

<b>Grundlagen der Sicherheitsanalyse und des Designs</b> <i>Foundations of Security Analysis and Design</i>							Modulnummer: MB-699.04													
Master Pflicht/Wahl <input type="checkbox"/> Wahl <input checked="" type="checkbox"/> Basis <input checked="" type="checkbox"/> Ergänzung <input type="checkbox"/> Sonderfall <input type="checkbox"/>				Zugeordnet zu Masterprofil  <table border="0"> <tr> <td></td> <td style="text-align: right;">Basis</td> <td style="text-align: right;">Ergänzung</td> </tr> <tr> <td>Sicherheit und Qualität (SQ)</td> <td style="text-align: right;"><input checked="" type="checkbox"/></td> <td style="text-align: right;"><input type="checkbox"/></td> </tr> <tr> <td>KI, Kognition, Robotik (KIKR)</td> <td style="text-align: right;"><input type="checkbox"/></td> <td style="text-align: right;"><input type="checkbox"/></td> </tr> <tr> <td>Digitale Medien und Interaktion (DMI)</td> <td style="text-align: right;"><input type="checkbox"/></td> <td style="text-align: right;"><input type="checkbox"/></td> </tr> </table>						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"/>
	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: Mathematik und Theoretische Informatik																				
Modulteilbereich: 699 Spezielle Gebiete der Theoretischen Informatik																				
Anzahl der SWS		V	UE	K	S	Prak.	Proj.	$\Sigma$	Kreditpunkte: 6	Turnus i. d. R. jedes Jahr										
		2	2	0	0	0	0	4												
Formale Voraussetzungen: -																				
Inhaltliche Voraussetzungen: Kenntnisse in formalen Methoden bzw. Informationssicherheit sind nützlich aber nicht zwingend erforderlich																				
Vorgesehenes Semester: ab 1. Semester																				
Sprache: Deutsch																				
Ziele: <ul style="list-style-type: none"> <li>• Verfahren der (formalen) Modellierung von (Informations)Sicherheitsanforderungen und Sicherheitsmechanismen kennen</li> <li>• Verschiedene Sicherheitsanalysetechniken einschätzen und bewerten können</li> <li>• Die Modellierungstiefe und deren Auswirkungen auf die Analyse einschätzen und bewerten können</li> <li>• Das Zusammenspiel von verschiedenen Sicherheitsanforderungen und -garantien verstehen</li> </ul>																				
Inhalte: Grundlagen der Modellierung im Bereich der Informationssicherheit Design und Analyse von Sicherheitsprotokollen <ul style="list-style-type: none"> <li>• Modellierung eines Angreifers</li> <li>• Prinzipien des Designs von Sicherheitsprotokollen</li> <li>• Analyse und Verifikation von Sicherheitsprotokollen</li> </ul> Design und Analyse von Sicherheitspolitiken <ul style="list-style-type: none"> <li>• Modellierung (formaler) Sicherheitspolitiken</li> <li>• Grundlagen der Informationsflusskontrolle, Vertraulichkeit und Integrität als Informationsflusseigenschaften</li> <li>• Zustandsbasierte Informationsflusskontrolle</li> <li>• sprachbasierte Informationsflusskontrolle und Programmanalyse</li> <li>• Realisierung von Informationsflusskontrolle durch Zugriffskontrolle</li> </ul> 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