Course Description IT-Security

Keywords: attacks, threats, security measures, cryptography

Target Group:	**6th Semester SWB**	**Module Number:**	**SWB 644**
Workload:	**5 ECTS**		**150 h**
Divided into:	**Contact time**		**60 h**
	Self-study		**60 h**
	Exam preparations		**30 h**
Course language:	**German and English**		
Module director:	**Prof. Dr. Dominik Schoop**		
Valid from:	**01.03.2014**		

Requirements:

Background in computer networks and programming

Overall Aims of the Module:

Students will gain understanding of secure system operations.

The following courses contribute to the overall aims of this module:

- Computer Science 1-3
- Operating Systems
- Computer Networks
- IT Security

Aim of this course:
Students will be capable of conducting risk assessments and of selecting from the various security measures available.

Contents:

- IT Security key concepts
- Security weaknesses in network protocols
- System access controls
- System attacks
- Programming for a secure system
- Discrete mathematics
- Cryptography fundamentals
- Modern encryption techniques
- Cryptographic security services
- Authentication systems
- Security management approaches

Literature:

B. Schneier: Angewandte Kryptographie, Pearson Education Deutschland.
M. Bishop: Introduction to Computer Security, Addison Wesley Verlag.
W. Stalling: Sicherheit im Internet, Addison Wesley Verlag.

Offered:

Every semester

Submodules and Assessment:

Type of instruction/learning:	Lecture with self-study and exam preparations
Type of assessment:	Written exam (90 minutes)
Hours per week:	4 SWS
Estimated student workload:	120 hours

Learning outcomes:

Students will be able to identify the safety faults in information technology and the respective selection of security measures that can be taken. They will be proficient in conducting risk evaluations and risk calculations. Additionally, they will be familiar with secure encryption techniques.

Type of instruction/learning:	Laboratory exercises
Type of assessment:	Report and presentation
Hours per week:	1 SWS
Estimated student workload:	30 hours

Learning outcomes:

Students will be capable of executing attack scenarios and identifying security weaknesses in network protocols. They will be able to implement defence measures, as well as apply encryption techniques.

Overall Assessment:

Written exam, non-graded attendance certificate