Module:	**Mobile Computing and Security Testing**
Lecturer:	Prof. Dr.-Ing. Thomas Kemmerich
Language:	English
Teaching Method:	Lecture and practical exercise
Credit Points:	1 ECTS
Attendance requirements:	Basic knowledge of mobile operating systems, file systems, computer hardware and networks
Goals / Skill:	This lecture consists of two parts which are independent from each other: Smart devices like smartphones, tablets, smart watches etc. are becoming more and more popular also in the business world of computing. The first part of the lecture gives an introduction to mobile security. Different operating systems are available for smart devices and the question is what are the structures and methodologies in serving a secure environment. Technical and organizational measures will be discussed to secure the devices and the applications. In the second part we will discuss several penetration testing methods for practical usage during the following tutorial. This includes tools like Wireshark, nmap and frameworks like metasploit. During the Tutorial the basics of hacker tools are introduced and the students shall penetrate a local IT-System. Two groups can compete in securing and penetrating a dedicated Web-and DB-server.
Detailed Content:	1. Mobile communication using Smart devices. 2. Security concepts of different systems, IOS, Android, BB, Windows Phone 3. Technical and organizational measures securing smart devices 4. Penetration testing According to the lecture the practical laboratory is introduced where the students will penetrate a prepared IT-System with some common hacker tools
Media Used:	Electronic Presentation, Blackboard Illustrations, Practical Demonstrations, practical network and device access
Literature:	Security Engineering: A Guide to Building Dependable Distributed Systems, Ross Anderson Corporate Computer and Network Security [Hardcover] Raymond Pankow, Prentice Hall, 2010 ISO/IEC 27001 Standards Computer Networks, Andrew S. Tanenbaum, Prentice Hall 2003 http://www.metasploit.com http://nmap.org http://www.wireshark.org
Assigned Tutorials:	Tutorial 3: Observation, Analytics and Anonymity Techniques • Understand the tracking and observation techniques, to provide knowledge on countermeasures and to sensitize to possible use and misuse Tutorial 4: Cracking • Learning the possibilities with penetration test tools to gather security relevant information of a dedicated server system
Suggested Reading before the start of the summer school:	DRAFT Cloud Computing Synopsis and Recommendations, www.nist.gov http://www.metasploit.com