EXAMINATION

The exam is open book, open laptop and open Internet. But you have to provide your individual solutions – the collaboration in any form is not allowed. You can provide your solutions either on paper or electronically. In case of the electronic solutions, please email the file to <rma@ut.ee> no later than 14:05 with a subject “[SSD] exam solutions”.

PART I: Security Risk Management

Introduction: During the guest lecture, Dr. Margus Freudenthal has presented the X-Road system used in Estonia. Based on this example, perform security risk management process (see Fig. 1) to elicit one security risk to the X-Road system assets and to propose countermeasures to mitigate this risk. When performing this process answer and complete the given questions and tasks.

T1. Give a short description of the context where potentially the security risk could be identified. (5 points)
Creativity – your key to secure software!!!

**T2.** What are *business assets, IS assets,* and what is the *support* relationship between different assets? What are *security criteria?*  

<table>
<thead>
<tr>
<th>Assets</th>
<th>Business assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td></td>
</tr>
<tr>
<td>System assets</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Support relationship</th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Security criterion</th>
<th></th>
</tr>
</thead>
</table>

**T3.** What are *risk* and its components?  

<table>
<thead>
<tr>
<th>Risk</th>
<th></th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

(8 points)
T4. What are risk treatment decision, security requirements and potential security controls which implement suggested security requirements? (Hint: security requirements must satisfy criteria for good security requirements) (10 points)

<table>
<thead>
<tr>
<th>Risk treatment decision</th>
<th>Security requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Controls</td>
<td></td>
</tr>
</tbody>
</table>

PART II: Security Risk Modelling

Introduction: Select one graphical modelling language and create a model following your answers given for tasks T1-T4. You can choose any modelling language presented during the course or modelling language, which you experienced before.

(if you select language, which was not analysed during the course, give short introduction on language syntax and semantics)

Selected graphical modelling language:

Using selected modelling language you need to create three diagrams:

T5. Diagram for context, assets, and security criteria visualisation. Input for the diagram – your answers given for T1 and T2. (10 points)

T6. Diagram for security risk visualisation. Input for diagram is your answer given for T3. (10 points)

T7. Diagram for security countermeasure visualisation. Input for diagram is your answer for T4. (10 points)
T8. Discuss what are benefits of security risk management when developing software systems. (10 points)

**PART III: Modelling Role-based Access Control Policy**

**Introduction:** Define the role-based access control (RBAC) policy for the given scenario (see below). When preparing the policy, answer and complete the given questions and tasks.

T9. What are the protected object, its attributes, and its protected operations? Please use the class diagram notation to answer this question (5 points)

T10. What are the roles and potential actors involved in this scenario? (5 points)

<table>
<thead>
<tr>
<th>Roles</th>
<th>Actors</th>
<th>Role actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Lecturer</td>
<td>Raimundas Matulevičius</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
T11. Prepare the UMLsec model (i.e., the UML activity diagram extended for the RBAC modelling) to visualise the RBAC policy for the given scenario.  

(10 points)

T12. Write down all needed authorisation constraints.  

(10 points)

Examination Process Scenario

Description: The process starts with the creation of the protocol report by the course manager from the dean’s office. The information transferred from the exam registration sheet includes the name of the subject, the list of the students who took the exam (each student entry includes student ID number, name and surname, and study program), and the course lecturer name. Lecturer fills in the grades for each student, however lecturer is not able to see the student names but only their ID numbers. But the lecturer can enter a new student to the protocol (in case this information was not transferred or not available in the examination registration sheet). Lecturer can also change the date of the examination for each student. After the grades are filled the lecturer submits the protocol for the approval. If the protocol is not approved, the lecturer can still change the grading information. Once the course manager approves the protocol, students can view the examination results, and the faculty official responsible for the study programs, can use it to prepare the final study report of the semester.

Roles: student, course manager, lecturer, and faculty official.

![Examination Protocol](attachment:image.png)

Fig. 5. Examination protocol
Creativity – your key to secure software!!!

Multiple-Choice Questionnaire
[Each correctly answered question gives 1 point]

1. What is risk migration?
   a) A risk treatment decision to share with another party the burden of loss from a risk;
   b) A risk treatment decision not to become involved in a risk;
   c) A risk treatment decision to accept the burden of loss from a risk;
   d) A risk treatment decision to lessen the negative consequence associated with the risk;
   e) All a, b, c and d;
   f) Neither a, b, c nor d.

2. What is security needs?
   a) A standard means by which a threat agent carries out a threat;
   b) A security objective that characterises the application of a security criterion on a business asset;
   c) A property on business asset that describes object effectiveness, availability and defensibility;
   d) A characteristic of business asset that constitute a weakness or a flaw in terms of security;
   e) All a, b, c and d;
   f) Neither a, b, c nor d.

3. What are attack trees?
   a) A potential attack, carried out by an agent that may lead to harm to assets;
   b) A combination of a threat vulnerabilities and impact;
   c) A way of thinking and describing security of systems and subsystems;
   d) A way of capturing security expertise and reusing it;
   e) All a, b, c and d;
   f) Neither a, b, c nor d.

4. To what functionality components system could be decomposed?
   a) Distributed controls;
   b) Communication and addressing;
   c) User interactions;
   d) Data/storage and resource management;
   e) All a, b, c and d;
   f) Neither a, b, c nor d.

5. What is dependability?
   a) Degree to which essential, mission-critical services continue to be neglected in spite of either accident or malicious harm;
   b) Degree to which various kinds of users can depend on a work product;
   c) A target of safety level that is expected to meet by the information system;
   d) Estimation of trustworthy characteristics of the analysed system;
   e) All a, b, c and d;
   f) Neither a, b, c nor d.
6. What is phishing?
   a) Trojan horse variant that uses physical media and relies on curiosity of victim;
   b) Action of stealthily observing the target to obtain confidential information;
   c) Act of creating and using an invented scenario to divulge target’s sensitive information;
   d) Giving something to get something in return;
   e) All a, b, c and d;
   f) Neither a, b, c nor d.

7. What is OWASP?
   a) A device (as a hook) for holding objects or parts together;
   b) Cigital security touchpoints;
   c) Open web application security project;
   d) Comprehensive lightweight application security process;
   e) All a, b, c and d;
   f) Neither a, b, c nor d.

8. What is security pattern?
   a) A particular recurring security problem;
   b) A specific security context where problems occur;
   c) A well-proven generic security scheme for a security solution;
   d) All a, b, and c;
   e) Neither a, b, c nor d.

9. What is anonymity?
   a) When pseudonyms are used as identifiers;
   b) When it is not possible sufficiently distinguish whether item of interest exists or not;
   c) When is not possible sufficiently distinguish whether these items of interest are related or not;
   d) When item of interest is not identifiable within a set of subjects;
   e) All a, b, c and d;
   f) Neither a, b, c nor d.

10. What are integrity 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.