About the Course

Course material

<https://courses.cs.ut.ee/2022/SSD/>

- Lectures
  - Links to slides and videos
- Reading
  - Self-study material
  - Articles and other readings
- Upload
- Grading
- Exam
Lecture 1
Development Process for Secure Software

Microsoft SSDL
OWASP CLASP
Seven Touchpoints
Lecture 2

Modelling Perspective

- Structural perspective
- Goal and rule perspective
- Functional perspective
- System model
- Actor and role perspective
- Behavioral perspective
- Topological perspective

Lecture (3), 4 and 5

Workshop 1
Key Tasks

Describe:

1. What is the system?
2. What is its architecture (layers)?
3. What are
   – system assets,
   – business asset and their security criteria

4. Create models for
   – System architecture
   – System and business assets and their security criteria

You need to use at least four different modelling perspectives (and four modelling languages), for example:
   – Structural (**UML class diagrams**), Functional (**BPMN**), Behavioural (**UML use cases**), Actor and role (**i*/ **Tropos**) and other perspectives
   – Models can be at the different level of abstraction

5. Define and maintain **Team management plan**
6. Prepare and present your solution
Lecture 6

Define Risk Explicitly
Lecture 7

Security Risk-oriented BPMN
Lecture 7

Security risk-aware Secure Tropos

- Identify risks and estimate them qualitatively or quantitatively
Lecture 7

Security Risk-oriented misuse cases

Context and asset identification

Determination of security objectives

Risk analysis and assessment

Risk treatment

Security requirements definition

Control selection and implementation

Incorrect game report stored in game storage

Submit game report

Update game report

Check umpire's login and password

Check game storage access repeatedly

Obtain umpire's login name

Collect info about accessing game report

Change game report

ERIS

Integrity of game report

Number of checks is not limited

Security criterion

impact

constraint of

harm

threaten

lead to

include

exploit

include

include

include

include

include
Lecture 7
Mal-activities for security risk management
Lecture 8, 9 and 10

Workshop 2
Key Tasks

1. What are security risks?
   • Each team member should propose at least 2 security risks
   • For each risk:
     o it must be clear what are threat agent, attack method, vulnerability and impact
     o it must be clear which system asset(s) is (are) **targeted** by the identified risk

2. For one risk of your choice
   • create security risk management model using security risk-oriented BPMN
   • Write information which was not possible to express using this language

3. For another risk of your choice
   • create security risk management model using security risk-aware Secure Tropos
   • Write information which was not possible to express using this language

4. For the third risk of your choice
   • create security risk management model using security risk-oriented misuse cases
   • Write information which was not possible to express using this language

5. For the fourth risk of your choice
   • create security risk management model using Mal-activities for security risk management
   • Write information which was not possible to express using this language

6. (OPTIONAL!!!) Continue maintaining team management plan

7. Prepare and present your solution
Lecture 11

Security Requirements

- Identification requirements
- Authentication requirements
- Authorisation requirements
- Immunity requirements
- Integrity requirements
- Intrusion detection requirements
- Privacy requirements
- System maintenance security requirements
- Physical protection requirements
- Survivability requirements
- Security auditing requirements
- Nonrepudiation requirements

Security requirements modelling
Lecture 11

Security Metrics

- **Risk1**: Blacklisted passenger presents fake document, gets checked-in because personnel could be bribed.

- **Risk2**: Attacker uses phishing email to extract passenger booking number and uses it to check-in to the flight.

- **Risk3**: The personnel records values lower than actual weight of luggage and ground operations uses the information in the loading of the aircraft.

- **Risk4**: The personnel accepts luggage and adds contraband items to a passenger’s luggage.

- **Fuel slip**
  - **Risk5**: A malicious insider with access to the computer that stores the fuel slip performs changes to the data contained in the fuel slip.
  - **Risk6**: The attacker intercepts the fuel slip, changes the data contained in it, and sends it to the supplier.

- **Cargo assignment**
  - **Risk7**: A malicious insider with access rights performs changes to the cargo assignment document before it is sent to a service provider.
  - **Risk8**: An attacker hacks the airline mailing list, receives the cargo assignment, changes the data contained and sends the cargo assignment to a service provider.

---

**Lecture 11 Security Metrics**

- **Risk reduction level vs Value**
- **Risk reduction level vs Cost**
- **Cost vs Value**
Lecture 12

RBAC

Sandhu and Coyne, 1996; Ferraiolo et al., 2001
Secure UML model

UMLsec model
Model Driven Security

- Security model is translated to security code
- Software code and security code are generated into system architectures
Lectures 13, 14, 15

Workshop 3
Key Tasks (1)

1. What are security requirements?
   - Each risk identified in workshop 2
     - **Write security requirements which should mitigate these risks**
     - Security requirements must be written according to the criteria of good requirements

What are security controls which implement security requirements and mitigate the identified risks?
   - Explain shortly how (where) the controls should be implemented in the system
Key Tasks (2)

