Name: _________________________________________________________________________

Evaluation results

<table>
<thead>
<tr>
<th>Test, exercises</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Questionnaire</td>
<td>/ 10</td>
</tr>
<tr>
<td>Exercise 1:</td>
<td>/ 5</td>
</tr>
<tr>
<td>Exercise 2:</td>
<td>/ 5</td>
</tr>
<tr>
<td>Exercise 3:</td>
<td>/ 5</td>
</tr>
<tr>
<td>Exercise 4:</td>
<td>/ 5</td>
</tr>
<tr>
<td>TOTAL:</td>
<td>/ 30</td>
</tr>
</tbody>
</table>

( / 10 course points)

Questionnaire

1. What does security pattern describe?  
   - ☐ A fundamental structure and workflow of application domain  
   - ☐ A particular recurring security problem  
   - ☐ A specific security context where security problem arises  
   - ☐ A well-proven generic scheme for a security solution  
   \[1\] point

2. What are patterns for enterprise security and risk management about?  
   - ☐ Threat assessment  
   - ☐ Asset valuation  
   - ☐ Automated identification and authentication design alternatives  
   - ☐ Enterprise partner communication  
   - ☐ Role-based access control  
   \[1\] point

3. What are patterns for operating system access control about?  
   - ☐ Full access with errors  
   - ☐ Limited access  
   - ☐ Access control in operating systems  
   - ☐ Malicious activity  
   \[1\] point

4. What are patterns for identification and authentication about?  
   - ☐ Threat assessment  
   - ☐ Asset valuation  
   - ☐ PKI design alternatives  
   - ☐ Unregistered users I&A requirements  
   - ☐ Role-based access control  
   \[1\] point

5. What are the major information processing functions?  
   \[1\] point
6. What is the input for the SREBP method?  

- Business processes models defined in the value chain and business process diagrams
- Security objectives determined for business supported by the systems assets
- Pattern occurrences identified when applying security risk-oriented patterns

7. What does acronym SRP mean?  

- Security requirements patterns
- Security risk-oriented patterns
- Security risk process

8. Which steps do not belong to the security requirements elicitation from business processes (the SREBP method)?  

- Identify business assets
- Determine security objectives
- Analyse and assess security risks
- Make security risk treatment decision
- Identify patterns, extract security model and derive security requirements

9. What components needs to be identified when securing data transmitted between business entities?  

- Functional-unit and business partner
- Input interface and input data
- Secret key and private key
- Communicators and data transmission

10. What components needs to be identified when securing business services against denial of service attacks?  

- Functional-unit and business partner
- Input interface and input data
- Secret key and private key
- Communicators and data transmission

--- End of Questionnaire ---
In business process diagram (see Fig. 1 a), four occurrences were identified using the SRP1 pattern (Secure data from unauthorized access).

Fig. 1: Business process diagram (a) and asset model of SRP 1 (b)
Exercise 1: Extract security model (for the Game business asset)  

Exercise 2: Derive security requirements
Exercise 3: SRP4 pattern was applied to the business process diagram as illustrated in Fig. 2. How security model (see Fig. 3) should be completed?

5 points

**SRP4:** Secure business services against denial of service attacks

Fig. 2: Application of SRP 4

Fig. 3: SRP4 security model
Exercise 4: The following security requirements were elicited using the SREBP method.

**SecReq.1:** Umpire should be able to update the gameReport.
**SecReq.3:** FootballFederationEmployee should be able to update the confirmation.
**SecReq.4:** ERIS should have unique identity in the form of key pairs (public key, private key) certified by a certification authority.
**SecReq.5:** Umpire should encrypt and sign game report (and other data communicated to ERIS) using keys before sending it to ERIS.
**SecReq.7:** Update game report should filter the input (i.e., game report).
**SecReq.10:** Update game report should establish a rule base (i.e., a collection of constraints used by different firewalls) to communicate with the Umpire.
**SecReq.11:** Packet Filter Firewall should filter the Umpire’s address to determine if that is not a host used by the threat agent.
**SecReq.14:** The ERIS should audit the operations after the retrieval, storage or any other manipulation of data in the Game storage.

Annotate the business process diagram (Fig. 4) with security requirements (for annotations use only the requirements IDs).
Alternatively, in case you do not have means to annotate the model, write/explain where these requirements should be annotated in the model.

5 points