Important notice: The ISiS package will be offered in 2019–2020 for the last time and is not available for students of the generation 2018–2019. In 2020–2021 only exam possibilities will be available for students who registered in earlier years.

Offered by: Department of Mathematics and Computer Science
Language: English
Interesting for: all Bachelor students (Software Science and Mathematics students with technical interests should consider the Security package instead)
Contact: dr. B.M.M. de Weger (b.m.m.d.weger@tue.nl)
Website: http://www.win.tue.nl/ISiS

ISiS 2019/2020 Overview

This package provides a broad introduction to Information Security, from the perspective of an individual person's (employee's) needs and responsibilities, both in his professional and private life. It is to be expected that engineers in their future work environments will encounter digital fraud, integrity issues and legal issues related to digital information. In all three courses Information Security will be viewed from both technical and societal perspectives. In this package the following disciplines come together: cryptography, digital security engineering, risk theory, law. Students work together in developing a Wiki with a common base of knowledge. Finally each student develops a personal / professional Information Security Roadmap.

<table>
<thead>
<tr>
<th>Course code</th>
<th>Course name</th>
<th>(Quarter/Slot)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2AC10</td>
<td>Information security basics</td>
<td>Quarter 2/ Slot B</td>
</tr>
<tr>
<td>2AC20</td>
<td>Digital security engineering</td>
<td>Quarter 3/ Slot D</td>
</tr>
<tr>
<td>2AC30</td>
<td>Information security roadmap engineering</td>
<td>Quarter 4/ Slot E</td>
</tr>
</tbody>
</table>

Course descriptions

2AC10 Information security basics

A start is made with laying the foundations of knowledge and competences needed for developing an Information Security Roadmap. The basics of Information Security Engineering, in particular the concepts of information risk, confidentiality, integrity, authenticity, availability, and policy, are explained. Introductions to risk theory, applied cryptography and crypto law are given. A framework for the roadmap will be set up, and the technical and legal details – as far as they were covered in the lectures – will be filled in.

2AC20 Digital Security Engineering

The foundation of knowledge and competences from the first course is expanded and completed with topics from system level security (computer security, network security, web security, security architecture, hacking), and penal and civil law. The roadmap develops.

2AC30 Information security roadmap engineering

The third course is a project course in which the basic knowledge from the first two courses is applied and integrated in a detailed personal Information Security Roadmap for use in a personal and a professional environment. Such a roadmap not only describes environmental (e.g. legal) constraints, operational rights and duties and intended behavior of the individual, but also contains a concrete plan of security measures and their technical realization.