Role-base access control

2. Write down scenario where Role-base access control policy could be applied in the Scenario, which you selected/analysed in previous Workshops
   • Your scenario should include:
     – At least three different roles
     – Data / Form, to which different roles would have different access permissions

3. Select either SecureUML or UMLsec and model the RBAC policy for scenario written in task 2
Phishing Assignment

Pre-questionnaire results:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Average</td>
<td>11.67 / 20 points</td>
</tr>
<tr>
<td>Median</td>
<td>12 / 20 points</td>
</tr>
<tr>
<td>Range</td>
<td>6 - 16 points</td>
</tr>
</tbody>
</table>

Total points distribution

DEADLINE to complete the Phishing Assignment
2. June
Modalities and Assessment

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Team formation</td>
<td>2</td>
</tr>
<tr>
<td>Workshop 1</td>
<td>10</td>
</tr>
<tr>
<td>Workshop 1 presentation</td>
<td>5</td>
</tr>
<tr>
<td>Post-workshop 1 questionnaire</td>
<td>2</td>
</tr>
<tr>
<td>Workshop 2</td>
<td>10</td>
</tr>
<tr>
<td>Workshop 2 presentation</td>
<td>5</td>
</tr>
<tr>
<td>Post-workshop 2 questionnaire</td>
<td>2</td>
</tr>
<tr>
<td>Workshop 3</td>
<td>10</td>
</tr>
<tr>
<td>Workshop 3 presentation</td>
<td>5</td>
</tr>
<tr>
<td>Post-workshop 3 questionnaire</td>
<td>2</td>
</tr>
<tr>
<td>Examination</td>
<td>40</td>
</tr>
<tr>
<td>Phishing assignment</td>
<td>10</td>
</tr>
<tr>
<td>(as part of the exam grade)</td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>103</strong></td>
</tr>
</tbody>
</table>

To be admitted to the exam, at least **33** points from the practical assignments (workshop, presentations, questionnaires) need to be collected during the semester.

- **Exam**
  - Open book
  - Examples of exam tasks could be found at [https://courses.cs.ut.ee/2022/SSD/Main/Exam](https://courses.cs.ut.ee/2022/SSD/Main/Exam)

<table>
<thead>
<tr>
<th>Points Range</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>91-100</td>
<td>A</td>
</tr>
<tr>
<td>81-90</td>
<td>B</td>
</tr>
<tr>
<td>71-80</td>
<td>C</td>
</tr>
<tr>
<td>61-70</td>
<td>D</td>
</tr>
<tr>
<td>51-60</td>
<td>E</td>
</tr>
<tr>
<td>6-50</td>
<td>F</td>
</tr>
<tr>
<td>0-5</td>
<td>Not attended</td>
</tr>
</tbody>
</table>

- 91-100 points – A
- 81-90 points – B
- 71-80 points – C
- 61-70 points – D
- 51-60 points – E
- 6-50 points – F
- 0-5 points – Not attended
Modalities and Assessment

<table>
<thead>
<tr>
<th>Activity</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Team formation</td>
<td>2</td>
</tr>
<tr>
<td>Workshop 1</td>
<td>10</td>
</tr>
<tr>
<td>Workshop 1 presentation</td>
<td>5</td>
</tr>
<tr>
<td>Post-workshop 1 questionnaire</td>
<td>2</td>
</tr>
<tr>
<td>Workshop 2</td>
<td>10</td>
</tr>
<tr>
<td>Workshop 2 presentation</td>
<td>5</td>
</tr>
<tr>
<td>Post-workshop 2 questionnaire</td>
<td>2</td>
</tr>
<tr>
<td>Workshop 3</td>
<td>10</td>
</tr>
<tr>
<td>Workshop 3 presentation</td>
<td>5</td>
</tr>
<tr>
<td>Post-workshop 3 questionnaire</td>
<td>2</td>
</tr>
<tr>
<td>Examination</td>
<td>40</td>
</tr>
<tr>
<td>Phishing assignment (as part of the exam)</td>
<td>10</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>103</strong></td>
</tr>
</tbody>
</table>

To be admitted to the exam, at least 33 points from the practical assignments (workshop, presentations, questionnaires) need to be collected during the semester.

- **Exam**
  - Open book

If you passed the course:
- There will be no extra assignments
- You will not be allowed to retake the exam

<table>
<thead>
<tr>
<th>Score Range</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>91-100 points</td>
<td>A</td>
</tr>
<tr>
<td>81-90 points</td>
<td>B</td>
</tr>
<tr>
<td>71-80 points</td>
<td>C</td>
</tr>
<tr>
<td>61-70 points</td>
<td>D</td>
</tr>
<tr>
<td>51-60 points</td>
<td>E</td>
</tr>
<tr>
<td>6-50 points</td>
<td>F</td>
</tr>
<tr>
<td>0-5 points</td>
<td>Not attended</td>
</tr>
</tbody>
</table>
e-mail: rma@ut.ee
Subject: [SSD2022]