Name: _____________________________________________

Evaluation results

<table>
<thead>
<tr>
<th>Test, exercises</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test IV</td>
<td>/ 10</td>
</tr>
<tr>
<td>Exercise 1.1:</td>
<td>/ 5</td>
</tr>
<tr>
<td>1.2:</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>TOTAL:</td>
<td>/ 30</td>
</tr>
</tbody>
</table>

( / 5 course points)

Test IV

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. Patterns for firewall architecture represent trade-offs between complexity, speed and security, which are tailored to control attacks on specific layers of the network. What are the major types of the firewall architecture patterns?
   ☐ Proxy-base firewalls
   ☐ Address filtering lanes
   ☐ Packet filter firewalls
   ☐ Statefull firewalls
   ☐ Keep state procurements
   1 point
5. What are the major information processing functions? 
☐ Capturing, transmitting, storing, retrieving, manipulating and digging information
☐ Capturing, transmitting, storing, retrieving, managing and displaying information
☐ Capturing, transmitting, storing, reorganising, manipulating and displaying information
☐ Capturing, transmitting, storing, retrieving, manipulating and displaying information

6. What does acronym SREBP mean? 
☐ Security requirements engineering from banned products
☐ Security requirements elicitation from business processes
☐ Software requirements elicitation from business processes

7. 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

8. What components needs to be identified when creating role-based access control security model? 
☐ Resources, roles (and users)
☐ Secured operations
☐ Permissions and security constraints
☐ Confirmations and reports

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 are next engineering activities once security requirements are elicited using the SREBP method? 
☐ Lean back and get some refreshments
☐ Prioritise security requirements
☐ Introduce security requirements and the security constraints to the business process model
☐ Implement security requirements to the developed system
Exercise 1: In business process diagram (see Fig. 1 a), four occurrences were identified using the SRP1 pattern (*Secure data from unauthorized access*).

1.1: Extract security model (for the *Game* business asset)  
1.2: Derive security requirements

![Fig. 1: Business process diagram (a) and asset model of SRP 1 (b)](image-url)
Exercise 2: SRP4 pattern was applied to the business process diagram as illustrated in Fig. 2. How security model (see Fig. 3) should be completed?

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

Fig. 2: Application of SRP 4
**Exercise 3:** The following security requirements were elicited using the SREBP model.

- **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).

*5 points*
Fig. 4: Business process diagram