inf461 - Security of Cyber-Physical Systems

Module label: Security of Cyber-Physical Systems
Module code: inf461
Credit points: 3.0 KP
Workload: 90 h
Used in course of study:
- Master's Programme Computing Science > Theoretische Informatik
- Master's Programme Engineering of Socio-Technical Systems > Systems Engineering

Contact person:
Module responsibility:
- Sibylle Fröschle
- Die im Modul Lehrenden

Authorized examiners:
- Die im Modul Lehrenden
- Sibylle Fröschle

Entry requirements:

Skills to be acquired in this module:

Professional competences:
The students:

- are aware of the threats posed by cyber attacks to cyber-physical systems
- understand security solutions specific to CPS
- know examples of security architectures of CPS
- are able to apply this knowledge to assess the risk of cyber attacks to a given CPS as well as
to develop a conceptual systems security architecture for it

Methodological competences:
The students:

- carry out a threat and risk assessment for a given CPS
- formulate security requirements for a given CPS
- develop a systems security architecture for a given CPS to meet them

(These are examples, the exact skills depend on the focus chosen by the student.)

Social competences:
The students:

- are able to master a new topic by self-study and interaction with experts and peers
- are able to explain the significance and facets of security for CPS to experts and non-experts
- are able to expertly discuss security risks and incidents of CPS

Self-competences:
The students:

- follow up and critically assess current developments in the security of CPS including relevant
  security incidents
- are security aware and foster a security culture with respect to CPS and the resulting critical
  infrastructures

Module contents:
Embedded systems in the energy, transportation, and health domains are currently undergoing a
technological transition towards highly networked automated cyber-physical systems (CPS). Such
systems are potentially vulnerable to cyber attacks, and these can have physical impact. This
includes targeted sabotage of a plant (e.g. Stuxnet), large-scale sabotage of infrastructure to cause
economic damage (e.g. attacks against energy grids), and indiscriminate attacks to cause civilian
casualties (e.g. by compromise of transportation systems).
In this module we investigate and discuss security principles, solutions, and architectures for CPS as
well as real-life security incidents. The topics include distance bounding protocols, location tracking
and counter-measures, safety and security engineering of CPS, security in the automotive and
maritime domain including car hacking and vehicle-2-x communication, hacking in the medical
domain, attacks against energy grids, Stuxnet, CPS and society: benefits, risks, acceptance.

Reader's advisory:
Recent scientific papers and reports in the public domain news.
<table>
<thead>
<tr>
<th>Links</th>
<th><a href="http://vhome.offis.de/sibyllef">http://vhome.offis.de/sibyllef</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Language of instruction</td>
<td>English</td>
</tr>
<tr>
<td>Duration (semesters)</td>
<td>1 Semester</td>
</tr>
<tr>
<td>Module frequency</td>
<td>once a year</td>
</tr>
<tr>
<td>Module capacity</td>
<td>unlimited</td>
</tr>
<tr>
<td>Modulelevel</td>
<td>AS (Akzentsetzung / Accentuation)</td>
</tr>
<tr>
<td>Modulart</td>
<td>Pflicht o. Wahlpflicht / compulsory or optioal</td>
</tr>
<tr>
<td>Lern-/Lehrform / Type of program</td>
<td>S or V</td>
</tr>
<tr>
<td>Vorkenntnisse / Previous knowledge</td>
<td>Security</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Examination</th>
<th>Time of examination</th>
<th>Type of examination</th>
</tr>
</thead>
<tbody>
<tr>
<td>Final exam of module</td>
<td>At the end of the lecture period</td>
<td>Presentation and written documentation, oral exam, or exam</td>
</tr>
</tbody>
</table>

Course type: Course or seminar

<table>
<thead>
<tr>
<th>SWS</th>
<th>2.00</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>SuSe and WiSe</td>
</tr>
<tr>
<td>Workload attendance</td>
<td>28 h</td>
</tr>
</tbody>
</table>