Grundlagen der Sicherheitsanalyse und des Designs

Foundations of Security Analysis and Design

Modulnummer: MB-699.04

Master

Pflicht/Wahl ☐
Wahl ☒ Basis ☒ Ergänzung ☐
Sonderfall ☐

Zugeordnet zu Masterprofil

	Basis	Ergänzung
Sicherheit und Qualität (SQ)	☒	☐
KI, Kognition, Robotik (KIKR)	☐	☐
Digitale Medien und Interaktion (DMI)	☐	☐

Modulbereich: Mathematik und Theoretische Informatik

Modulteilbereich: 699 Spezielle Gebiete der Theoretischen Informatik

Anzahl der SWS

V	UE	K	S	Prak.	Proj.	Σ
2	2	0	0	0	0	4

Kreditpunkte: 6

Turnus: i. d. R. jedes Jahr

Formale Voraussetzungen: -

Inhaltliche Voraussetzungen: Kenntnisse in formalen Methoden bzw. Informationssicherheit sind nützlich aber nicht zwingend erforderlich

Vorgesehenes Semester: ab 1. Semester

Sprache: Deutsch

Ziele:

- Verfahren der (formalen) Modellierung von (Informations)Sicherheitsanforderungen und Sicherheitsmechanismen kennen
- Verschiedene Sicherheitsanalysetechniken einschätzen und bewerten können
- Die Modellierungstiefe und deren Auswirkungen auf die Analyse einschätzen und bewerten können
- Das Zusammenspiel von verschiedenen Sicherheitsanforderungen und -garantien verstehen

Inhalte: Grundlagen der Modellierung im Bereich der Informationssicherheit

Design und Analyse von Sicherheitsprotokollen

- Modellierung eines Angreifers
- Prinzipien des Designs von Sicherheitsprotokollen
- Analyse und Verifikation von Sicherheitsprotokollen

Design und Analyse von Sicherheitspolitiken

- Modellierung (formaler) Sicherheitspolitiken
- Grundlagen der Informationsflusskontrolle, Vertraulichkeit und Integrität als Informationsflusseigenschaften
- Zustandsbasierte Informationsflusskontrolle
- sprachbasierte Informationsflusskontrolle und Programmanalyse
- Realisierung von Informationsflusskontrolle durch Zugriffskontrolle

Komposition verschiedener Sicherheitsmechanismen am Beispiel des Semantic Web

Unterlagen (Skripte, Literatur, Programme usw.): Skript bzw. Folien

Dieter Gollmann: Computer Security, Wiley&Sons, 2006

Matt Bishop: Computer Security, Art und Science, Addison Wesley, 2003

Diverse Fachartikel

Form der Prüfung:
Bearbeitung von Übungsaufgaben und Fachgespräch oder mündliche Prüfung

Arbeitsaufwand

Präsenz	56 h
Übungsbetrieb/Prüfungsvorbereitung	124 h
Summe	180 h

Lehrende: Prof. Dr. D. Hutter	Verantwortlich: Prof. Dr. D. Hutter