Modul PSI-AdvaSP-M Advanced Security and Privacy *Advanced Security and Privacy*	6 ECTS / 180 h 45 h Präsenzzeit 135 h Selbststudium

(seit SS18)
Modulverantwortliche/r: Prof. Dr. Dominik Herrmann

Inhalte:

Information security and privacy are relevant in almost all information systems today. Many real-world use cases have complex security and privacy requirements involving multiple parties. Often there are multiple stakeholders with different, sometimes even contradictory interests. For instance, some use cases call for a solution that allows a service provider to process sensitive data without learning its content. In other cases it is not the content but some meta information such as location and usage intensity that has to be protected. And then there are scenarios where seemingly harmless pieces of data can be used to disclose or infer very personal pieces of information about an individual.

This module covers advanced techniques for information security and privacy that can be used to satisfy the complex requirements of practical systems. It builds upon the basic concepts in information security that are introduced in the module "Introduction to Security and Privacy" (PSI-IntroSP-B).

Lernziele/Kompetenzen:

This module is designed to bring students towards the research boundaries in the field of security and privacy technologies by covering a selection of contemporary topics in depth. The focus of the module is on technical safeguards that can be used by system designers and users to enforce properties such as confidentiality and integrity. Moreover, sophisticated attacks on security and privacy are explained.

Successful students will be able to explain attack strategies and defenses discussed in recent research papers. They will also be able to analyze whether a particular attack or defense is relevant in a specific scenario. Finally, they will be able to implement selected attacks and defenses with a programming language of their choice.

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.

Lecture and tutorials are partially taught in form of a paper reading class. Participants are expected to read the provided literature in advance and participate in the discussions.

Workload breakdown:

- 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: Participants should be familiar with basic concepts in information security and privacy, which can be acquired, for instance, by taking	**Besondere Bestehensvoraussetzungen:** keine

the module "Introduction to Security and Privacy" (PSI-IntroSP-B). This includes basic knowledge about the commonly used security terminology, common types of malware and attacks, buffer overflows and related attacks, cryptography, network security, web security, and concepts of privacy. Moreover, participants should have practical experience with at least one scripting or programming language such as Python or Java.

Angebotshäufigkeit: SS, jährlich	**Empfohlenes Fachsemester:**	**Minimale Dauer des Moduls:** 1 Semester

Lehrveranstaltungen	
1. Advanced Security and Privacy **Lehrformen:** Vorlesung **Sprache:** Englisch/Deutsch **Angebotshäufigkeit:** SS, jährlich	**2,00 SWS**

Lernziele:

cf. module description

Inhalte:

Selected topics:

- Cryptographic methods and protocols, e.g., homomorphic encryption, attribute-based credentials, secure multi-party computation, zero-knowledge proofs, format-preserving and identity-based encryption, group signatures, and proxy re-encryption.
- Attacks on privacy in datasets and communications (inference techniques, online tracking)
- Privacy engineering and privacy enhancing technologies (e.g., Tor)
- Usable security and privacy
- Other current topics in privacy and security

Some parts of the lecture are aligned with current events and recently published research. The selected topics are therefore subject to change.

Literatur:

Selected books:

- R. Anderson: Security Engineering
- A. Shostack: Threat Modelling
- J.-P. Aumasson: Serious Cryptography
- W. Stallings: Computer Security: Principles and Practice
- B. Schneier et al.: Cryptography Engineering
- J. Erickson: Hacking: The Art of Exploitation
- J. Katz & Y. Lindell: Introduction to Modern Cryptography
- L. Cranor & S. Garfinkel: Security and Usability

2. Tutorials for Advanced Security and Privacy **Lehrformen:** Übung **Sprache:** Englisch/Deutsch **Angebotshäufigkeit:** SS, jährlich	**2,00 SWS**

Prüfung
schriftliche Modulprüfung (Klausur) / Prüfungsdauer: 90 Minuten
zentral organisiert: ja
Beschreibung:
The written exam may be replaced with an *oral exam* (20 minutes). The type of examination that applies within a semester will be announced in the first lecture at the beginning of the semester. The same type of examination will be used for the repeat exam in the consecutive semester.

The content that is relevant for the exam consists of the content presented in the lecture and tutorials (including the assignments) as well as the content of the discussed papers. 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.