MTAT.03.307

Principles of Secure Software Design

Dr. Raimundas Matulevičius
University of Tartu
email: rma@ut.ee
About the Course

- **Course material** <https://courses.cs.ut.ee/2021/SSD/spring>
  - **Lectures**
    - Links to slides and videos
  - **Practicals**
    - Tests, exercises, and workshop
  - **Readings**
    - Self-study material
    - Articles and other readings
Lecture 1
Lecture 2

Define Risk Explicitly
Lecture 2

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
Lecture 2

Security Metrics

- **Luggage information**
  - **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 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 3 and 4

Workshop 1
Lecture 5
Security Risk-oriented BPMN
Lecture 5

Security risk-aware Secure Tropos

- Identify risks and estimate them qualitatively or quantitatively
Lecture 6
Security Risk-oriented misuse cases
Lecture 6

Mal-activities for security risk management

- Context and asset identification
- Determination of security objectives
- Risk analysis and assessment
- Risk treatment
- Security requirements definition
- Control selection and implementation

[Table]

<table>
<thead>
<tr>
<th>Violator</th>
<th>Intercepted channel</th>
<th>ERIS</th>
<th>Umpire</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intercept transfer of game report</td>
<td>Modify game report</td>
<td>Transmission can be intercepted</td>
<td>Submit game report</td>
</tr>
<tr>
<td>Pass game report</td>
<td>Register game report</td>
<td>Store game report</td>
<td>Integrity of game report</td>
</tr>
</tbody>
</table>

11
Lectures 7, 9, 10

Workshop 2
Lecture 11

RBAC

Sandhu and Coyne, 1996; Ferraiolo et al., 2001
Secure UML model
Lecture 11

Model Driven Security

- Security model is translated to security code
- Software code and security code are generated into system architectures
Lecture 12

X-Road
Lecture 13

Security Patterns

- Identification and authentication
  - Password design and use
  - Biometrics design
  - Hardware token design

- Access control models
  - Authorisation
  - Role-based access control
  - Multi-level security

- Enterprise security and risk management
- Cryptographic key management
  - Cryptographic key generation
  - Public key exchange principles
- Secure Internet applications
  - Information obscurity
  - Secure channels
  - Delimitarised zone
- Firewall architecture
  - Proxy-based firewall
  - Packet filter firewall
  - Statefull firewall
- Operating system access control
  - Single access point
  - Check point
  - Security sessions
- System access control architecture
  - Operation control
  - Resource access
  - File access
- Accounting
  - Non-repudiation
  - Intrusion detection
  - Audit trails and loggings
Lecture 13 and 14

Workshop 3
# Modalities and Assessment

<table>
<thead>
<tr>
<th>Activity</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial course questionnaire</td>
<td>2</td>
</tr>
<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>50</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>105</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 find at [https://courses.cs.ut.ee/2020/SSD/spring/Main/Exam](https://courses.cs.ut.ee/2020/SSD/spring/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>

20
# Modalities and Assessment

<table>
<thead>
<tr>
<th>Activity</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial course questionnaire</td>
<td>2</td>
</tr>
<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 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>50</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/2020/SSD/spring/Main/Exam](https://courses.cs.ut.ee/2020/SSD/spring/Main/Exam)

<table>
<thead>
<tr>
<th>Points 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>

If you passed the course:
- There will be no extra assignments
- You will not be allowed to retake the exam
e-mail: rma@ut.ee
Subject: [SSD2021]