Principles of Data Protection (2IMS25): Exam 27/1/2016

Questions

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

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

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

   by executing the sequence of commands α defined as follows:

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

   Hints:

   - Command $CONFER_{*read}$ is equal to $CONFER_{read}$ but grants $*read$ instead of $read$. Similar principle applies to $CONFER_{*exec}$ and $CONFER_{*write}$.
   - 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. **(1.5 points)** Recall the definition of RT_0.

   - *Simple Member*: $A.r \longleftarrow D$ With this statement A asserts that D is a member of $A.r$.
   - *Simple Inclusion*: $A.r \longleftarrow B.r_1$: With this statement A asserts that $A.r$ includes (all members of) $B.r_1$. This represents a delegation from A to B, as B may add principals to become members of the role $A.r$ by issuing statements defining $B.r_1$.
   - *Linking Inclusion*: $A.r \longleftarrow A.r_1.r_2$. With this statement A asserts that $A.r$ includes $B.r_2$ for every B that is a member of $A.r_1$.
   - *Intersection Inclusion*: $A.r \longleftarrow B_1.r_1 \cap B_2.r_2$ With this statement A asserts that $A.r$ includes every principal who is a member of both $B_1.r_1$ and $B_2.r_2$.

   Write an RT_0 model of the following situation: We have a school ALPHA and a company BETA. BETA has three subsidiaries BETA1, BETA2 and BETA3, defined by the following rules

```
BETA.sub <- BETA1
BETA.sub <- BETA2
BETA.sub <- BETA3
```

   Each of the subsidiaries has a list of its own employees.

```
BETA1.employee <- Sandro
BETA1.employee <- . . .
. . .
BETA2.employee <- . . .
. . .
BETA3.employee <- . . .
```

Also ALPA has subsidiaries, though more than 3: ALPHA1, ALPHA2, ALPHA3, ALPHA4, ...

```
ALPHA.sub <- ALPHA1
ALPHA.sub <- ALPHA2
. . .
```

And each subsidiary keeps track of its own graduated students.

```
ALPHA1.graduated <- Tom
ALPHA1.graduated <- John
. . .
ALPHA9.graduated <- . . .
```

BETA now wants to define centrally a role BETA.studied such that $[\![\text{BETA.studied}]\!]$ contains all employees at one of BETA subsidiaries who have graduated at one of ALPHA subsidiaries. Your task is to define the rules defining it using the grammar above. Note: you may define rules both for ALPHA and BETA.

3. **(2 points)** Consider the following RT_0 policy.

   $C.t \longleftarrow C.r.s$
   $C.r \longleftarrow C.u$
   $C.r \longleftarrow A$
   $C.u \longleftarrow B$
   $A.s \longleftarrow D$
   $C.s \longleftarrow E$
   $B.s \longleftarrow C$

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

4. **(1.5 points)** Write a UCON policy supporting the following scenario.

   A content provider offers an on-demand media streaming service. In order 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 Europe.

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

α	1	0	$\bot$
1	1	$\bot$	1
0	$\bot$	0	0
$\bot$	1	0	0

   (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 $\rho_{76} : \mathcal{D}_7 \to \mathcal{D}_6$ 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 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: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">
                physician
            </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>
    </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-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                patientRecord
            </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: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">
                 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-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 />
    <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">
                  cardiologist
               </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: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">
                  14:00
               </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">
              physician
           </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: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">
              14:00
           </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="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">
              radiologist
           </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: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">
              14:00
           </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="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 />
  <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">
                physician
             </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: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">
                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>
       <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="true"
                 Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:subject: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">
                read
             </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>
    <Rule Effect="Deny" 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:1.0:subject: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">
                 read
              </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>
    <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>
```