Principles of Data Protection (2IMS25): Exam 4/11/2016

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	File 3
Alice	own		*write
Bob		*read	
Charlie		own	own
David			

   by executing the sequence of commands α defined as follows:

1	$TRANSFER_{write}(Alice, Bob, File1)$	11	$REVOKE_{read}(Bob, Charlie, File4)$
2	$CONFER_{*read}(Charlie, Alice, File2)$	12	$CONFER_{*write}(Bob, Alice, File4)$
3	$CONFER_{exec}(Alice, Charlie, File1)$	13	$REVOKE_{read}(Charlie, Bob, File2)$
4	$CREATE(Bob, File1)$	14	$REVOKE_{write}(Charlie, Alice, File4)$
5	$CONFER_{*read}(Bob, Charlie, File1)$	15	$TRANSFER_{read}(Bob, David, File2)$
6	$TRANSFER_{read}(Charlie, David, File1)$	16	$TRANSFER_{read}(Charlie, David, File4)$
7	$REVOKE_{read}(Alice, David, File1)$	17	$REVOKE_{write}(Alice, Alice, File3)$
8	$CREATE(Bob, File4)$	18	$TRANSFER_{write}(Alice, David, File3)$
9	$CONFER_{*read}(Bob, Charlie, File4)$	19	$TRANSFER_{write}(Alice, Bob, File3)$
10	$TRANSFER_{read}(Charlie, Alice, File4)$	20	$REVOKE_{write}(Charlie, Alice, File3)$

   Hints:

   - 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. **(1.5 points)** Represent the Biba model with low-water mark for objects in UCON.

3. **(2 points)** RT

   (a) Consider the following RT_0 policy:

   $A.s \longleftarrow A.t.u$
   $A.t \longleftarrow B.t$

   $A.t \longleftarrow G$

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

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

   $C.t \longleftarrow F$

   - Find all principals populating $A.s$ (which means, compute $[\![A.s]\!]$).
   - 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".)

(b) Give three examples of credentials that may not be disclosed just to anyone (i.e., they should remain private as much as possible).

(c) Conceive a situation in which you have to disclose a private credential; how do you go about it according to what we discussed in the lectures?

4. **(1.5 points)** EPAL

(a) Explain the notion of policy refinement in EPAL and give a scenario in which policy refinement is needed.

(b) Describe the main steps of the scope-based policy comparison algorithm for policy refinement.

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	$\bot$

(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

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

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:1.0: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: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">
                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:3.0:policy-combining-algorithm:deny-unless-permit">
  <Target>
       <AnyOf>
          <AllOf>
           <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="false"
                 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>
  <Policy PolicyId="P1"
    RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:permit-overrides">
    <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">
                  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">
                  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">
               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="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">
               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">
               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="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="true"
                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: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">
                 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>
     </AnyOf>
     <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>
        </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">
                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">
                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>
      </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>
```