

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