

## IT-Security

### Attacks, threats, networks, systems, security measures

<b>Target group(s):</b>	7. Semester KTB 7. Semester SWB 7. Semester TIB	<b>Module number</b>	IT 701-23
<b>Workload:</b>	<b>2 Credits</b>		<b>60 Hours</b>
<b>therefrom</b>	<b>Contact hours</b>		<b>30 Hours</b>
	<b>Self study</b>		<b>15 Hours</b>
	<b>Exam preparation</b>		<b>15 Hours</b>
<b>Language of instruction:</b>	German / English		
<b>Module owner:</b>	Prof. Dr. Dominik Schoop		
<b>Date:</b>	01. 10. 2011		

#### Prerequisites:

- Basics in communication technology
- Programming language C

#### Total Target:

Encouragement of safety awareness, ability of risk evaluation and the selection of appropriate security measures in information technology.

#### Module content:

- Fundamental terms of IT-Security
- Basic attacks in computer networks
- Security weaknesses in network protocols (ARP, IP, UDP, TCP, ICMP)
- Attacks against systems (e.g. buffer overflows, viruses, worms)
- Access control in networks with firewalls
- Access control in systems
- Cryptographic Security services (symmetric, asymmetric, hybrid)
- Password authentication systems
- Challenge- Response- authentications systems
- Secure protocols (e.g. SSL, SSH)

#### Reference material:

- M. Bishop: Introduction to Computer Security, Addison-Wesley
- C. Eckert, IT-Sicherheit, Oldenbourg-Verlag
- N. Pohlmann: Firewall-Systeme, MITP-Verlag
- G. W. Selke: Kryptographie – Verfahren, Ziele, Einsatzmöglichkeiten, O'Reilly
- W. Stallings: Sicherheit im Internet, Addison-Wesley
- E. D. Zwicky, S. Cooper, B. Chapman: Building Internet Firewalls, O'Reilly

#### Offered:

Summer semester

#### Submodules and assessment:

<b>Type of instruction:</b>	Lectures with follow-up work and preparation for examination
<b>Type of assessment:</b>	Oral examination, 20 minutes
<b>Semester periods per week:</b>	2 SWS
<b>Estimated student workload:</b>	60 hours
<b>Aims, learning outcomes:</b>	

The students shall be able to recognize security weaknesses in information technology, to estimate the existent risks and apply appropriate counter measures.