Distributed Trust Management; Exam 31/1/2013

Questions

1. **(1.5 points)** Explain the safety problem in Harrison-Ruzzo-Ullman Model. State under which condition(s) the safety problem is decidable.

2. **(1.5 points)** Let TOP SECRET, SECRET, CONFIDENTIAL and UNCLASSIFIED be the security levels (ordered from highest to lowest), and Navy and Army two categories. We have four subjects:

   - the president has TOP SECRET clearance for Navy and Army,
   - the colonel has SECRET clearance for Army,
   - the major has CONFIDENTIAL clearance for Navy, and
   - the soldier has UNCLASSIFIED clearance for Army and Navy.

   We also have some objects (documents):

   - the army position with security class $\langle$SECRET,{Army}$\rangle$,
   - the fleet position with security class $\langle$SECRET,{Navy}$\rangle$,
   - the number of army units with security class $\langle$CONFIDENTIAL,{Army}$\rangle$,
   - the number of navy units with security class $\langle$CONFIDENTIAL,{Navy}$\rangle$,
   - the costs of the army with security class $\langle$UNCLASSIFIED,{Army}$\rangle$, and
   - the costs of the navy with security class $\langle$UNCLASSIFIED,{Navy}$\rangle$.

   Answer the following questions based on the Biba model:

   (a) Draw the lattice of classifications.
   (b) Can the president compute the overall defense costs (army + navy)?
   (c) Can the major compute the cost per army unit?
   (d) Can the soldier compute the cost per navy unit?
   (e) Can the colonel change the overall defense position?
   (f) Can the major change the cost of navy and army?
   (g) Can the soldier change the fleet position?

   Justify the answers.

3. **(1.5 points)** Recall the definition of the RT_0 grammar. Consider the following RT_0 policy:
   $A.r \longleftarrow B.s \cap D.t$
   $B.s \longleftarrow B.s.t$
   $B.s \longleftarrow B.t$
   $B.s \longleftarrow D$
   $D.t \longleftarrow E$
   $D.t \longleftarrow C$
   $C.t \longleftarrow F$

   Find all principals populating $A.r$ (which means, compute $[[A.r]]$).

4. **(1 points)** Explain briefly the main differences between a rule-based trust management system and a reputation system. Give also two scenarios in which the first one is more suitable for a reputation system and the second one is more suitable for a rule-based system.

5. **(1.5 points)** Define the purpose hierarchy, role hierarchy, and access purpose authorizations in Purpose-based Access Control for the following scenario.

   Doctors are allowed to access patient information for providing medical treatment after they have worked for at least three years at the hospital. However, specialized doctors can access patient information for treating disease related to their specialization with one year experience at the hospital. For instance, cardiologists can treat cardiac arrhythmia and cardiac arrest, while immunologists can treat immune system related diseases. Nurses can access patient information for providing medical treatment. However, access is allowed only if the nurse has worked at the hospital for at least five years. Nurses in the cardiology division can access patient information for cardiac arrhythmia treatment with only two year experience at the hospital. Doctors with at least five year experience (at the hospital or in other research institutes) can access patient information for research purposes. Access to patient information for research purposes is allowed only within the hospital network.

6. **(1.5 points)** Explain the notion of policy refinement in Enterprise Privacy Authorization Language (EPAL). Describe the scope-based policy comparison algorithm for policy refinement.

7. **(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".

Access Request

```
  <Request>
    <Subject>
      <Attribute
          AttributeId="urn:oasis:names:tc:xacml:2.0:subject:subject-id"
          DataType="http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>
            John
        </AttributeValue>
      </Attribute>
      <Attribute
          AttributeId="urn:oasis:names:tc:xacml:2.0:subject:role"
          DataType="http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>
            clerk
        </AttributeValue>
      </Attribute>
      <Attribute
          AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-time"
          DataType="http://www.w3.org/2001/XMLSchema#time">
        <AttributeValue>
            10:00
        </AttributeValue>
      </Attribute>
     </Subject>
     <Resource>
      <Attribute
          AttributeId="urn:oasis:names:tc:xacml:2.0:resource:resource-id"
          DataType="http://www.w3.org/2001/XMLSchema#anyURI">
        <AttributeValue>
           MedicalRecord
        </AttributeValue>
      </Attribute>
    </Resource>
    <Action>
      <Attribute
         AttributeId="urn:oasis:names:tc:xacml:2.0:action: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"
    PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:first-applicable"
    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" />
        </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">physician</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">read</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 Effect="Permit" 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">Hard token</AttributeValue>
```

```
            <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-method"
                DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true" />
          </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">read</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="Deny" 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">nurse</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:anyURI-equal">
            <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#anyURI">medRecord</AttributeValue>
            <ResourceAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:1.0:resource:xpath"
                DataType="http://www.w3.org/2001/XMLSchema#anyURI" />
          </ResourceMatch>
        </Resource>
      </Resources>
    </Target>
  </Rule>
  <Obligations>
    <Obligation FulfillOn="Permit" ObligationId="O1" />
    <Obligation FulfillOn="Deny" ObligationId="O2" />
  </Obligations>
</Policy>
<Policy PolicyId="P2"
```

```
      RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:permit-overrides">
<Target>
  <Resources>
    <Resource>
      <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
        <AttributeValue
           DataType="http://www.w3.org/2001/XMLSchema#anyURI">MedicalRecord</AttributeValue>
        <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
           DataType="http://www.w3.org/2001/XMLSchema#anyURI" />
      </ResourceMatch>
    </Resource>
  </Resources>
</Target>
<Rule Effect="Deny" 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">nurse</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">
          <AttributeValue
              DataType="http://www.w3.org/2001/XMLSchema#time">14:00</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>
    <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" />
        </ActionMatch>
      </Action>
    </Actions>
  </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">nurse</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-greater-than">
            <AttributeValue
                DataType="http://www.w3.org/2001/XMLSchema#time">14:00</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">nurse</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">Hard token</AttributeValue>
            <SubjectAttributeDesignator
                AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-method"
                DataType="http://www.w3.org/2001/XMLSchema#string" />
          </SubjectMatch>
        </Subject>
      </Subjects>
    </Target>
  </Rule>
  <Obligations>
    <Obligation FulfillOn="Permit" ObligationId="O3" />
    <Obligation FulfillOn="Deny" ObligationId="O4" />
  </Obligations>
</Policy>
<Obligations>
  <Obligation FulfillOn="Permit" ObligationId="O5" />
  <Obligation FulfillOn="Deny" ObligationId="O6" />
</Obligations>
</PolicySet>
```