Module:	**Network Security**
Lecturer:	MSc. Dennis Boldt
Language:	English
Teaching Method:	Lecture and practical exercise
Credit Points:	1 ECTS
Attendance requirements:	Basic knowledge of operating systems, file systems, computer hardware, and networks.
Goals / Skill:	This lecture provides an overview on network security including theoretical foundations and real-world implementations. It starts with fundamental terms and assumptions that are typical for network security. Following, the basic attacks in networks are discussed and the security services violated by these as well as potential countermeasures are introduced. The practical (non-mathematical, non-theoretical) fundamentals of cryptography are discussed. Authenticity and digital signatures are discussed in detail as they are instrumental for today's commercialized internet. Finally, the implementation of some security services is illustrated at the example of well-known and widely deployed technologies such as SSL/TLs.
Detailed Content:	1. Basics of Network Security (Safety Objectives, Communication Model) 2. Attacker Model and Attack Classification 3. Countermeasures, Security Services, and Security Mechanisms 4. Authenticity and Digital Signatures
Media Used:	Electronic Presentation, Blackboard Illustrations, Practical Demonstrations
Literature:	• Bruce Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C, Wiley, ISBN-13: 978-0471117094 • Jon Erickson: Hacking: The Art of Exploitation, No Starch Press, ISBN-13: 978-1593271442
Assigned Tutorial:	OpenSSL • Getting familiar with the OpenSSL software package for data encryption and decryption
Suggested Reading before the start of the summer school:	• William Stallings: Cryptography and Network Security: Principles and Practice, Prentice Hall, ISBN-13: 978-0136097044