

Lehrende/r	Marcel Schaible	Modulbeauftragte/r	Herwig Unger
	Dauer des Moduls ein Semester	ECTS 10	Workload 300 Stunden
			Häufigkeit in jedem Semester
Lehrveranstaltung(en)	01711	Fehlertoleranz in Computersystemen und Netzwerken	WS/SS SWS 2+1
	01867	Sicherheit im Internet II	WS/SS SWS 2+1
Detaillierter Zeitaufwand	Bearbeiten der Kurseinheiten: 140 Stunden Bearbeiten der Übungsaufgaben: 70 Stunden Onlineveranstaltungen und Prüfungsvorbereitung: 90 Stunden		
Qualifikationsziele	<p>Die Studierenden erwerben ein vertieftes Verständnis konkreter Angriffe und Gefahren im Internet. Sie sind in der Lage, Schutzmaßnahmen für einzelne Rechner sowie für Netzwerke zu beurteilen, auch im rechtlichen Kontext, sowie bei der Implementierung solcher Schutzmaßnahmen mitzuwirken.</p> <p>Die Studierenden erwerben grundlegende theoretische Grundlagen auf dem Gebiet der Fehlertoleranz. Sie haben gelernt, dieses Kenntnisse in komplexen Methoden auf praktische Fragestellungen anzuwenden, wobei insbesondere Beispiele aus dem Bereich der Rechnerarchitektur und Kommunikationsnetze im Zielpunkt der Wissensvermittlung stehen.</p>		
Inhalte	<p>01867 vertieft das Thema Sicherheit im Internet und baut dazu auf dem Kurs 01866 "Sicherheit im Internet I" auf. Er besteht aus vier Teilen. Im ersten Teil werden typische Angriffe auf Systeme genauer vorgestellt. Hierzu gehören die Angriffe auf Schwächen in Protokollen ebenso wie Angriffe auf die Konfiguration von Systemen. Spezielle Überwachungs-, bzw. Angriffsprogramme werden vorgestellt. Den Abschluss des ersten Teils bildet ein Abschnitt zu Angriffen auf Verschlüsselungsalgorithmen. Der zweite Teil beschäftigt sich mit der Benutzersicherheit. Ausgehend von typischen E-Commerce Transaktionen werden verschiedene Möglichkeiten zur Bezahlung im Internet mit ihren Eigenschaften vorgestellt. Insbesondere anonyme Bezahlverfahren, also elektronisches Bargeld wird mit den dahinter stehenden Prinzipien diskutiert. Außerdem werden in dieser Kurseinheit einige eher mathematische Aspekte des Thema Sicherheit betrachtet: Advanced Hashing, Primzahltest und Zufallszahlen. Der dritte Teil beschäftigt sich mit der Anbietersicherheit. Konkret geht es um den Aufbau eines privaten Netzes über öffentliche Netzwerke. Dies wird durch Virtual Private Networks (VPN) realisiert. Ihre Basistechnologien und ihr Aufbau werden vorgestellt. Außerdem werden Intrusion Detection Systeme (IDS) zur Unterstützung bei der Erkennung von Angriffen besprochen. Es werden wieder die zugrunde liegenden Techniken und die Eigenschaften von IDS besprochen. Im letzten Teil des Kurses geht es um die Erstellung von sicheren Systemen. Zunächst werden die Rahmenbedingungen (wie beispielsweise gesetzliche Vorschriften) vorgestellt, die Einfluss auf die Eigenschaften sicherer Systeme haben. Anschließend werden Hinweise zu Software Engineering Prozessen gegeben. Die Beachtung dieser Hinweise vereinfacht die Erstellung sicherer Systeme.</p> <p>01711 untersucht nach einer Klärung wichtiger Begriffe sowie der Unterschiede zwischen Fehlertoleranz und Risikominimierung die grundlegenden Arten von Fehlern und Prinzipien der Fehlertoleranz. Dies umfasst zunächst die Behandlung der theoretischen Grundlagen, die im Wesentlichen ein Basiswissen der Wahrscheinlichkeitsrechnung und der Statistik umfassen. Darauf aufbauend werden Ansätze vorgestellt, die zu einer fehlertolerierenden Datenspeicherung und Datenübertragung beitragen. Ein letzter Kursschwerpunkt fokussiert auf die Entwicklung fehlertoleranter Kommunikationssysteme und verteilter Rechnersysteme mittels protokollbasierter Ansätze.</p>		

#### Ergänzende Literatur:

C. Eckert: IT-Sicherheit. 2. Auflage. Oldenbourg 2003  
 R. Oppliger: Security Technologies for the World Wide Web 2nd Edition, Artech House 2003  
 B. Schneier: Applied Cryptography 2nd Edition, Wiley 1996  
 Bacon, J. and Harris, T. (2003). Operating Systems Concurrent and Distributed Software Design. NY: Addison-Wesley.  
 Bertsekas, D. P. and Gallager, R. (1987). Data Networks (2nd Ed.). NJ: Pearson Prentice Hall.  
 Devore, J. L. (2007). Probability and Statistics for Engineering and the Sciences. CA: Brooks/Cole Publishing Company  
 Koren, I. and Mani Krishna, C. (2007). Fault-Tolerant Systems. CA: Elsevier.  
 Tanenbaum, A. S.(2008). Modern Operating Systems (3rd Ed.). NJ: Pearson Prentice Hall.

**Inhaltliche  
Voraussetzung**

Kurs 01867: Modul 63512 "Sicherheit im Internet" (01866) oder Modul 63017 "Datenbanken und Sicherheit im Internet" (01866) sowie dessen Voraussetzungen, oder äquivalente Kenntnisse

**Lehr- und  
Betreuungsformen**

Kurs 01711: Grundkenntnisse; z.B. aus Modul 63012 "Softwaresysteme" (01801)  
 Kursmaterial  
 Einsendeaufgaben mit Korrektur und/oder Musterlösung  
 Betreuung und Beratung durch Lehrende  
 internetgestütztes Diskussionsforum

**Anmerkung**

Früher Kursnummer 21811, neue Kursnummer 01711  
 Das Modul kann letztmalig im SS 2022 belegt werden. Eine Prüfungsteilnahme ist nur noch bis einschließlich SS 2023 möglich.

**Verwendung des Moduls**

M.Sc. Informatik  
 M.Sc. Praktische Informatik  
 M.Sc. Wirtschaftsinformatik

**Prüfungsformen**

Art der Prüfungsleistung	Voraussetzung
bestandene benotete Prüfungsklausur	keine

**Prüfung**

Stellenwert der Note s. PO