Exercise

Role-based Access Control
Goals

• Learn and apply languages for role-based access control modelling
• Understand the limitations of these languages
Consider the Following Scenario

The football game report is started before the match, continued during the match, and finalised once the match is over. The new report is created by the league secretary, who is employed by the Football Federation. The league secretary fills in initial information such as league name, his own contact data, region, division, and game numbers as well as the names of the competing teams. Once done, the league secretary informs the team representatives, so that they could provide the team composition for the game, including player names and their registration numbers. The team composition should be provided no later than 2 h before the game.
Consider the Following Scenario

(slide 2)

During the match the game report needs to be maintained by the umpire, who needs to register the scored goals and “given” cards. The umpire is also responsible for filling in the match results, including the scores (including final, full time, extra time and penalties). After the match, the umpire needs to invite the team representatives to sign the report and (optionally) provide comments. Once signatures from the team representatives are received, the umpire himself comments and signs the report. After the game the report is sent to the league secretary for confirmation.
WOLFS FOOTBALL LEAGUE MATCH REPORT FORM

League Secretary
CALEX KARUUNA
20 STREET ALLEA
CITY

Each team representative is to sign this form and ensure that all details are correct and that all players are registered with the ERIS system.

<table>
<thead>
<tr>
<th>LEAGUE NAME</th>
<th>WOLFS</th>
<th>DIVISION</th>
<th>A</th>
</tr>
</thead>
<tbody>
<tr>
<td>REGION</td>
<td>AA</td>
<td>GAME</td>
<td>45</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HOME TEAM NAME</th>
<th>Final score: 3</th>
<th>AWAY TEAM NAME</th>
<th>Final score: 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Green Rabbits</td>
<td></td>
<td>Orange Carrots</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FULL NAME</th>
<th>REG, NO</th>
<th>CARDS</th>
<th>GOALS</th>
<th>FULL NAME</th>
<th>REG, NO</th>
<th>CARDS</th>
<th>GOALS</th>
</tr>
</thead>
<tbody>
<tr>
<td>[1] John</td>
<td>1</td>
<td></td>
<td></td>
<td>Joseph</td>
<td>11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[2] Peter</td>
<td>2 YY-&gt;R</td>
<td>1</td>
<td></td>
<td>Boris</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[4] Davy</td>
<td>5</td>
<td></td>
<td></td>
<td>Ferdinandy</td>
<td>10 Y</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[6] King</td>
<td>7</td>
<td></td>
<td></td>
<td>Svetoslay</td>
<td>4 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[7] Shark</td>
<td>9 Y</td>
<td></td>
<td></td>
<td>Jevegenyi</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[8] Anupras</td>
<td>10</td>
<td></td>
<td></td>
<td>Matheus</td>
<td>6 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>[9] George</td>
<td>11 1</td>
<td></td>
<td></td>
<td>Annis</td>
<td>55 YY-&gt;R</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Full time score | Extra time score | Penalties | Full time score | Extra time score | Penalties
2 | 1 | - | 2 | 0 | -

Signature of Home Team Representative: HomeSignedIt
Signature of Away Team Representative: AwaySignedIt

I am satisfied with my opponents registration/performance (Please indicate YES or NO above)
YES |
NO |

Home Team Caution: No problem, everything is OK
Away Team Caution: No problem, everything is OK

Umpire Name: Billy-Goat the Beard
Referee signature: BilGoalB
No comments
Umpire Comment: No comments

Confirmation by league secretary: Confirmed
Confirmation date: 2020.02.20

5
Task 1

• Define the SecureUML model representing role-based access control policy regarding the gathered and registered data
Task 1

- Define the SecureUML model representing role-based access control policy regarding the gathered and registered data.

To guide your solution, consider:
- What are objects and their concerned attributes?
- What operations do change the values of the attributes?
- What are roles?
- What are the security actions?
- What are the permissions of roles towards the object?
- Who are the users?
Task 1

• Define the SecureUML model representing role-based access control policy regarding the gathered and registered data

To guide your solution, consider
• What are objects and their concerned attributes?
• What operations do change the values of the attributes?
• What are roles?
• **What are the security actions?**
• What are the permissions of roles towards the object?
• Who are the users?

- The **question in blue** should explicitly be answered in a separate diagram
- Answers to other questions can be given directly in the defined SecureUML model
Task 1

• Define the **SecureUML** model representing role-based access control policy regarding the gathered and registered data

• What authorisation constraints should be defined in your model?
  – They can be defined in any *formal, semiformal* or *natural* language (in case of natural language, use **English 😊**)

Task 2

- Define the UMLsec model representing the role-based access control policy regarding the gathered and registered data
Task 2

• Define the UMLsec model representing the role-based access control policy regarding the gathered and registered data

To guide your solution, consider
• What are the objects
• What are their operations?
• What are the roles?
• What are the role’s rights?
• What are the associated tags?
• Who are the users?
Task 2

• Define the UMLsec model representing the role-based access control policy regarding the gathered and registered data

To guide your solution, consider
• What are the objects
• What are their operations?
• What are the roles?
• What are the role’s rights?
• What are the associated tags?
• Who are the users?

{\text{protected} = \text{protected\_action}}
{\text{role} = (\text{actor}, \text{role})}
{\text{right} = (\text{role, protected\_action})}
Task 3

Explain what **RBAC policy concerns are captured** in your…

... *SecureUML* model and *not* in the *UMLsec* model

... *UMLsec* model and *not* in the *SecureUML* model