

Modulnummer	Modulname	Verantwortliche Dozentin bzw. verantwortlicher Dozent
INF-DSE-20-M-SEC	Foundations of Security and Cryptography	Prof. Dr. Florian Tschorsch florian.tschorsch@tu-dresden.de
Qualifikationsziele	Nach erfolgreichem Abschluss dieses Moduls verfügen die Teilnehmenden über grundlegende Fähigkeiten, eine Anforderungsanalyse aus Sicherheitssicht durchzuführen, d. h. sie können umzusetzende Schutzziele identifizieren und eine Angreifermodellierung vornehmen. Sie sind in der Lage, bezüglich der Schutzziele Vertraulichkeit und Integrität ein grundlegendes Sicherheitskonzept zu bewerten und selbst zu erstellen. Sie verstehen die grundlegenden Wirkmechanismen von symmetrischen und asymmetrischen kryptographischen Algorithmen.	
Inhalte	Inhalt des Moduls sind Grundlagen der Datensicherheit: potentielle Sicherheitsrisiken und Angriffsszenarien, eine Übersicht zu dienstbasierter Sicherheit einschließlich Schutzzielen sowie die Themen Kryptografie und Zugriffskontrolle.	
Lehr- und Lernformen	Das Modul umfasst Vorlesungen im Umfang von 2 SWS und Übungen im Umfang von 2 SWS sowie Selbststudium.	
Voraussetzungen für die Teilnahme	Es werden grundlegende Kenntnisse und Fähigkeiten zu Datenschutz und Datensicherheit auf Bachelorniveau vorausgesetzt.	
Verwendbarkeit	Das Modul ist ein Pflichtmodul im Masterstudiengang Distributed Systems Engineering. Es schafft die Voraussetzungen für die Module Internship sowie Across the Disciplines of Distributed Systems Engineering.	
Voraussetzungen für die Vergabe von Leistungspunkten	Die Leistungspunkte werden erworben, wenn die Modulprüfung bestanden ist. Die Modulprüfung besteht aus einer Klausurarbeit von 90 Minuten Dauer.	
Leistungspunkte und Noten	Durch das Modul können 5 Leistungspunkte erworben werden. Die Modulnote entspricht der Note der Prüfungsleistung.	
Häufigkeit des Moduls	Das Modul wird jedes Sommersemester angeboten.	
Arbeitsaufwand	Der Arbeitsaufwand beträgt 150 Stunden.	
Dauer des Moduls	Das Modul erstreckt sich über ein Semester.	