Distributed Trust Management; Exam 9/4/2014

Questions

1. **(1.5 points)** Consider a protection system with the following commands:

   command grant_right_owner (s, o, r)
   if own in $A[s, o]$
   then *enter* r *into* $A[s, o]$
   end

   command grant_right_others (s_1, s_2, o, r)
   if own in $A[s_1, o]$ and
   $r \neq write$
   then *enter* r *into* $A[s_2, o]$
   end

   command transfer_right (s_1, s_2, o, r)
   if read in $A[s_1, o]$ and
   r in $A[s_1, o]$
   then *enter* r *into* $A[s_2, o]$
   end

   Suppose Alice has developed an application and shared the application with other users. Any user should be able to execute the application, but the application should not be modified (consider right *write* for modification). Is the system secure? Justify the answer.

2. **(1.5 points)** Define a RBAC_3 system to regulate permissions within a bank branch. The system should implement the following requirements:

   (a) A bank employee can be a clerk, a manager, an auditor, or the head of the bank branch.
   (b) A bank branch can have only one head.
   (c) The head of the bank branch is a manager.
   (d) An auditor cannot be a clerk or a manager.
   (e) Clerks can make loan offers to customers.
   (f) Loan offers should be reviewed by a different clerk before they can be approved.
   (g) Loan offers lower than \$10K can be approved either by clerks or managers.
   (h) Loan offers equal or greater than \$10K must be approved by a manager.
   (i) A bank employee cannot approve loan offers he made or reviewed.
   (j) Approved loan offers should be analyzed by two auditors.

3. **(2 points)** Recall the definition of the RT_0 grammar.

   - *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 $B_2.r_2$.

Write an RT_0 model of the following situation: We have three companies: CITA (in Italy) and CUS (in the US). They decide to join forces on a given cooperative project that we will call projX. Each of these companies has an RT system in place, with the following rules.

```
CITA.partner <- Antonio.
CITA.partner <- Sandro.
CITA.partner <- . . .

CITA.employee <- . . .


CUS.ceo <- BigBoss.

CUS <- employee . . .
```

CITA and CUS agree that most of the documents developed in projX should be accessible only to people working at the project, and that some particularly confidential documents should be accessed only by people who have special permissions to read the documents of promX. To implement this, the two companies agree to employ the role names projX and accesstoX. So CITA will introduce the roles CITA.projX and CITA.accesstoX, and CUS will introduce the roles CUS.projX and CUS.accesstoX (so if say John is a member of the role [[CITA.projX]], it means that he is a member of project X according to CITA, and if John is a is a member of the role [[CUS.accesstoX]] or of the role [[CITA.accesstoX]] it means that he has access to these particularly confidential documents).

Your task is to define the rules defining CITA.projX, CITA.accesstoX, CUS.projX CUS.accesstoX, so that they reflect the following policies.

In CITA, any partner may decide who participates to projectX (i.e. who belongs to the role CITA.projX – notice that this means that each partner will need to define his/her own roles); moreover, any participant to projectX who is also a "partner" of CITA should be considered a senior participant to project.

In CUS, the ceo delegates to John the task of defining the projectX team as well as defining senior people in it.

To have access to the particularly confidential documents (i.e. to belong to [[CUS.accesstoX]] or of the role [[CITA.accesstoX]]) one needs the permission from at least one CITA participant to projectX AND one CUS participant to projectX

Tip: define roles: CITA.givespermission and CUS.givespermission

4. **(1.5 points)** List and explain the decision properties in UCON. Decribe how they are modeled in the language.

5. **(1.5 points)** Privacy-aware Access Control.

   (a) Explain why access purpose verification is needed.

   (b) Describe access purpose verification in purpose-based access control.

6. **(2 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>
   <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">
                Bob
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                doctor
            </AttributeValue>
         </Attribute>
         <Attribute IncludeInResult="false"
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                nurse
            </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:esource-id">
            <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                patientRecord
            </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:1.0:policy-combining-algorithm:permit-overrides">
  <Target>
       <AnyOf>
          <AllOf>
           <Match
             MatchId="urn:oasis:names:tc:xacml:1.0:function:function:string">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 patientRecord
             </AttributeValue>
             <AttributeDesignator
                 MustBePresent="false"
                 Category="urn:oasis:names:tc:xacml:1.0: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:1.0:rule-combining-algorithm:deny-overrides">
    <Target>
      <Target>
        <AnyOf>
          <AllOf>
           <Match
             MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
             <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                 doctor
             </AttributeValue>
             <AttributeDesignator
                 MustBePresent="false"
                 Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
                 AttributeId="urn:oasis:names:tc:xacml:1.0:role"
                 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">
                  cardiologist
               </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>
     </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">
              nurse
           </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>
    </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">
              nurse
```

```
            </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>
  <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: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">
               nurse
           </AttributeValue>
           <AttributeDesignator
               MustBePresent="false"
               Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
               AttributeId="urn:oasis:names:tc:xacml:1.0:role"
               DataType="http://www.w3.org/2001/XMLSchema#string"/>
         </Match>
        </AllOf>
      </AnyOf>
  </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">
                doctor
             </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="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="Deny" RuleId="R5">
      <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>
```