Evaluation results

<table>
<thead>
<tr>
<th>Test, exercises</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test III</td>
<td>/ 15</td>
</tr>
<tr>
<td>Exercise 1:</td>
<td>/ 3</td>
</tr>
<tr>
<td>Exercise 2:</td>
<td>/ 5</td>
</tr>
<tr>
<td>Exercise 3:</td>
<td>/ 10</td>
</tr>
<tr>
<td>Exercise 4:</td>
<td>/ 2</td>
</tr>
<tr>
<td>TOTAL:</td>
<td>/ 35</td>
</tr>
</tbody>
</table>

( / 5 course points)

Test III

Modelling languages

1. Which of the following constructs can be used to represent system assets in Security risk-oriented misuse cases? 

   ☐ Security Use Case
   ☐ System Boundary
   ☐ Use Case

2. Which of the following constructs can be used to represent vulnerability in Security risk-oriented misuse cases?

   ☐ Misuser
   ☐ Misuse case
   ☐ Vulnerability

3. Which of the following constructs can be used to represent impact using Mal-activities for the risk management?

   ☐ Swimlane
   ☐ Decisions
   ☐ Malicious Activity

4. Which of the following constructs can be used to represent control using Mal-activities for the risk management?

   ☐ Mitigation Activity
   ☐ Swimlane
   ☐ Activity
   ☐ Decision
**Model transformation**

How to transform security risk management model from Security risk-oriented misuse cases (misuse cases) to Mal-activities for the risk management (mal-activity)?

5. Regarding **system asset**

☐ From misuse cases *Security Constraint* to mal-activity *Activity*  
☐ From misuse cases *Use case* to mal-activity *Activity*  
☐ From misuse cases *Use case* to mal-activity *Comment*

6. Regarding **attack method**

☐ From misuse cases *Misuse case* to mal-activity *Mitigation activity*  
☐ From misuse cases *Misuse case* to mal-activity *Malicious activity*  
☐ From misuse cases *Misuser* to mal-activity *Mal-swimlane*

**Privacy properties**

7. What does it mean when an attacker cannot sufficiently distinguish whether an item of interest (from the attacker’s perspective) exists or not?

☐ Unlinkability  
☐ Undetectability  
☐ Unobservability

8. What does it mean when an attacker cannot sufficiently identify the subject within a set of subjects (from the attacker perspective)?

☐ Anonymity  
☐ Unobservability  
☐ Pseudonymity

9. What does it mean “PET” in the context of the privacy-by-design?

☐ A domestic or tamed animal kept for companionship or pleasure  
☐ Privacy enhancing technology  
☐ Privacy enforcing technique  
☐ Policy enhancing technology

**Role-Based Access Control Modelling**

10. How is a specific type of interaction between a subject and an object that results in the flow of information from one to another called?

☐ Access control  
☐ Session  
☐ Access  
☐ Permission assignment
11. How is an active entity that causes information to flow among objects or changes the system state called? 1 point

- ☐ Administrator
- ☐ User
- ☐ Subject
- ☐ Role

12. How is a partial order of relationships established among roles called? 1 point

- ☐ Sessions
- ☐ Permission hierarchy
- ☐ Role hierarchy
- ☐ Constraints

13. What are the major tasks of the system administrator? 1 point

- ☐ Predefine secured operations and objects
- ☐ Manage users and roles
- ☐ Create assignment relationships
- ☐ Establish relationships between roles, secured operations and objects

14. Which modelling languages are specifically extended to model role-based access control? 1 point

- ☐ Secure Tropos
- ☐ SecureUML
- ☐ KAOS extension to security
- ☐ Misuse cases
- ☐ Mal-activity diagrams
- ☐ UMLsec

15. What are the main security actions? 1 point

- ☐ Insert / create
- ☐ Select / read
- ☐ Change / update
- ☐ Remove / delete
Exercise 1: In the given Mal-activities for security risk management model (see Fig. 1), identify which elements represent:

- Impact:

- Attack method:

- Security requirements:

3 points

Fig. 1: Mal-activities for security risk management
Exercise 2: Fill in the Visibility matrix (Table 1) with values V (visible), A (accessible), and H (hidden) for the model given in Fig. 2.

Table 1: Visibility matrix

<table>
<thead>
<tr>
<th></th>
<th>D1</th>
<th>D2.1</th>
<th>D2.2</th>
<th>D4.1</th>
<th>D4.2</th>
<th>D5.1</th>
<th>D5.2</th>
<th>D6.1</th>
<th>D6.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>RapidGatherApp</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PE Android</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compute Server 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compute Server 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Exercise 3:** The SecureUML model (see Fig. 3) was received by transforming the corresponding UMLsec model. Complete this SecureUML model by introducing missing language constructs. Do not forget (!) to define and apply needed security actions.

*Fig. 3: SecureUML model*

**Exercise 4:** There exist different access control models besides the role-based access control (RBAC) model. Please write names of at least 2 other access control models

1. 
2. 
...