

Modulbezeichnung	<b>Informationssicherheit</b>								
Modulverantwortliche(r)	Prof. Dr. C. Bormann								
Modulart	Pflicht/Wahl <input type="checkbox"/> Wahlpflicht <input checked="" type="checkbox"/>								
Spezialisierungsbereich	Systemsoftware / Eingebettete Systeme								
Dauer des Moduls	1 Semester								
Kreditpunkte	6 CP								
Arbeitsaufwand	<table> <tr> <td>Berechnung des Workloads</td> <td></td> </tr> <tr> <td>Präsenz</td> <td>56 h</td> </tr> <tr> <td>Übungsbetrieb/Prüfungsvorbereitung</td> <td>124 h</td> </tr> <tr> <td>Summe</td> <td>180 h</td> </tr> </table>	Berechnung des Workloads		Präsenz	56 h	Übungsbetrieb/Prüfungsvorbereitung	124 h	Summe	180 h
Berechnung des Workloads									
Präsenz	56 h								
Übungsbetrieb/Prüfungsvorbereitung	124 h								
Summe	180 h								
Turnus des Moduls	i. d. R. angeboten alle 2 Semester								
Voraussetzung für die Teilnahme	Keine <input type="checkbox"/> Folgende Inhaltliche Voraussetzungen: Technische Informatik 2								
Lehr- und Lernformen	Seminar <input type="checkbox"/> Vorlesung <input checked="" type="checkbox"/> Tutorium <input checked="" type="checkbox"/> Praktikum <input type="checkbox"/> Projekt <input type="checkbox"/>								
Lernziele	<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>								
Lerninhalte	<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>								
Prüfungsformen	i.d.R. Bearbeitung von Übungsaufgaben und Fachgespräch oder mündliche Prüfung								

Literatur

- (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