EXAMINATION
[The sum of points equals to 100]

PART I: Internet Store example

Description: Internet store (or online shopping) is a form of electronic commerce, which allows consumers to directly buy goods or services from a seller over the Internet using a web browser. As such it potentially could involve different security concerns including social engineering attacks, privacy, trust and trustworthiness, scripting attacks and similar.

An extract of the model for the security risk management in the Internet store case is provided in Fig. 1, 2, and 3. The model is created using the security risk-aware business process model and notation (BPMN) language and it gives the analyses viewpoints on assets (Fig. 1), security risks (Fig. 2), and security risk treatment (Fig. 3).

Fig. 1. Internet store: asset analysis
Creativity – your key to secure software!!!

**Fig. 2.** Internet store: security risk analysis

**Fig. 3.** Internet store: security risk treatment analysis
**Task 1**: Fill in Table 1 with the details that correspond to the description of security risk management model provided in Fig. 1, 2, and 3.

**Table 1**: Recognizing concepts of security risk management

<table>
<thead>
<tr>
<th>Concepts of the domain model for the information systems security risk management</th>
<th>What is (are) business asset(s) in the Internet Store example, given Fig. 1, 2, and 3?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assets</strong></td>
<td></td>
</tr>
<tr>
<td>Business assets</td>
<td></td>
</tr>
<tr>
<td>Information System assets</td>
<td></td>
</tr>
<tr>
<td>Security criterion</td>
<td></td>
</tr>
<tr>
<td>Risk</td>
<td></td>
</tr>
<tr>
<td>Impact</td>
<td></td>
</tr>
<tr>
<td>Event</td>
<td></td>
</tr>
<tr>
<td>Threat</td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td></td>
</tr>
<tr>
<td>Threat agent</td>
<td></td>
</tr>
<tr>
<td>Attack method</td>
<td></td>
</tr>
<tr>
<td>Risk treatment decision</td>
<td></td>
</tr>
<tr>
<td>Security requirements</td>
<td></td>
</tr>
<tr>
<td>Controls</td>
<td></td>
</tr>
</tbody>
</table>
**Task 2**: If the concept of the security risk management is not represented in the model, define it (and write it in Table 1) following your intuition on the modelled example. Discuss your proposal(s).

<table>
<thead>
<tr>
<th>Table 1</th>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset(s)</td>
<td>Risk(s)</td>
<td>Risk treatment(s)</td>
</tr>
</tbody>
</table>

If you were able to fill all the table lines from the given Fig. 1, 2, and 3, tick this box.  

- [ ] (5 points)

**Description**: Use different security risk-oriented language (*but not BPMN!!!*) and model how asset(s), risk(s) and risk treatment(s) defined by you in Table 1, is (are) represented using the selected language. You can choose, for example, *one* language from security risk-aware/oriented (*i*) Secure Tropos, (*ii*) Misuse cases diagrams, or (*iii*) Mal-activity diagrams.

Three diagrams needs to be created in order to show:

**Task 3**: What are the context, assets and their security criteria;  

**Task 4**: How does the security risk constitute itself;  

**Task 5**: What is the countermeasure (i.e., risk treatment, security requirements, and controls), and how does it mitigate the security risk.

**Note**: Although a picture is worth 1000 words, short textual explanations of the diagrams are welcome!
**PART II: Application for Japanese course**

The developers of the course registration system have sent us the description and the example of the registration form for the Japanese course. They have requested a help to define the access policy to the course-related information.

**Description:** The process starts with student filling in the subscription. Student specifies his contact information, school and current grade point average and registered course number. The subscription requests are sent to an evaluation team in the university who will not see the actual contact information of the subscriber, but only the previous study information, student SSN and course the student would like to register to. The evaluation team will mark requirements fulfilled or not. If the requirements are not filled then the document is rejected, process stops and the student is notified. If the requirements are filled, then it is sent to study committee, who will decide in what amount or if any the course cost will be funded with a scholarship. The study committee can only view the application with an exception to add scholarship amount to the document. After the study committee has made its decision the document is sent to accounting department to approve payment. If the payment is accepted, then the accounting department marks it as paid.

