

Modul PSI-IntroSP-B Introduction to Security and Privacy <i>Introduction to Security and Privacy</i>	6 ECTS / 180 h
(seit WS19/20) Modulverantwortliche/r: Prof. Dr. Dominik Herrmann	
Inhalte: This module introduces students to the most fundamental concepts in the fields of information security and the protection of privacy. It provides a broad overview over the most relevant topics from a technical perspective. The focus lies on practical issues that have to be considered when professional and personal information systems are built and operated.	
Lernziele/Kompetenzen: Successful students will know the mathematical background behind basic cryptographic primitives and be able to explain fundamental concepts of information security and privacy, including classical attacks and defenses. They will be able to apply their knowledge when implementing simple attack programs and configuring security properties of selected systems.	
Sonstige Informationen: This module is taught in English. It consists of a lecture and tutorials. During the course of the tutorials there will be theoretical and practical assignments (task sheets). Assignments and exam questions can be answered in English or German. Workload breakdown: <ul style="list-style-type: none"> • Lecture: 22.5 hours (2 hours per week) • Tutorials: 22.5 hours (2 hours per week) • Preparation and studying during the semester: 30 hours • Assignments: 67.5 hours • Preparation for the exam (including the exam itself): 37.5 hours 	
Zulassungsvoraussetzung für die Belegung des Moduls: keine	
Empfohlene Vorkenntnisse: It is strongly recommended to take this module only after successful completion of PSI-EIRBS-B, which lays the foundation for PSI-IntroSP-B. To be successful in PSI-IntroSP-B, participants should already be familiar with fundamentals of computer architecture (binary representation of strings and numbers in computers, bitwise operators like XOR, operation of a CPU, basics of assembly language), operating systems (memory layout and process management), and computer networks (basic IP routing and addressing, TCP/IP connection establishment). Finally, basic familiarity with the Linux command line is recommended. Moreover, basic familiarity with common web technologies (HTTP, HTML, JavaScript) as well as relational database systems and SQL is recommended. Finally, participants should have working knowledge in	Besondere Bestehensvoraussetzungen: keine

at least one programming language (e.g., Python, C, or Java) so that they can write small tools for automation purposes on demand.		
Angebotshäufigkeit: WS, jährlich	Empfohlenes Fachsemester:	Minimale Dauer des Moduls: 1 Semester

Lehrveranstaltungen	
1. Introduction to Security and Privacy Lehrformen: Vorlesung Sprache: Englisch Angebotshäufigkeit: WS, jährlich	2,00 SWS
Lernziele: cf. module description	
Inhalte: Selected topics <ul style="list-style-type: none"> • Security Terminology (protection goals, attacker and attack types) • Authentication and Authorization Fundamentals • Software Security in C and Assembler (e.g., buffer overflows, selected defenses) • Cryptography (e.g., historic ciphers, symmetric and asymmetric systems, Diffie-Hellman key exchange, TLS protocol) • Network Security (spoofing, denial of service, authentication protocols, intrusion detection systems) • Web Security (attacks and defenses related to the OWASP Top 10 including SQL injections and Cross Site Scripting) • Privacy and Techniques for Data Protection (re-identification risks, anonymization networks, k-anonymity, the idea of differential privacy) 	
Literatur: Selected books: <ul style="list-style-type: none"> • A. Shostack: Threat Modelling • W. Stallings: Computer Security: Principles and Practice • J. Erickson: Hacking: The Art of Exploitation 	
2. Introduction to Security and Privacy Lehrformen: Übung Sprache: Englisch Angebotshäufigkeit: WS, jährlich	2,00 SWS

Prüfung schriftliche Prüfung (Klausur) / Prüfungsdauer: 90 Minuten Beschreibung: The content that is relevant for the exam consists of the content presented in the lecture and tutorials (including the assignments). The maximum number of points that can be achieved in the exam is 100.	
---	--

Participants that solve all assignments correctly can collect up to 20 bonus points. Details regarding the number of assignments, the number of points per assignment, and the type of assignments will be announced in the first lecture. If the points achieved in the exam are sufficient to pass the exam on its own (generally, this is the case when at least 50 points have been obtained), the bonus points will be added to the points achieved in the exam. The grade 1.0 can be achieved without the bonus points.

Assignments and exam questions can be answered in English or German.