

<b>Modul – Nr.</b>	<b>217</b>		<b>Pflicht</b>
<b>Bezeichnung</b>	<b>IT-Sicherheit</b>		
Verantwortlicher	Prof. M. Schölzel		
Titel der Lehrveranstaltung	IT-Sicherheit		
Prüfungsbezeichnung	IT-Sicherheit		
Fachsemester	6		
Art der Lehrveranstaltung	Sprache	Vorlesung	Deutsch
SWS/ ECTS/ Workload	4 V	5	150 h
Formale Teilnahmebedingungen	keine		
<b>1. Inhalte und Qualifikationsziele</b>			
<b>Inhalte:</b>			
<ol style="list-style-type: none"> <li>1. Einführung in die IT-Sicherheit, Terminologie</li> <li>2. relevante Konzepte der Rechnerkommunikation</li> <li>3. Tools zur Analyse von Netzwerk-Verkehr</li> <li>4. Grundlagen und Einsatzbereiche kryptografischer Protokolle (symmetrische und asymmetrische Kryptografie, Hash-Funktionen, Signaturen, Schlüsselaustausch) sowie deren praktischer Einsatz</li> <li>5. Entwurf von Rechnernetz-Topologien (unter Einsatz von Proxy-Servern, Firewalls, VPN, DMZ) zum Schutz sensibler Daten gegen unbefugten Zugriff</li> <li>6. Verfahren zum Erreichen von Netzwerksicherheit und zum Schutz der Privatsphäre in neuartigen Internet-Anwendungen am Beispiel partizipativer Sensoranwendungen</li> </ol>			
<b>Qualifikationsziele:</b>			
Die Studierenden können Sicherheitsrisiken in vernetzten Rechnersystemen erkennen und bewerten. Sie können Internet-basierte Applikationen durch geeignete Schutzmechanismen absichern. Die Studierenden sind in der Lage, geeignete Netzwerktopologien zum Schutz wichtiger Infrastruktur zu entwerfen. Sie kennen Verfahren zum Schutz der Privatsphäre im Netz und können diese einsetzen.			
<b>2. Lehrformen</b>			
Vorlesung mit integrierten Übungen (4 SWS)			
<b>3. Voraussetzung für die Teilnahme</b>			
Formale Voraussetzungen für die Teilnahme bestehen nicht. Es wird empfohlen, dass die Module „Betriebssysteme und Rechnerorganisation“ und „verteilte Systeme“ vorher absolviert wurden.			
Zur Vorbereitung und Nachbereitung der Vorlesungen wird folgende Literatur empfohlen:			
<ul style="list-style-type: none"> <li>• Claudia Eckert: "IT-Sicherheit: Konzepte - Verfahren - Protokolle", De Gruyter, 9. aktualisierte Auflage, ISBN: 978-3486778489</li> <li>• Charlie Kaufman, Radia Perlman, Mike Speciner: "Network Security – Private Communication in a Public World", 2nd Edition, Prentice Hall, 2002, ISBN: 978-0130460196</li> <li>• Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno: "Cryptography Engineering", John Wiley &amp; Sons, 2010, ISBN 978-0470474242</li> </ul>			
<b>4. Verwendbarkeit der Studieneinheit</b>			
Das Modul ist Pflichtmodul im Studiengang „Informatik“ und kann als Wahlpflichtmodul in den Studiengängen „Internet – Technologie und Anwendungen“ und „Automatisierung und Elektronikentwicklung“ verwendet werden.			
<b>5. Voraussetzungen für die Vergabe von Leistungspunkten</b>			
Voraussetzung für die Vergabe von Leistungspunkten ist das Bestehen der Modulklausur. Die Klausur gilt als bestanden, wenn sie mindestens mit „ausreichend“ bewertet wurde.			
<b>6. Leistungspunkte und Noten</b>			
Die Note entspricht der Benotung der Klausur. Bei erfolgreichem Abschluss des Moduls werden 5 Leistungspunkte (ECTS) vergeben.			
<b>7. Häufigkeit des Angebots der Studieneinheit</b>			
Das Modul wird einmal pro Jahr angeboten, i.d.R. im Sommersemester.			
<b>8. Arbeitsaufwand (work load)</b>			
Der Arbeitsaufwand setzt sich wie folgt zusammen: Besuch der Lehrveranstaltungen: 45 h; Nachbereitung des Vorlesungsstoffes: 65 h; Vorbereitung und Teilnahme an der Klausur: 40 h			
<b>9. Dauer des Studieneinheit</b>			
1 Semester			