**Roles:** student, study committee, evaluation team, and accounting

<table>
<thead>
<tr>
<th>Student SSN: A62112</th>
<th>Email: <a href="mailto:skanfandr.aleksandr@ut.ee">skanfandr.aleksandr@ut.ee</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Last name: Skanfandr</td>
<td>Full name of School: University X</td>
</tr>
<tr>
<td>First name: Aleksandr</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Registered course number</th>
</tr>
</thead>
<tbody>
<tr>
<td>[x] JA 101</td>
</tr>
<tr>
<td>[ ] JA 102</td>
</tr>
<tr>
<td>[ ] JA 103</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fee: 400$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scholarship: 100$</td>
</tr>
<tr>
<td>Grade point average (previous year): 4.2</td>
</tr>
<tr>
<td>Requirements filled: Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Payment info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cardholder's name: Aleksandr Skanfandr</td>
</tr>
<tr>
<td>Card Number: 213213123122312</td>
</tr>
</tbody>
</table>

**Fig. 4. Application for Japanese course**
**Task 6:** Using the SecureUML modelling language, create a class diagram, which would define the role-based access control (RBAC) policy in correspondence to the application for Japanese course.

The class diagram should specify:

- Protected Resource(s), its Attributes and protected Operations \( (10 \text{ points}) \)
- Users, Roles, and User assignments \( (5 \text{ points}) \)
- Permissions, Permissions assignment \( (5 \text{ points}) \)
- Security actions (as separate class diagram) \( (5 \text{ points}) \)

**Task 7:** Define at least 5 security authorisation constraints (either in plain text or using object constraint language (OCL)). This means, describe the link between the security actions of the roles and the resource operations (over the attributes). \( (10 \text{ points}) \)
BONUS – A Multiple-Choice Questionnaire

[Each correctly answered question gives you 1 point.]

1. What are enterprise security and risk management patterns?
   a) Patterns, which define security constraints at the architectural level, the application level
   b) Patterns, which define specific requirements and design for the identification and authentication services;
   c) Patterns, which are essential for systems that permit or deny the use explicitly
   d) Patterns, which represent trade-offs between complexity, speed, and security;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

2. What is risk reduction?
   a) An action to lessen the probability, negative consequences, or both, associated with a risk;
   b) A decision not to become involved in, or to withdraw from, a risk;
   c) A decision of how to treat the identified risks;
   d) A sharing with another party the burden of loss from a risk;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

3. Why is consideration of security from early stages of software system development important?
   a) Because it helps envisage threats, their consequences and countermeasures;
   b) Because the need to secure systems and software becomes a necessity rather than an option;
   c) Because it discard design alternatives that do not offer a sufficient security level;
   d) Because it help re-scope or cancel a project if the risk is too high;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

4. What are intrusion detection requirements?
   a) Requirements that characterise the extent to which a business, application, or component shall verify the identity of its externals before interacting;
   b) Requirements that characterise the extent to which an application or component shall ensure that its data and communications are not intentionally corrupted via unauthorized creation, modification, or deletion;
   c) Requirements that characterise the extent to which a business, application, or component shall keep its sensitive data and communications private from unauthorized individuals and programs;
   d) Requirements that characterise the extent to which an application or component shall detect and record attempted access or modification by unauthorized individuals;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.
5. What are the problems of input validation and representation?
   a) Cross-site scripting attacks;
   b) Command injection;
   c) Password management;
   d) SQL injection;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

6. What is an access?
   a) A mapping between a user and an activated subset of roles the user is assigned to;
   b) A passive entity that contains or receives information;
   c) A specific type of interaction between a subject and an object that result in the flow of information from one to the other;
   d) A job function within the organisation that describes the authority and responsibility conferred on a user assigned to the role;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

7. Which best practices are applied in the comprehensive lightweight application security process?
   a) Institute awareness programs
   b) Perform application assessments
   c) Capture security requirements
   d) Build vulnerability remediation procedures
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

8. What is shoulder surfing?
   a) Pawing through a target’s garbage in search of valuable information;
   b) Stealth observation of the target to obtain or deduce confidential information;
   c) Exploiting user’s curiosity to deliver malware;
   d) Continuing to function even if a data centre is destroyed;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

9. What is a risk impact?
   a) A component or part of the IS that has value to the organisation and is necessary for achieving its objectives;
   b) A property or constraint on business assets that characterises their security needs;
   c) A potential negative consequence of a risk that may harm assets of a system or an organisation, when a threat is accomplished;
   d) A combination of a threat and one or more vulnerabilities
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.