### inf460 - Security

<table>
<thead>
<tr>
<th>Module label</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module code</td>
<td>inf460</td>
</tr>
<tr>
<td>Credit points</td>
<td>6.0 KP</td>
</tr>
<tr>
<td>Workload</td>
<td>180 h</td>
</tr>
</tbody>
</table>

**Used in course of study**
- Master's Programme Computing Science > Theoretische Informatik
- Master's Programme Engineering of Socio-Technical Systems > Embedded Brain Computer Interaction
- Master's Programme Engineering of Socio-Technical Systems > Systems Engineering

**Contact person**

- **Module responsibility**
  - Sibylle Fröschle

- **Authorized examiners**
  - Die im Modul Lehrenden
  - Sibylle Fröschle

**Entry requirements**

The goal of this module is to provide a foundation in computer and network security.

**Skills to be acquired in this module**

**Professional competences:**

The students:

- are aware of the threats posed by cyber attacks to computer and network systems
- understand the basic principles and mechanisms to protect a system against these threats
- are able to apply this knowledge to assess the risk of cyber attacks to a given system as well as to develop and evaluate countermeasures against them

**Methodological competences:**

The students:

- carry out a threat and risk assessment
- formulate security requirements for a given system
- identify and apply standard security solutions 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 principles and applications of computer security to experts and non-experts
- are able to expertly discuss security risks and incidents

**Self-competences:**

The students:

- follow up and critically assess current developments in computer security including security incidents
- are security aware in their own behaviour, in their assessment of the systems they work with, and those they develop

**Module contents**

This module provides a broad and comprehensive knowledge in computer security. The topics cover threat analysis and attack trees, essential cryptographic tools, user authentication, access control, malware, intrusion detection and prevention, denial-of-service attacks and defences, software security and trusted systems, and network security.

Students without prior knowledge in computer security focus on basic principles such as listed above. Students with prior knowledge in computer security can deepen their knowledge by studying real-world examples such as the SSL/TLS protocol. Typically, they will illustrate their topic by
discussing a security incident reported in the public domain security news.

Reader’s advisory


Links

- access from http://vhome.offis.de/sibyllef

Language of instruction | English
---|---
Duration (semesters) | 1 Semester
Module frequency | once a year
Module capacity | unlimited
Reference text | Associated with the module(s):
| Security of Cyber-Physical Systems
Modullevel | AS (Akzentsetzung / Accentuation)
Modulart | Pflicht o. Wahlpflicht / compulsory or optional
Lern-/Lehrform / Type of program | V+Ü
Vorkenntnisse / Previous knowledge | - Basic knowledge in security

Examination | Time of examination | Type of examination
---|---|---
Final exam of module | will be specified in class | Presentation and paper, oral exam, or exam (depending on the number of students)

Course type | Course or seminar
---|---
SWS | 2.00
Frequency | SuSe
Workload attendance | 28 h