

Informationssicherheit — Prozesse und Systeme							Modulnummer:		
<i>Information Security — Processes and Systems</i>									
Bachelor Pflicht/Wahl <input checked="" type="checkbox"/> Wahlpflicht <input type="checkbox"/> Wahl <input type="checkbox"/> Sonderfall <input type="checkbox"/>				Modulbereich: Pflicht					
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: <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 									
Inhalte: Systeme: <ol style="list-style-type: none"> 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) Grundlagen manipulationssicherer Systeme (tamperproof systems) 									
Prozesse: <ol style="list-style-type: none"> Softwaresicherheit <ul style="list-style-type: none"> • Sicherheit im Software-Lifecycle • Statische Analyse, Symbolic Execution, Fuzzers usw. Security Management <ul style="list-style-type: none"> • Awareness • Incident-Response • Logging/Auditing Risk-Assessment <ul style="list-style-type: none"> • Risiko-Wahrnehmung • Qualitative und quantitative Modelle • Insider-Threat-Modelle Security Usability <ul style="list-style-type: none"> • 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