Principles of Data Protection (2IMS25): Exam 2/11/2018

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	own		
Bob		*read	own
Charlie		own	
David			

   by executing the sequence of commands α defined as follows:

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

   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)** Chinese Wall

   (a) Explain the goal of the Chinese Wall model and describe the main concepts and properties of the model.

   (b) Explain the main differences between the Chinese Wall model and the Bell-LaPadula model.

3. **(1.5 points)** Represent RBAC_1 in UCON_{ABC}.

4. **(2 points)** RT

   (a) Explain what are the differences and similarities of the following three systems:

   - Role-based access control
   - Role-based Trust management
   - Reputation systems

   (Max 500 words, use concrete examples)

   (b) Recall the definition of RT_0.

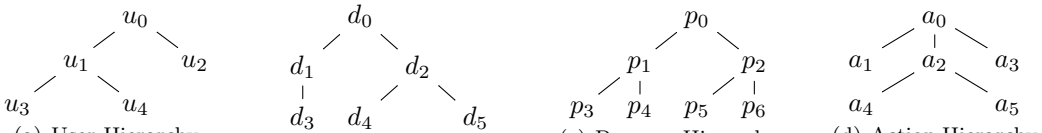
   - *Simple Member*: $A.r \longleftarrow D$. With this statement A asserts that D is a member of $A.r$.
   - *Simple Inclusion*: $A.r \longleftarrow B.r_1$. With this statement A asserts that $A.r$ includes (all members of) $B.r_1$. This represents a delegation from A to B, as B may add principals to become 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 $B_2.r_2$.

Explain what is attribute-based delegation, and how it can be implemented in a concrete RT_0 policy. Give a concrete meaningful example.

5. **(1.5 points)** Let *pol* be an EPAL policy defined over the user hierarchy, data hierarchy, purpose hierarchy and action hierarchy in Figure 1.

$$pol = \begin{cases} \langle (u_2, d_1, p_2, a_0)(\circ, true, o_1) \rangle \\ \langle (u_1, d_2, p_2, a_2)(+, true, o_2) \rangle \\ \langle (u_4, d_0, p_4, a_4)(-, true, o_3) \rangle \\ \langle (u_0, d_2, p_0, a_2)(\circ, true, o_4) \rangle \\ \langle (u_2, d_0, p_1, a_0)(-, true, o_5) \rangle \\ \text{Default ruling:+} \\ \text{Default obligations:} \{o_6\} \end{cases}$$



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

Figure 1: Hierarchies

Evaluate the following access requests against *pol*:

$req_1 = (u_3, d_5, p_1, a_3)$
$req_2 = (u_2, d_4, p_4, a_4)$
$req_3 = (u_0, d_3, p_1, a_2)$
$req_4 = (u_2, d_3, p_3, a_2)$

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">
                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">
                manager
            </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: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-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">
                 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:3.0:rule-combining-algorithm:permit-overrides">
    <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">
                   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:string-equal">
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                   write
                </AttributeValue>
                <AttributeDesignator MustBePresent="false"
                   Category="urn:oasis:names:tc:xacml:1.0:subject-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="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: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">
               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>
        <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">
               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="Deny" RuleId="R3">
    <Target>
     <AnyOf>
       <AllOf>
         <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>
         <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>
    </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:first-applicable">
  <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">
               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">
               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="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">
                 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>
          <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:1.0:subject-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>
```