

Modulnummer	Modulname	Verantwortliche Dozentin bzw. verantwortlicher Dozent
INF-DSE-20-E-ASC	Advanced Security and Cryptography	Professur für Privacy and Security dud-lehre@tu-dresden.de
Qualifikationsziele	Nach erfolgreichem Abschluss dieses Moduls sind die Teilnehmenden in der Lage, selbständig die Sicherheit und Robustheit von verteilten Systemen einzuschätzen. Sie kennen die grundlegenden Methoden zur Sicherheitsanalyse und Absicherung von verteilten Systemen. Darüber hinaus können sie verteilte Systeme zur Umsetzung von Schutzzielen entwerfen und anwenden. Außerdem sind sie befähigt, sich neues Wissen zu den Themen Netzsicherheit und Sicherheit von sowie durch verteilte(n) Systeme(n) aus wissenschaftlicher Literatur zu erschließen und diese Systeme auf Schwachstellen analysieren bzw. bezüglich ihrer Sicherheitseigenschaften zu bewerten.	
Inhalte	Dieses Modul beinhaltet die Grundlagen sicherer Netzwerke und verteilter Systeme sowie einen Überblick über aktuelle Bedrohungen und Schutzmaßnahmen. Dies umfasst neben der Sicherheit von verteilten Systemen selbst auch den Einsatz verteilter Systeme zur Umsetzung von Schutzzielen. Gegenstand des Moduls sind Methodiken der Sicherheitsanalysen, Betrachtung von Angriffen auf ein Netz sowie darin befindliche, verteilte Anwendungen, sowie aktuelle Gegenmaßnahmen. Die Angriffsszenarien umfassen dabei Angriffe auf die Inhalte sowie die anfallenden Meta-Daten, als auch Angriffe auf die Dienste selbst (Denial of Service). Die Gegenmaßnahmen umfassen sowohl proaktive als auch reaktive Mechanismen. Weiterhin beinhaltet das Modul Mechanismen zur unbeobachtbaren Kommunikation und Grundprinzipien von Anonymität und Pseudonymität.	
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 zu Fragestellungen der Datensicherheit, wie sie entsprechend des Moduls Foundations of Security and Cryptography vermittelt werden, vorausgesetzt.	
Verwendbarkeit	Das Modul ist ein Wahlpflichtmodul der fachlichen Vertiefung im Masterstudiengang Distributed Systems Engineering.	
Voraussetzungen für die Vergabe von Leistungspunkten	Die Leistungspunkte werden erworben, wenn die Modulprüfung bestanden ist. Die Modulprüfung besteht aus einer mündlichen Prüfungsleistung von 30 Minuten Dauer.	
Leistungspunkte und Noten	Durch das Modul können 6 Leistungspunkte erworben werden. Die Modulnote entspricht der Note der Prüfungsleistung.	
Häufigkeit des Moduls	Das Modul wird jedes Sommersemester angeboten.	
Arbeitsaufwand	Der Arbeitsaufwand beträgt 180 Stunden.	
Dauer des Moduls	Das Modul erstreckt sich über ein Semester.	