Modulbezeichnung	**Informationssicherheit — Prozesse und Systeme**
Modulverantwortliche(r)	Prof. Dr. C. Bormann
Modulart	Pflicht/Wahl ☐ Wahlpflicht ☒
Spezialisierungsbereich	Systemsoftware / Eingebettete Systeme
Dauer des Moduls	1 Semester
Kreditpunkte	6 CP
Arbeitsaufwand	Berechnung des Workloads Präsenz 56 h Übungsbetrieb/Prüfungsvorbereitung 124 h Summe 180 h
Turnus des Moduls	i. d. R. angeboten alle 2 Semester
Voraussetzung für die Teilnahme	Keine ☐ Folgende Inhaltliche Voraussetzungen: Informationssicherheit
Lehr- und Lernformen	Seminar ☐ Vorlesung ☒ Tutorium ☒ Praktikum ☐ Projekt ☐
Lernziele	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

Lerninhalte	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
Prüfungsformen	In der Regel Bearbeitung von Übungsaufgaben und Fachgespräch oder mündliche Prüfung
Literatur	