PART I: Meeting Scheduling example

Description: Electronic meeting Scheduling system helps meeting initiator to schedule a meeting. The major functionality includes the process of agreeing about the meeting date and place. Potentially, in the specific cases, the details (e.g., time, date and place) of the meeting agreement could be known only to the interested and targeted audience. As such the scheduling problem could involve different security concerns including analysis of the social engineering attacks, privacy, trust and trustworthiness, scripting attacks and similar.

An extract of the model for the security risk management in the meeting Scheduler case is provided in Fig. 1, 2, 3, and 4. The model is created using the security risk-aware Secure Tropos language and it gives the analyses viewpoints on assets (Fig. 1), security risks (Fig. 2 and 3), and security risk treatment (Fig. 4).

Fig. 1. Meeting Scheduler: asset analysis and determination of security objectives
Creativity – your key to secure software!!!

**Fig. 2.** Meeting Scheduler: initial analysis of security risk(s)

**Fig. 3.** Meeting Scheduler: security risk analysis

**Fig. 4.** Meeting Scheduler: 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, 3 and 4

**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) &lt;business asset(s), information system assets, security criterion, …&gt; in the meeting Scheduler example, given Fig. 1, 2, 3, and 4?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assets</td>
<td>Business assets</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).

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 Secure Tropos!!*) 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)* BPMN, *(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; *(15 points)*

**Task 4:** How does the security risk constitute itself; *(15 points)*

**Task 5:** What is the countermeasure (i.e., risk treatment, security requirements, and controls), and how does it mitigate the security risk. *(15 points)*

**Note:** Although a picture is worth 1000 words, short textual explanations of the diagrams are welcome!
PART II: Example of examination protocol

Developers of the university information system have sent us a description and an example of the examination protocol. They have requested a help to define what access could be granted to different stakeholders.

**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 Nr.:** MT2013/2014-QWERTY00543

**Faculty:** Faculty of Mathematics and Computer Science  
**Subject:** MTAT.03.246 Principles of Secure Software Design  
**Credits:** 3 ECTS  
**Study year:** 2012/2013  
**Exam date/place:** 30-04-2014, 10:15-14:00, J. Liivi 2-111  
**Lecturer:** Raimundas Matulevičius

<table>
<thead>
<tr>
<th>No</th>
<th>Student ID</th>
<th>Name, surname</th>
<th>Study program</th>
<th>Grade</th>
<th>Examination date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A23456</td>
<td>Mait Saar</td>
<td>MT, 1st year, Regular, mas., Software Engineering</td>
<td>A (Excellent)</td>
<td>30-04-2013</td>
</tr>
<tr>
<td>2</td>
<td>B09876</td>
<td>John Siim Jeferson</td>
<td>MT, 1st year, Regular, mas., Cybersecurity</td>
<td>F (Failed)</td>
<td>30-04-2013</td>
</tr>
<tr>
<td>3</td>
<td>C23443</td>
<td>Arunas Miliauskas</td>
<td>MT, 1st year, Regular, mas., Cybersecurity</td>
<td>C (Good)</td>
<td>30-04-2013</td>
</tr>
</tbody>
</table>

Signature of the Lecturer

**Status:** NOT APPROVED

---

**Fig. 5.** Examination protocol
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 points)
- Users, Roles, and User assignments (5 points)
- Permissions, Permissions assignment (5 points)
- Security actions (as separate class diagram) (5 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 points)
BONUS – A Multiple-Choice Questionnaire

[Each correctly answered question gives you 1 point]

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

2. 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.

3. What are authentication requirements?
   a) 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;
   b) Requirements that characterise the extent to which a business, application, or component shall verify the identity of its externals before interacting;
   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.

4. What is a risk event?
   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.
5. What is risk retention?
   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.

6. What are the problems of input validation and representation?
   a) Password management;
   b) Cross-site scripting attacks;
   c) Command injection;
   d) SQL injection;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

7. 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 it discard design alternatives that do not offer a sufficient security level;
   c) Because it help re-scope or cancel a project if the risk is too high;
   d) Because the need to secure systems and software becomes a necessity rather than an option;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.

8. What is an access control?
   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.

9. What is tailgating?
   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) Following an authorised person into a building;
   e) All a, b, c, and d;
   f) Neither a, b, c, nor d.