

Informationssicherheit — Prozesse und Systeme (Kopie vom Fri May 22 16:43:08 +0200 2020) (deleted:Fri May 22 16:53:43 +0200 2020)

Information Security — Processes and Systems

Modulnummer:
MB-707.05

Master

Pflicht/Wahl
 Wahl Basis Ergänzung
 Sonderfall

Zugeordnet zu Masterprofil

	Basis	Ergänzung
Sicherheit und Qualität (SQ)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
KI, Kognition, Robotik (KIKR)	<input type="checkbox"/>	<input type="checkbox"/>
Digitale Medien und Interaktion (DMI)	<input type="checkbox"/>	<input type="checkbox"/>

Modulbereich: Praktische und Technische Informatik

Modulteilbereich: 707 Sichere Systeme

Anzahl der
SWS

V	UE	K	S	Prak.	Proj.	Σ
0	0	4	0	0	0	4

Kreditpunkte: 6

Turnus

i. d. R. angeboten alle 2 Semester

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