Informationssicherheit — Prozesse und Systeme *Information Security — Processes and Systems*	Modulnummer: MB-707.05

Master						Zugeordnet zu Masterprofil	Basis	Ergänzung
Pflicht/Wahl	☐					Sicherheit und Qualität (SQ)	☒	☐
Wahl	☒	Basis	☒	Ergänzung	☐	KI, Kognition, Robotik (KIKR)	☐	☐
Sonderfall	☐					Digitale Medien und Interaktion (DMI)	☐	☐

Modulbereich: Praktische und Technische Informatik

Modulteilbereich: 707 Sichere Systeme

Anzahl der SWS	V	UE	K	S	Prak.	Proj.	Σ	Kreditpunkte: 6	Turnus i. d. R. angeboten alle 2 Semester
	0	0	4	0	0	0	4		

Formale Voraussetzungen: -

Inhaltliche Voraussetzungen: Informationssicherheit

Vorgesehenes Semester: ab 1. Semester

Sprache: Deutsch

Ziele: Studierende:

- haben vertiefte Kenntnisse in der Sicherung komplexer soziotechnischer Systeme
- können komplexe kryptographische Sicherheitsprotokolle bewerten und in ihrem Einsatzbereich weiterentwickeln
- verstehen Sicherheit als Prozess mit ihren technischen und nicht-technischen Komponenten
- kennen wichtige Sicherheitsprozesse, so wie sie heute in ISMS eingesetzt werden, und können diese weiterentwickeln

Inhalte: Systeme:

1. Fortgeschrittene Anwendung von Kryptographie
   - ECC und seine Varianten
   - Lebenszyklus kryptographischer Verfahren; Stand aktueller Verfahren
   - Zero-Knowledge-Protokolle, Zero-Knowledge-Password-Proof
   - Zertifikate, Beweiswerterhaltung/LTANS
   - Composability von Sicherheitsprotokollen
   - Browserbasierte Sicherheitsprotokolle (SAML/Liberty, OpenID, OAuth)
2. Grundlagen manipulationssicherer Systeme (tamperproof systems)

Prozesse:

1. Softwaresicherheit
   - Sicherheit im Software-Lifecycle
   - Statische Analyse, Symbolic Execution, Fuzzers usw.
2. Security Management
   - Awareness
   - Incident-Response
   - Logging/Auditing
3. Risk-Assessment
   - Risiko-Wahrnehmung
   - Qualitative und quantitative Modelle
   - Insider-Threat-Modelle
4. Security Usability
   - Usability als Sicherheitsfaktor
   - Benutzbare Autorisierung

Unterlagen (Skripte, Literatur, Programme usw.):		
Form der Prüfung: In der Regel Bearbeitung von Übungsaufgaben und Fachgespräch oder mündliche Prüfung		
Arbeitsaufwand	Präsenz 56 h Übungsbetrieb/Prüfungsvorbereitung 124 h Summe 180 h	
Lehrende: Prof. Dr. C. Bormann		Verantwortlich: Prof. Dr. C. Bormann