Distributed Trust Management; Exam 3/2/2012

Questions

1. **(1.5 points)** Consider the access matrix of HRU model.

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

	File 1	File 2	File 3
Alice	own	own	
Bob	read		own
Charlie	read		write

   by executing the sequence of commands α defined as follows:

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

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

2. **(1 points)** Describe the main differences between the Bell-LaPadula model and the Chinese Wall model.

3. **(1.5 points)** Define a $RBAC_3$ system to regulate a review system of a conference. The system should implement (at least) the following requirements:

   (a) An author can submit a paper to the conference.

   (b) An author can only access her submissions.

   (c) A conference has a Program Committee (PC) which is in charge of reviewing the submitted papers.

   (d) Each paper should be reviewed by at least three PC members.

   (e) Authors may be PC members. (Note that an author may not be PC members.)

   (f) However, authors cannot review their own papers.

   (g) The (final) decision about the acceptance of a paper is made by the PC Chairs.

   (h) There are at most two PC Chairs, who are PC members.

   (i) The PC Chairs cannot submit a paper to the conference.

4. **(1.5 points)** Consider the following RT_0 Policy.
   $A.r \longleftarrow A.s.t$
   $A.s \longleftarrow A.r$
   $A.s \longleftarrow B.t$
   $B.t \longleftarrow C$
   $B.t \longleftarrow D$
   $B.t \longleftarrow E$
   $C.t \longleftarrow B$
   $C.t \longleftarrow F$
   Assume that the top level query is "find all principals populating $A.r$" (which means, compute $[[A.r]]$).

   - Write down the graph generated by the top-down algorithm when computing the semantics of $A.r$. (the top-down algorithm is also known as the "backward algorithm").
   - Is RT_0 "monotonic"? (you should know the meaning of the word).
     - If the answer is yes: give an example of a policy (in plain English words) that cannot be written in RT_0 because of the fact that RT_0 is monotonic.
     - If the answer is no: give an example of a non-monotonic policy in RT_0.
   - Where are credential stored in RT_0? Is the computation algorithm of RT_0 centralized or distributed? Are RT_0 credentials kept confidential during the execution of the top-down algorithm?

5. **(1 point)** Describe the access purpose verification in Purpose-based Access Control.

6. **(1.5 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 "Indeterminate".

7. **(1 point)** Describe how $RBAC_1$ is implemented in the RBAC profile of XACML.

Access Request

```
  <Request>
    <Subject>
      <Attribute
          AttributeId="urn:oasis:names:tc:xacml:2.0:subject:subject-id"
          DataType="http://www.w3.org/2001/XMLSchema#anyURI">
        <AttributeValue>
            John
        </AttributeValue>
      </Attribute>
      <Attribute
          AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
          DataType="http://www.w3.org/2001/XMLSchema#anyURI">
        <AttributeValue>
            clerk
        </AttributeValue>
      </Attribute>
      <Attribute
          AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
          DataType="http://www.w3.org/2001/XMLSchema#anyURI">
        <AttributeValue>
            accountant
        </AttributeValue>
      </Attribute>
     </Subject>
     <Resource>
      <Attribute
          AttributeId="urn:oasis:names:tc:xacml:2.0:subject:resource-id"
          DataType="http://www.w3.org/2001/XMLSchema#anyURI">
        <AttributeValue>
           record
        </AttributeValue>
      </Attribute>
    </Resource>
    <Action>
      <Attribute
         AttributeId="urn:oasis:names:tc:xacml:2.0:subject:action-id"
         DataType="http://www.w3.org/2001/XMLSchema#string">
       <AttributeValue>
           read
       </AttributeValue>
      </Attribute>
    </Action>
    <Environment/>
  </Request>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<PolicySet 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"
     PolicySetId="PS">
  <Target>
    <Actions>
      <Action>
        <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">read</AttributeValue>
          <ActionAttributeDesignator
                      AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                      DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true" />
        </ActionMatch>
      </Action>
    </Actions>
  </Target>
  <Policy PolicyId="P1"
          RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable">
    <Target>
      <Subjects>
        <Subject>
          <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">clerk</AttributeValue>
            <SubjectAttributeDesignator
                      AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                      DataType="http://www.w3.org/2001/XMLSchema#string" />
          </SubjectMatch>
        </Subject>
      </Subjects>
      <Resources>
        <Resource>
          <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">record</AttributeValue>
            <ResourceAttributeDesignator
                      AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
                      DataType="http://www.w3.org/2001/XMLSchema#string" />
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
    <Rule Effect="Deny" RuleId="R1">
      <Target>
        <Subjects>
          <Subject>
            <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">clerk</AttributeValue>
              <SubjectAttributeDesignator
                     AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                     DataType="http://www.w3.org/2001/XMLSchema#string" />
            </SubjectMatch>
```

```
        </Subject>
      </Subjects>
      <Actions>
        <Action>
          <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">write</AttributeValue>
            <ActionAttributeDesignator
                   AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                   DataType="http://www.w3.org/2001/XMLSchema#string" />
          </ActionMatch>
        </Action>
      </Actions>
    </Target>
  </Rule>
  <Rule Effect="Permit" RuleId="R2">
    <Target>
      <Subjects>
        <Subject>
          <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">clerk</AttributeValue>
            <SubjectAttributeDesignator
                   AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                   DataType="http://www.w3.org/2001/XMLSchema#string" />
          </SubjectMatch>
        </Subject>
        <Subject>
          <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">manager</AttributeValue>
            <SubjectAttributeDesignator
                   AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                   DataType="http://www.w3.org/2001/XMLSchema#string" />
          </SubjectMatch>
        </Subject>
      </Subjects>
    </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="Permit" RuleId="R3">
    <Target>
      <Subjects>
        <Subject>
          <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">clerk</AttributeValue>
            <SubjectAttributeDesignator
```

```
                AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                DataType="http://www.w3.org/2001/XMLSchema#string" />
        </SubjectMatch>
        <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">manager</AttributeValue>
          <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                DataType="http://www.w3.org/2001/XMLSchema#string" />
        </SubjectMatch>
      </Subject>
    </Subjects>
  </Target>
</Rule>
<Rule Effect="Permit" RuleId="R4">
  <Target>
    <Subjects>
      <Subject>
        <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">clerk</AttributeValue>
          <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                DataType="http://www.w3.org/2001/XMLSchema#string" />
        </SubjectMatch>
        <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">accountant</AttributeValue>
          <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                DataType="http://www.w3.org/2001/XMLSchema#string" />
        </SubjectMatch>
        <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:time-less-than-or-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#time">08:00</AttributeValue>
          <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
                DataType="http://www.w3.org/2001/XMLSchema#time" MustBePresent="true" />
        </SubjectMatch>
      </Subject>
    </Subjects>
  </Target>
</Rule>
<Rule Effect="Deny" RuleId="R5">
  <Target>
    <Subjects>
      <Subject>
        <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">accountant</AttributeValue>
          <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
                DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true" />
        </SubjectMatch>
      </Subject>
    </Subjects>
```

```
      </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>
```