_{read}$ but grants $*read$ instead of $read$. Similarly, $CONFER_{*write}$ is equal to $CONFER_{write}$ but grants $*write$ instead of $write$.
   - Command $REVOKE_{read}$ removes both $read$ and $*read$. Similar principle applies to $REVOKE_{exec}$ and $REVOKE_{write}$.

   (b) Is α leaking access privileges? (Consider only David to be untrusted) Justify the answer.

2. **(2 points)** Consider the following situation. Consider the following RT_0 Policy.

   $A.s \longleftarrow B.s \cap D.t$
   $B.s \longleftarrow B.s.t$
   $B.s \longleftarrow B.t$

   $B.t \longleftarrow A$
   $B.t \longleftarrow B$
   $B.t \longleftarrow C$
   $B.t \longleftarrow D$

   $B.u \longleftarrow C$
   $B.u \longleftarrow D$
   $B.u \longleftarrow E$

   $D.t \longleftarrow E$
   $D.t \longleftarrow C$

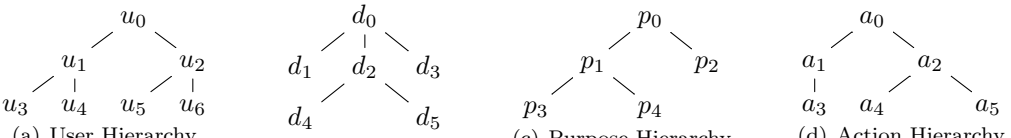
   $C.t \longleftarrow F$

   Find all principals populating $A.s$, and $B.s$ (which means, compute $[[A.s]]$ and $[[B.s]]$). Write down the graph generated by the top-down algorithm when computing the semantics of $A.s$. (the top-down algorithm is also known as the "backward algorithm").

3. **(1.5 points)** Explain briefly how the concept of risk plays a role in reputation-based trust management and rule-based trust management.

4. **(1.5 points)** Let *pol* be an EPAL policy and the hierarchies in Figure 1 the user hierarchy, data hierarchy, purpose hierarchy and action hierarchy.

$$pol = \begin{cases} \langle (u_2, d_3, p_0, a_1)(+, true, o_1) \rangle \\ \langle (u_1, d_3, p_2, a_2)(\circ, true, o_2) \rangle \\ \langle (u_4, d_0, p_4, a_4)(-, true, o_3) \rangle \\ \langle (u_0, d_2, p_0, a_1)(\circ, true, o_4) \rangle \\ \langle (u_1, d_0, p_3, a_0)(+, true, o_5) \rangle \\ \text{Default ruling:} + \\ \text{Default obligations:} \{o_6\} \end{cases}$$



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

Figure 1: Hierarchies

Evaluate the following access requests against *pol*:

$req_1 = (u_3, d_5, p_1, a_3)$
$req_2 = (u_2, d_4, p_1, a_0)$
$req_3 = (u_4, d_3, p_2, a_3)$
$req_4 = (u_6, d_2, p_3, a_2)$

5. **(1.5 points)** Consider an operator α defined over the three-valued decision set $\mathcal{D}_3 = \{1, 0, \perp\}$ defined as follows:

α	1	0	$\perp$
1	$\perp$	$\perp$	1
0	$\perp$	$\perp$	0
$\perp$	1	0	$\perp$

   (a) Define α over a seven-valued decision set $\mathcal{D}_7$ point-wise (Recall $\mathcal{D}_7 = \wp(\mathcal{D}_3) \setminus \emptyset$).

   (b) Explain when a decision reduction is safe with respect to an operator.

   (c) Let $\mathcal{D}_6 = \{P, D, NA, I(P), I(D), I(PD)\}$ be a six-valued decision set and $\rho_{76} : \mathcal{D}_7 \to \mathcal{D}_6$ be a decision reduction that maps a decision in $\mathcal{D}_7$ to a decision in $\mathcal{D}_6$ such that

$$\rho_{76}(d) = \begin{cases} P & \text{if } d = 1 \quad I(P) \quad \text{if } d = \{1, \perp\} \\ D & \text{if } d = 0 \quad I(D) \quad \text{if } d = \{0, \perp\} \\ NA & \text{if } d = \perp \quad I(PD) \quad \text{if } d = \{1, 0\} \vee d = \{1, 0, \perp\} \end{cases}$$

   Determine whether ρ_{76} is safe with respect to the operator α defined over $\mathcal{D}_7$.

6. **(2 points)** Given the XACML policy and access request below, determine the access response.
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 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: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>
```