03-IMAT-GSD	Grundlagen der Sicherheitsanalyse und des Designs
	Foundations of Security Analysis and Design

Lehrform *(teaching format)* / **SWS** *(hours per week)*: 2VL + 2UE

Kreditpunkte *(credit points)*: 6

Turnus *(frequency)*: i.d.R. jedes SoSe

Inhaltliche Voraussetzungen *(content-related prior knowledge/skills)*: Kenntnisse in formalen Methoden bzw. Informationssicherheit sind nützlich aber nicht zwingend erforderlich

Sprache *(language)*: Deutsch

Lehrende *(teaching staff)*: Prof. Dr. Dieter Hutter

Studiengang *(degree program)*	Module	Semester
Informatik (Master)	IMAT, IMA-SQ	ab 1.Sem.
Systems Engineering I/II (Master)	M07-IM-ESS	ab 1./2.Sem.
Informatik (Bachelor)	nur *Freie Wahl*	

Lernergebnisse:

- 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

Learning Outcome:

- To know procedures for the formal modeling of security requirements, and to be able to select and apply appropriate security mechanisms
- To assess and evaluate different security analysis techniques
- To assess and evaluate the depth of modeling and its impact on analysis techniques
- To understand the interplay between different security requirements and guarantees.

Inhalte:

Grundlagen der Modellierung im Bereich der Informationssicherheit

Design und Analyse von Sicherheitsprotokollen

- Modellierung eines Angreifers
- Prinzipien des Designs von Sicherheitsprotokollen
- Techniken zur 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

Contents:

Foundations in modeling aspects of information security

Design and analysis of security protocols

- Modeling of an attacker
- Principles of security protocol design
- Techniques to analyze and verify security protocols

Design and analysis of security policies

- Modeling of (formal) security policies
- Basics of information flow control; confidentiality and integrity as information flow properties
- State-based information flow control
- Language-based information flow control and program analysis
- Realization of information flow control by access control

Composition of different security mechanisms in practice

Hinweise *(remarks)*: In der Tabelle sind nur die primären/spezifischsten Module aufgelistet, denen diese Veranstaltung zugeordnet ist.