MTAT.03.247
Principles of Secure Software Design: Project Work
(3 ECTS)

Raimundas Matulevičius
Sven Heiberg
Margus Freudenthal
Indrek Saar
Urmas Aavasalu

About the Course

• **Goal:**
  – Analyze a potentially real system, which requires security solutions
  – Apply a systematic way of designing security solutions

• **Course website**
  **No lectures !**

• **Consultations about your project progress with:**
  – Scientific advisor
  – Topic advisor

• **Team work**
  – 3-4 persons

• **Assessment**
  – Performance (20%)
  – Presentation (40%)
  – Report (40%)
    • Be submitted after the presentation
Roles and Responsibilities

Scientific advisor
- advises on solution methods
- evaluates

Student group
- defines
- is analyzed by

Topic advisor
- advises on given problem
- gives
- evaluates

Solution

defines

Topics and People

• Scientific advisor for all projects
  - Raimundas Matulevičius, rma@ut.ee

<table>
<thead>
<tr>
<th>Project</th>
<th>Responsible</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. A Systematic Approach Towards Security Risk-free Systems</td>
<td>Raimundas Matulevičius, <a href="mailto:rma@ut.ee">rma@ut.ee</a></td>
</tr>
<tr>
<td>2. Host/Application-based Intrusion Detection</td>
<td>Sven Heiberg, <a href="mailto:sven@cyber.ee">sven@cyber.ee</a></td>
</tr>
<tr>
<td>3. Attack Tree-based Risk Analysis of p-Voting</td>
<td>Sven Heiberg, <a href="mailto:sven@cyber.ee">sven@cyber.ee</a></td>
</tr>
<tr>
<td>4. Threat-model for Distributed Intrusion Detection Networks</td>
<td>Sven Heiberg, <a href="mailto:sven@cyber.ee">sven@cyber.ee</a></td>
</tr>
<tr>
<td>5. Achieving Long-term Validity and High Performance on Standards-based PKI</td>
<td>Margus Freudenthal, <a href="mailto:margus@cyber.ee">margus@cyber.ee</a></td>
</tr>
<tr>
<td>6. SSL Management Framework/Solution</td>
<td>Indrek Saar, <a href="mailto:Indrek.Saar@playtech.com">Indrek.Saar@playtech.com</a></td>
</tr>
<tr>
<td>7. Javascript Library for HTML5 to Detect Sensitive Data</td>
<td>Indrek Saar, <a href="mailto:Indrek.Saar@playtech.com">Indrek.Saar@playtech.com</a></td>
</tr>
<tr>
<td>8. Security Framework for Software Analyst</td>
<td>Indrek Saar, <a href="mailto:Indrek.Saar@playtech.com">Indrek.Saar@playtech.com</a></td>
</tr>
<tr>
<td>9. Role-based Authentication and Authorization with LDAP + Linux hosts</td>
<td>Indrek Saar, <a href="mailto:Indrek.Saar@playtech.com">Indrek.Saar@playtech.com</a></td>
</tr>
<tr>
<td>10. Erakorralise meditsiini osakonna infosüsteem</td>
<td>Urmas Aavasalu, <a href="mailto:Urmas.Aavasalu@regionaalhaigla.ee">Urmas.Aavasalu@regionaalhaigla.ee</a></td>
</tr>
</tbody>
</table>
Time Schedule
for consultations with scientific advisor

<table>
<thead>
<tr>
<th></th>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.</td>
<td>13. April</td>
<td>Introduction</td>
</tr>
<tr>
<td>1.</td>
<td>20. April</td>
<td>Consultation – 1</td>
</tr>
<tr>
<td>2.</td>
<td>27. April</td>
<td>Consultation – 2</td>
</tr>
<tr>
<td>3.</td>
<td>04. May</td>
<td>Consultation – 3</td>
</tr>
<tr>
<td>4.</td>
<td>11. May</td>
<td>Consultation – 4</td>
</tr>
<tr>
<td>5.</td>
<td>18. May</td>
<td>Presentation – 1 (mandatory participation)</td>
</tr>
<tr>
<td>6.</td>
<td>25. May</td>
<td>Presentation – 2 (mandatory participation)</td>
</tr>
</tbody>
</table>

• The team have to contact the topic advisor and agree about the communication means

Before Consultation 1

• **Form your project team**
  – Find 2-3 colleagues with whom you will make a project
  – Select and divide project team roles

• **Select a project topic**
  – Ask the *scientific advisor* whether the topic is still available
  – Contact the *topic advisor* and establish the way of communication

• **Arrange the first meeting with the topic advisor**
  – The goal of such meeting is to clarify the project topic

• **Prepare for consultation 1 (with scientific advisor)**
  – Check the timing
  – Prepare to present the topic and its goals
  – Prepare to discuss next activities of the project