Module:	**Applications of Network Security**
Lecturer:	Prof. Dr-Ing. habil. Andreas Ahrens / Prof. Dr. rer. nat.Clemens Cap
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 required knowledge about the most important countermeasure, cryptography, is briefly discussed. A special focus is authenticity and digital signatures 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 Bluetooth, SSL/TLs, and PGP.
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. Cryptography Basics (Substitution and Transposition ciphers, One-Time-Pad, Feistel Networks, Stream- and Block-Ciphers, One-Way Functions) 5. Authenticity and Digital Signatures 6. Real-World Examples (Bluetooth, SSL/TLS, PGP)
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 Tutorials:	Tutorial 1: OpenSSL • Getting familiar with the OpenSSL software package for data encryption and decryption Tutorial 2: RSA & PGP • Getting familiar with RSA encryption and decryption as well as PGP for signing, encrypting and decrypting texts, e-mails, files and directories
Suggested Reading before the start of the summer school:	William Stallings: Cryptography and Network Security: Principles and Practice, Prentice Hall, ISBN-13: 978-0136097044