

Informationssicherheit — Prozesse und Systeme <i>Information Security — Processes and Systems</i>							Modulnummer: WI-W/10		
Bachelor Pflicht <input type="checkbox"/> Winf-Schwerpunkt-Pflicht <input type="checkbox"/> Winf-Schwerpunkt-Wahlpflicht <input type="checkbox"/> Winf-Wahl <input checked="" type="checkbox"/>				Schwerpunkt Computational Finance <input type="checkbox"/> E-Business <input checked="" type="checkbox"/> IT-Management <input checked="" type="checkbox"/> Logistik <input type="checkbox"/>					
Anzahl der SWS	V 0	UE 0	K 4	S 0	Prak. 0	Proj. 0	Σ 4	Kreditpunkte: 6	Turnus i. d. R. angeboten alle 2 Semester
Formale Voraussetzungen: -									
Inhaltliche Voraussetzungen: Informationssicherheit									
Vorgesehenes Semester: ab 6. 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"> 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) 									
Prozesse: <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 									
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