On successful completion of this course

• Identify causes and consequences of (lack of) system and software security

• Master essential techniques to reduce and avoid system and software security problems, to introduce and reason on security requirements and controls

• Apply advanced modelling techniques (notations, tools, and processes) to build secure systems and software
About the Course

- **Course material** <https://courses.cs.ut.ee/2019/ssd/>
  - Lectures
    - Links to slides and videos
  - **Practicals**
    - Tests, exercises, and workshop
  - **Readings**
    - Self-study material
    - Articles and other readings

---

Course outline / Schedule

<table>
<thead>
<tr>
<th></th>
<th>Introduction, ISSRM domain model</th>
<th>14 February</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Security risk, Security requirements, Metrics</td>
<td>21 February</td>
</tr>
<tr>
<td>3</td>
<td><strong>Practicals 1 (test and exercises)</strong></td>
<td>28 February</td>
</tr>
<tr>
<td>4</td>
<td>Security modelling: Securing business processes, Secure goals</td>
<td>7 March</td>
</tr>
<tr>
<td>5</td>
<td><strong>Practicals 2 (test and exercises)</strong></td>
<td>14 March</td>
</tr>
<tr>
<td>6</td>
<td>Security modelling: Securing System Functions and behaviour</td>
<td>21 March</td>
</tr>
<tr>
<td>7</td>
<td>Privacy modelling</td>
<td>28 March</td>
</tr>
<tr>
<td>8</td>
<td><strong>Workshop (day one)</strong></td>
<td>4 April</td>
</tr>
<tr>
<td>9</td>
<td><strong>Workshop (day two)</strong></td>
<td>11 April</td>
</tr>
<tr>
<td>10</td>
<td>Access control</td>
<td>18 April</td>
</tr>
<tr>
<td>11</td>
<td><strong>Practicals 3 (test and exercises)</strong></td>
<td>25 April</td>
</tr>
<tr>
<td>12</td>
<td>Security patterns</td>
<td>2 May</td>
</tr>
<tr>
<td>13</td>
<td><strong>Practicals 4 (test and exercises)</strong></td>
<td>9 May</td>
</tr>
<tr>
<td>14</td>
<td>Guest lectures</td>
<td>16 May</td>
</tr>
<tr>
<td>15</td>
<td>Secure system development approaches, Summary</td>
<td>23 May</td>
</tr>
</tbody>
</table>
Lecture 1
Lecture 2

Define Risk Explicitly

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

- **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.

- **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.

Lecture 3

Practicals 1
Lecture 4

Security Risk-oriented BPMN

Security risk-aware Secure Tropos

- Identify risks and estimate them qualitatively or quantitatively
Lecture 5
Practicals 2

Lecture 6
Security Risk-oriented misuse cases
Lecture 6
Mal-activities for security risk management

Lecture 7
Privacy Modelling
Lecture 7
Privacy Modelling

Lecture 8 & 9
Workshop
Lecture 10

RBAC

Sandhu and Coyne, 1996; Ferraiolo et al., 2001

Secure UML model

UMLsec model
Lecture 10

Model Driven Security

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

Lecture 11

Practicals 3
Lecture 14
Development Process for Secure Software

Modalities and Assessment

- **Practicals** – 40% of the final grade
  - Tests and Exercises
  - Submitted either during lecture or on Mondays next week

- **Workshop** – 20% of the final grade
  - Prepared in teams (4 people)

- **Exam** – 40% of the final grade
  - Examples of exam tasks could be find at [https://courses.cs.ut.ee/2018/ssd/spring/Main/Exam](https://courses.cs.ut.ee/2018/ssd/spring/Main/Exam)
Modalities and Assessment

- **Practicals** – 40% of the final grade
  - Tests and Exercises
  - Submitted either during lecture or on Mondays next week
  - Late submissions will be assessed with 50% grade penalty

- **Workshop** – 20% of the final grade
  - Prepared in teams (4 people)

To be admitted to the exam, at least 30% of grade from the practical assignments need to be collected during the semester

- **Exam** – 40% of the final grade
  - Closed book
  - Examples of exam tasks could be found at [https://courses.cs.ut.ee/2018/ssd/spring/Main/Exam](https://courses.cs.ut.ee/2018/ssd/spring/Main/Exam)

EXAM

Time 1: **30.May**, 12:15-16:00
Time 2: **6.June**, 12:15-16:00

A – 91 and more points
B – 81-90 points
C – 71-80 points
D – 61-70 points
E – 51-60 points
F – 0-50 points