

Modul: Secure Software Systems (6 Credits)	
Name im Diploma Supplement	Secure Software Systems
Verantwortlich	Prof. Dr. Lucas Davi
Voraussetzungen	Siehe Prüfungsordnung.
Workload	180 Stunden studentischer Workload gesamt, davon: <ul style="list-style-type: none"> <li>• Präsenzzeit: 60 Stunden</li> <li>• Vorbereitung, Nachbereitung: 75 Stunden</li> <li>• Prüfungsvorbereitung: 45 Stunden</li> </ul>
Dauer	Das Modul erstreckt sich über 1 Semester.
Qualifikationsziele	Die Studierenden <ul style="list-style-type: none"> <li>• kennen die wichtigsten Klassen von Angriffstechniken und Abwehrmethoden im Bereich der Softwaresicherheit von der Applikationsebene bis zum Betriebssystem.</li> <li>• besitzen fundierte Kenntnisse in der Entwicklung von Angriffstechniken auf Softwaresysteme.</li> <li>• sind in der Lage, eigenständig Proof-of-Concept-Angriffe auf Softwaresysteme zu entwickeln.</li> <li>• können konkrete Verfahren zur Härtung von Softwaresystemen gegen fortgeschrittene Softwareangriffe anwenden.</li> <li>• kennen hardware-basierte Verfahren zur Durchsetzung von Softwaresicherheit.</li> <li>• beherrschen die Konzepte von Softwarebasierten Angriffstechniken und Abwehrmethoden auf verschiedenen Rechnerplattformen.</li> <li>• kennen die aktuelle Forschung und Problemstellungen bezüglich der Entwicklung von sicheren Softwaresystemen.</li> </ul>
Prüfungsmodalitäten	Zum Modul erfolgt eine modulbezogene Prüfung in der Gestalt einer Klausur (in der Regel: 90-120 Minuten) oder mündlichen Prüfung (in der Regel: 20-40 Minuten); die konkrete Prüfungsform (Klausur oder mündliche Prüfung) wird in der ersten Woche der Vorlesungszeit von dem zuständigen Dozenten festgelegt.
Verwendung in Studiengängen	<ul style="list-style-type: none"> <li>• LA Info GyGe Master 2014 &gt; Wahlpflichtbereich Informatik &gt; 1.-3. FS, Wahlpflicht</li> <li>• Mathe Master 2013 &gt; Anwendungsfach "Informatik" &gt; weitere Informatik-Module &gt; 1.-4. FS, Wahlpflicht</li> <li>• SNE Master 2016 &gt; Wahlpflichtbereich &gt; 1.-3. FS, Wahlpflicht</li> <li>• TechMathe Master 2013 &gt; Anwendungsfach "Informatik" &gt; weitere Informatik-Module &gt; 1.-4. FS, Wahlpflicht</li> <li>• WiInf Master 2010 &gt; Wahlpflichtbereich &gt; Wahlpflichtbereich II: Informatik, BWL, VWL &gt; Wahlpflichtmodule der Informatik &gt; 1.-3. FS, Wahlpflicht</li> </ul>
Bestandteile	<ul style="list-style-type: none"> <li>• Vorlesung: Secure Software Systems (3 Credits)</li> <li>• Übung: Secure Software Systems (3 Credits)</li> </ul>

Vorlesung: Secure Software Systems (3 Credits)			
Name im Diploma Supplement	Secure Software Systems		
Anbieter	Lehrstuhl für Sichere Software Systeme <a href="https://www.syssec.informatik.uni-due.de/">https://www.syssec.informatik.uni-due.de/</a>		
Lehrperson	Prof. Dr. Lucas Davi		
SWS	2	Sprache	deutsch
Turnus	Wintersemester	maximale Hörschaft	unbeschränkt
empfohlenes Vorwissen			
Grundlegende Kenntnisse in Programmierung und Software Engineering			
Abstract			
In dieser Vorlesung erhalten die Studenten einen Überblick über aktuelle Forschung, Angriffstechniken und Abwehrmethoden im Bereich der Software- und Systemsicherheit. Es werden Sicherheitsprobleme und Schutztechnologien auf Applikations- und Betriebssysteme für unterschiedliche Rechnerarchitekturen (Desktop PCs, mobile und eingebettete Systeme) analysiert. Ein besonderer Fokus dieser Vorlesung ist die Verwundbarkeit von Softwaresystemen gegenüber Laufzeitangriffen (Exploits). Ziel der Vorlesung ist sowohl das Verständnis von modernen, praktischen Angriffstechniken gegen Softwaresysteme als auch die Entwicklung und Anwendung von Sicherheitstechnologien für Softwaresysteme.			
Lehrinhalte			
<ol style="list-style-type: none"> <li>1. Konventionelle und fortgeschrittene Software Exploittechniken (Buffer Overflow, Return-Oriented Programming)</li> <li>2. Entwicklung von Sicherheitstechnologien zur Detektion und Prävention von Software Exploits (Programmfluss-Integrität, Speicherrandomisierung)</li> <li>3. Software Fault Isolation und Application Sandboxing</li> <li>4. Betriebssystemsicherheit und Zugriffsmodelle mit praktischen Beispielen anhand von Sicherheitsarchitekturen in Multics, Android und Windows</li> <li>5. Trusted Computing Konzepte</li> <li>6. Hardware-basierte Konzepte zur Unterstützung von Softwaresicherheit</li> </ol>			
Literaturangaben			
<ul style="list-style-type: none"> <li>• T. Jaeger: Operating System Security, Morgan &amp; Claypool, 2008</li> <li>• C. Anley, J. Heasman, F. Lindner, G. Richarte: The Shellcoder's Handbook: Discovering and Exploiting Security Holes, Wiley, 2007</li> <li>• L. Davi: Building Secure Defenses Against Code-Reuse Attacks, Springer, 2015</li> <li>• R. Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley, 2008</li> <li>• Aktuelle wissenschaftliche Publikationen von einschlägigen Sicherheitstagungen (werden in der Vorlesung bekannt gegeben)</li> </ul>			

## Übung: Secure Software Systems (3 Credits)

Name im Diploma Supplement	Secure Software Systems		
Anbieter	Lehrstuhl für Sichere Software Systeme <a href="https://www.syssec.informatik.uni-due.de/">https://www.syssec.informatik.uni-due.de/</a>		
Lehrperson	Prof. Dr. Lucas Davi		
SWS	2	Sprache	deutsch
Turnus	Wintersemester	maximale Hörschaft	unbeschränkt
empfohlenes Vorwissen siehe Vorlesung			
<b>Abstract</b> Es werden sowohl praktische als auch theoretische Übungen durchgeführt. In den praktischen Übungen werden die Teilnehmer am Beispiel von verwundbaren Softwaresystemen die Anwendung von Exploittechniken kennenlernen. Zum Beispiel werden die Teilnehmer Proof-of-Concept Exploits auf mobilen Android Systemen selbstständig entwickeln und die Anwendung und Konfiguration von Sicherheitstechnologien zur Detektion dieser Angriffe kennenlernen. Die theoretischen Übungen beinhalten vertiefende Aufgaben zum Stoff der Vorlesung und Analysen von aktuellen wissenschaftlichen Publikationen im Bereich der Softwaresicherheit.			
<b>Lehrinhalte</b> siehe Vorlesung			
<b>Literaturangaben</b> siehe Vorlesung			