

# Principles of Data Protection (2IS27): Exam 8/4/2015

## Questions

1. (1.5 points) Let HIGH-CRITICAL, CRITICAL and NO-CRITICAL be the integrity levels (ordered from highest to lowest), and Navy and Army two categories. Consider the following subjects and objects along with their integrity class:

| Subject | Integrity Class          |
|---------|--------------------------|
| General | (HIGH-CRITICAL, {Army})  |
| Admiral | (HIGH-CRITICAL, {Navy})  |
| Major   | (CRITICAL, {Army, Navy}) |
| Soldier | (NO-CRITICAL, {Army})    |

| Object                | Integrity Class         |
|-----------------------|-------------------------|
| Position of army unit | (HIGH-CRITICAL, {Army}) |
| Position of navy unit | (HIGH-CRITICAL, {Navy}) |
| Number of army units  | (CRITICAL, {Army})      |
| Number of navy units  | (CRITICAL, {Navy})      |
| Cost of army unit     | (NO-CRITICAL, {Army})   |
| Cost of navy unit     | (NO-CRITICAL, {Navy})   |

Answer the following questions based on the Biba model with low-water-mark for objects:

- Draw the lattice of classification.
- Can the general compute the overall number of defense units (army + navy)?
- Can the general change the position of a navy unit?
- Can the admiral compute the overall cost of navy units?
- Can the admiral compute the overall cost of navy units after a soldier updated the cost of a navy unit?
- Can the major read the position of a navy unit after it was changed by a general?
- Can the soldier compute the overall cost of army units? (This requires access to the number and cost of army units.)

Justify the answers.

- (1.5 points) Explain the goal of the Chinese Wall model and describe the main concepts and properties of the model.
- (1.5 points) Define an RBAC<sub>3</sub> policy for an online grading system. The system should implement the following requirements:
  - A course has at least one lecturer.
  - A lecturer must be a professor.
  - A course can have no, one or more teaching assistants.
  - A teaching assistant can be a student.
  - Students can enroll in a course.
  - A student cannot be a teaching assistant in a course in which he/she is enrolled.
  - Lecturers can add, update and view grades.
  - Teaching assistants can add and view grades.

4. (2 points) Consider the following  $RT_0$  policy.

1 :  $B.s \leftarrow B.s.t$   
2 :  $B.s \leftarrow C$   
3 :  $B.s \leftarrow D$   
4 :  $C.t \leftarrow D.t$   
5 :  $C.t \leftarrow K$   
6 :  $D.t \leftarrow E$

- Find all principals populating  $B.s$  (which means, compute  $[[B.s]]$ ).
  - Write down the graph generated by the top-down algorithm when computing the semantics of  $B.s$ . (the top-down algorithm is also known as the “backward algorithm”).
  - Explain why it would be a bad idea to store the credentials defining  $C.t$  at the subject and all other credentials at the issuer. Explain what would happen.
  - Explain why it could be a good idea to store the credentials defining  $D.t$  at the subject and all other credentials at the issuer.
5. (1.5 points) Explain the notion of policy refinement in Enterprise Privacy Authorization Language (EPAL) and give a scenario in which policy refinement is needed. Describe the main steps of the scope-based policy comparison algorithm for policy refinement.
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/PolicySet 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">
        Alice
      </AttributeValue>
    </Attribute>
    <Attribute IncludeInResult="false"
      AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
        physician
      </AttributeValue>
    </Attribute>
    <Attribute IncludeInResult="false"
      AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role">
      <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
        cardiologist
      </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">
        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:deny-overrides">
  <Target>
    <AnyOf>
      <AllOf>
        <Match
          MatchId="urn:oasis:names:tc:xacml:1.0: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:permit-unless-deny">
    <Target>
      <AnyOf>
        <AllOf>
          <Match
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
              <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
                physician
              </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="Deny" 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">
                        radiologist

```

```

        </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:permit-overrides">
    <Target />
    <Rule Effect="Deny" 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">
                            physician
                        </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>
            </Target>
        </Rule>
    </Policy>

```

```

    <Match
      MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">
          radiologist
        </AttributeValue>
        <AttributeDesignator MustBePresent="true"
          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="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">
              physician
            </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>
  <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>
```