Workshop
Part 2

Security Risk Modelling

Workshop Part 2 Input
Scenario given during Workshop Part 1

• Partial solution of Workshop Part 1
  – Context and assets description
    • e.g., Section 1.2, Section 1.3, and Table 2
  – Descriptions of four most important / most severe security risks
    • Risks are described in Tables 3.x.
    • Use the results from Table 6 and select four risks with the highest priority
  – Description of security countermeasure which mitigate the selected four risks
    • e.g., Table 4.y

• Four modelling languages
  – Security risk-oriented BPMN
  – Security risk-aware Secure Tropos
  – Security risk-oriented misuse cases
  – Mal-activities for security modelling
Workshop Part 2 Input

Scenario given during Workshop 1

- Partial solution of Workshop 1
  - Context and assets description
    - e.g., Section 1.2, Section 1.3, and Table 2
  - Description of four most important/security risks
    - Risks are described in Tables 3.x.
    - Use the results from Table 6 and select four risks with the highest priority
  - Description of security countermeasure which mitigate the selected four risks
    - e.g., Table 4.y

Goal of Workshop Part 2
Apply modelling languages for security risk management

Four modelling languages
- Presented during

- Security risk-oriented
  - BPMN
  - Secure Tropos
  - Security risk-aware Secure Tropos
  - Security risk-oriented misuse cases
  - Mal-activities for security modelling

Tasks and Steps

Context and assets

- Security Risk.i
- Security Risk.ii
- Security Risk.iii
- Security Risk.iv

- Security Counter-measures.i
- Security Counter-measures.ii
- Security Counter-measures.iii
- Security Counter-measure.iv
1. Create security risk management model using security risk-oriented BPMN

- Model should consists of
  - Context and asset model,
  - Security risk model, showing how security risk harms assets and negate security criteria
  - Security countermeasure model showing how the security risk is mitigated

2. Explain what you were not able to model using the security risk oriented BPMN
Tasks and Steps

3. Create security risk management model using security risk-aware Secure Tropos
   - Model should consists of
     • Context and asset model,
     • Security risk model, showing how security risk harms assets and negate security criteria
     • Security countermeasure model showing how security risk is mitigated

4. Explain what you were not able to model using the security risk-aware Secure Tropos
Tasks and Steps

5. Create security risk management model using security risk-oriented misuse cases
   - Model should consists of
     - Context and asset model
     - Security risk model, showing how security risk harms assets and negate security criteria
     - Security countermeasure model showing how security risk is mitigated

6. Explain what you were not able to model using the security risk-oriented misuse cases
   - Model should consists of
     - Context and asset model
     - Security risk model, showing how security risk harms assets and negate security criteria
     - Security countermeasure model showing how security risk is mitigated
### Tasks and Steps

<table>
<thead>
<tr>
<th>Context and assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Countermeasures.\textit{i}</td>
</tr>
</tbody>
</table>

#### 7. Create security risk management model using Mal-activities for security risk management

- Model should consists of
  - Context and asset model
  - Security risk model, showing how security risk harms assets and negate security criteria
  - Security countermeasure model showing how security risk is mitigated

#### 8. Explain what you were not able to model using the Mal-activities for security risk management
Tasks and Steps

9. Estimate effort of each team member in the workshop

Workshop (Part 2) plan

• Presentation of the workshop tasks
• Work on the task
• From the mid of lecture 2
  – Result (so far) overview – presentation:
    • 120 seconds max per team
Workshop (Part 2) plan

- **Presentation of the workshop tasks**
  - Work on the task
  - From the mid of lecture 2
    - Result (so far) overview – presentation:
      - 120 seconds max per team

- If your team is not present at the workshop, **OR**
  - If less than 51% of the team members are present at the class
    - The team have to submit the *recorded video presentation* (of the final solution) together with the workshop solution.
Workshop (Part 2) plan

- **Present**
  - At the beginning of the presentation say:
    - your team name
  - the names of the team members

- **Work**

- **From**
  - If your team is not present at the workshop, OR
  - If less than 51% of the team members are present at the class
    - The team have to submit the *recorded video presentation* (of the final solution) together with the workshop solution
  - If you are not present at the workshop, but the majority of your team was present at the class, make sure that you contribute equally to the workshop solution

Submission

- To submit:
  - Use the course Website

- Deadline:
  
  **15.April, 23:59**

  *Penalty of late submission minus 50% from the evaluation grade*