

Modulbezeichnung	Informationssicherheit — Prozesse und Systeme (Kopie vom Fri May 22 16:43:08 +0200 2020) (deleted:Fri May 22 16:53:43 +0200 2020)								
Modulverantwortliche(r)	Prof. Dr. C. Bormann								
Modulart	Pflicht/Wahl <input type="checkbox"/> Wahlpflicht <input checked="" type="checkbox"/>								
Spezialisierungsbereich	Systemsoftware / Eingebettete Systeme								
Dauer des Moduls	1 Semester								
Kreditpunkte	6 CP								
Arbeitsaufwand	<table> <tr> <td colspan="2">Berechnung des Workloads</td> </tr> <tr> <td>Präsenz</td> <td>56 h</td> </tr> <tr> <td>Übungsbetrieb/Prüfungsvorbereitung</td> <td>124 h</td> </tr> <tr> <td>Summe</td> <td>180 h</td> </tr> </table>	Berechnung des Workloads		Präsenz	56 h	Übungsbetrieb/Prüfungsvorbereitung	124 h	Summe	180 h
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 <input type="checkbox"/> Folgende Inhaltliche Voraussetzungen: Informationssicherheit								
Lehr- und Lernformen	Seminar <input type="checkbox"/> Vorlesung <input checked="" type="checkbox"/> Tutorium <input checked="" type="checkbox"/> Praktikum <input type="checkbox"/> Projekt <input type="checkbox"/>								
Lernziele	<p>Studierende:</p> <ul style="list-style-type: none"> • 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	<p>Systeme:</p> <ol style="list-style-type: none"> 1. Fortgeschrittene Anwendung von Kryptographie <ul style="list-style-type: none"> • 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) <p>Prozesse:</p> <ol style="list-style-type: none"> 1. Softwaresicherheit <ul style="list-style-type: none"> • Sicherheit im Software-Lifecycle • Statische Analyse, Symbolic Execution, Fuzzers usw. 2. Security Management <ul style="list-style-type: none"> • Awareness • Incident-Response • Logging/Auditing 3. Risk-Assessment <ul style="list-style-type: none"> • Risiko-Wahrnehmung • Qualitative und quantitative Modelle • Insider-Threat-Modelle 4. Security Usability <ul style="list-style-type: none"> • Usability als Sicherheitsfaktor • Benutzbare Autorisierung
Prüfungsformen	In der Regel Bearbeitung von Übungsaufgaben und Fachgespräch oder mündliche Prüfung
Literatur	