Course Description Network Security

Keywords: **Secure Protocols, Authentication, Identity Management, Firewalls, Intrusion Detection**

Audience:	**Semester AIM 1 and AIM 2**	**Modul Number:**	**AIM 800 6625**
Workload:	**5 ECTS**		**150 h**
divided into	**Contact time**		**90 h**
	Self-study		**30 h**
	Exam preparation		**30 h**
Course language:	**English**		
Modul director:	**Prof. Dr. Tobias Heer**		
Valid as of:	**17.12.2020**		

Recommended requirements:

Understanding of computer networks, IT security and cryptography fundaments, basic programming skills

Desired learning outcomes of the module:

Students understand how to protect networks using both basic and advanced security methods.

Knowledge - professional competences

Students know:

- Network security objectives and basic attacks
- Security models for network protocols
- Cryptographic basics for network security protocols
- Security mechanisms on different network layers (PPP, IPsec, TLS, SSH)
- Authentication frameworks and identity management (e.g. OAuth, Kerberos, RADIUS)
- Basic protection solutions and devices (e.g., firewalls, VLAN, VPN, network monitoring, fail2ban)
- Advanced security mechanisms and algorithms (e.g., intrusion detection, honeypots)

Skills - methodical competences

Students are able to

- Perform a security risk analysis for complex network deployments
- Select and implement network security methods
- Segment networks into security zones
- Design networks with regard to security
- Understand and use network security devices
- Understand anonymization techniques and their limitations

Comprehensive Competencies

Students be able to

- Deploy secure networked applications and IT services
- Leverage advanced concepts in network security

Contents:

- Network security goals, attacks and protection mechanisms
- Security mechanisms in the Internet (e.g., VLAN, IEEE 802.1X, IPsec, OpenVPN, TLS, SSH)
- Design and functions of network security protocols
- Authentication frameworks and identity management (e.g., Single-Sign-On, OAuth, Kerberos, PKI)
- Network attacks and counter-measures (e.g., firewalls, intrusion detection systems,)
- Advanced security solutions and research (e.g., intrusion detection, honeypots)
- Secure network operation and network monitoring

Literature:

- W. Stallings: Network Security Essentials, Pearson Prentice Hall, 2007
- N. Ferguson, B. Schneier: Practical Cryptography John Wiley & Sons, 2003
- G. Schäfer, M. Roßberg: Netzsicherheit, 2. Auflage, dpunkt Verlag, 2014
- C. Eckert: IT-Sicherheit, Konzepte-Verfahren-Protokolle, Oldenbourg-Verlag, 2011
- R. Anderson: Security Engineering, Wiley, 2009
- B. Schneier: Applied Cryptography. Protocols, Algorithms, and Source Code in C. Wiley, New York 1996.

Offered:

Every summer semester

Submodules and Assessment:

Type of instruction:	Lecture with exercises and project work
Type of assessment:	Exam (90 minutes)
Hours per week:	4 SWS
Estimated student workload:	150 hours

Generation of the module grade:

Exam