Principles of Data Protection (2IMS25): Exam 22/1/2018

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			
Bob		own	own
Charlie	own	*read	
David			

   by executing the sequence of commands α defined as follows:

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

   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)**

   (a) Explain the difference between Access Control Lists (ACLs) and Capability lists, and their advantages over storing permissions using an Access matrix.

   (b) Represent an access control policy using Capability lists in UCON.

3. **(1.5 points)** Differentiate between static separation of duty (SSoD) and dynamic separation of duty (DSoD) constraints. Consider constraints $smer(\{r_1, r_2, r_3\}, 3)$ and $dmer(\{r_1, r_2, r_3\}, 3)$. What are the implications of having both these constraints enforced simultaneously?

4. **(2 points)** RT

   (a) Consider the following RT_0 policy.

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

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

   $D.s \longleftarrow G.$
   $D.s \longleftarrow H.$

$D.s \longleftarrow I.$

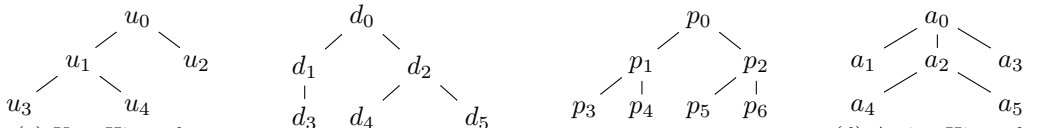
$H.t \longleftarrow W.$
$H.u \longleftarrow X.$
$H.s \longleftarrow Z.$

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

(b) Indicate shortly what are the main differences between (rule-based) Trust Management and classical Access Control (max 300 words).

5. **(1.5 points)** Let *pol* be an EPAL policy defined over a vocabulary *Voc* where *Voc* consists of the user, data, purpose and action hierarchies in Figure 1.

$$pol = \begin{cases} \langle (u_1, d_2, p_1, a_0)(\circ, true, o_1) \rangle \\ \langle (u_1, d_1, p_2, a_2)(+, true, o_2) \rangle \\ \langle (u_1, d_0, p_0, a_2)(\circ, true, o_3) \rangle \\ \langle (u_4, d_2, p_4, a_4)(-, true, o_4) \rangle \\ \langle (u_2, d_1, p_2, a_2)(+, true, o_5) \rangle \\ \text{Default ruling:} - \\ \text{Default obligations:} \{o_6\} \end{cases}$$



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

Figure 1: Hierarchies

Evaluate the following access requests against *pol*:

$req_1 = (u_3, d_5, p_1, a_2)$
$req_2 = (u_4, d_3, p_6, a_3)$
$req_3 = (u_2, d_6, p_2, a_4)$
$req_4 = (u_2, d_3, p_6, a_5)$

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">
                Charlie
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                manager
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                employee
            </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">
                financialRecord
            </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: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">
                financialRecord
            </AttributeValue>
            <AttributeDesignator
                MustBePresent="false"
                Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
                AttributeId="urn:oasis:names:tc:xacml:1.0:resource-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: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">
                  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 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">
                   accountant
                </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: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>
    <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">
                 manager
              </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>
    <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:permit-overrides">
  <Target />
  <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">
            employee
          </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>
      </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:1.0:subject: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">
              manager
          </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">
             manager
          </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="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">
             employee
          </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>
    <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>
```