

<b>Informationssicherheit (Kopie vom Fri May 22 16:52:33 +0200 2020) (deleted:Fri May 22 16:53:53 +0200 2020)</b> <i>Information Security</i>							Modulnummer: BB-707.01														
Bachelor 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 Sicherheit und Qualität (SQ) <input checked="" type="checkbox"/> KI, Kognition, Robotik (KIKR) <input type="checkbox"/> Digitale Medien und Interaktion (DMI) <input type="checkbox"/>																	
Modulbereich: Praktische und Technische Informatik Modulteilbereich: 707 Sichere Systeme																					
Anzahl der SWS		<table border="1"> <thead> <tr> <th>V</th> <th>UE</th> <th>K</th> <th>S</th> <th>Prak.</th> <th>Proj.</th> <th><math>\Sigma</math></th> </tr> </thead> <tbody> <tr> <td>2</td> <td>2</td> <td>0</td> <td>0</td> <td>0</td> <td>0</td> <td>4</td> </tr> </tbody> </table>		V	UE	K	S	Prak.	Proj.	$\Sigma$	2	2	0	0	0	0	4	Kreditpunkte: 6		Turnus i. d. R. angeboten alle 2 Semester	
V	UE	K	S	Prak.	Proj.	$\Sigma$															
2	2	0	0	0	0	4															
Formale Voraussetzungen: -																					
Inhaltliche Voraussetzungen: Technische Informatik 2																					
Vorgesehenes Semester: ab 5. Semester																					
Sprache: Deutsch																					
Ziele: <ul style="list-style-type: none"> <li>• Grundkonzepte der Informationssicherheit kennen;</li> <li>• Die gängigsten Sicherheitsprobleme in heutigen IT-Infrastrukturen und deren Ursachen kennen;</li> <li>• Notwendigkeit für den Einsatz von Sicherheitstechnik erkennen;</li> <li>• Grenzen der im Einsatz befindlichen Technologien einschätzen können;</li> <li>• Verschiedene Bereiche von Sicherheitstechnik einordnen können;</li> <li>• Modelle und Methoden zur systematischen Konstruktion sicherer Systeme kennen.</li> </ul>																					
Inhalte: <ul style="list-style-type: none"> <li>• Grundbegriffe der IT-Sicherheit, Bedrohungen und Sicherheitsprobleme: Vertraulichkeit, Integrität, Verfügbarkeit etc.; Viren, Würmer, Trojanische Pferde etc.</li> <li>• Kryptografie (Symmetrisch, Asymmetrisch, Hash, PRF): DES, 3DES, AES; RSA, DSA; MD5, SHA1; TLS-PRF, PBKDF2</li> <li>• Mechanismen zur Authentisierung und Integritätsprüfung digitaler Signaturen, Zertifikate, PKI</li> <li>• Zugriffskontrolle, Autorisierung, Rollen</li> <li>• Sicherheitsprotokolle, z.B. Schlüsselaustausch Diffie-Hellman, TLS (SSL), Kerberos</li> <li>• Probleme mit Protokollen, Angriffe (fehlende Bindung, Replay, ...)</li> <li>• Netzsicherheit (Firewalls/IDS, VPN, Anwendungssicherheit)</li> <li>• Sicherheit in Layer 2 (GSM, WLAN, ...)</li> <li>• Software-Zertifizierung: Common Criteria</li> <li>• Mobiler Code</li> <li>• Smart Cards, Trusted Computing Platform</li> <li>• Security Engineering</li> <li>• Organisationelle Sicherheit; Security: The Business Case</li> </ul>																					
Unterlagen (Skripte, Literatur, Programme usw.): <ul style="list-style-type: none"> <li>• (deutschsprachig:) Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren - Protokolle; Oldenbourg 2009; 981 Seiten</li> <li>• (englischsprachig:) Ross Anderson: Security engineering: a guide to building dependable distributed systems; Wiley 2008; 1040 Seiten</li> </ul>																					
Form der Prüfung: i.d.R. Bearbeitung von Übungsaufgaben und Fachgespräch oder mündliche Prüfung																					

Arbeitsaufwand	Präsenz	56 h
	Übungsbetrieb/Prüfungsvorbereitung	124 h
	Summe	180 h
Lehrende: Prof. Dr. C. Bormann, Dr. K. Sohr		Verantwortlich: Prof. Dr. C. Bormann