

Modulbezeichnung (eng.)	Angriffsszenarien und Gegenmaßnahmen (Defend Against Security Attacks)	
Semester	WPM	
ECTS-Punkte (Dauer)	5 (1 Semester)	
Art	Wahlpflichtmodul Zertifikat IT-Sicherheit	
Studentische Arbeitsbelastung	60 h Kontaktzeit + 90 h Selbststudium	
Voraussetzungen (laut BPO)		
Empf. Voraussetzungen	Kryptologie, Rechnernetze, C/C++	
Verwendbarkeit	BaI, BaE, BaEP, BaMT, BaIP	
Prüfungsform und -dauer	Klausur 1,5h oder mündliche Prüfung oder Kursarbeit	
Lehr- und Lernmethoden	Vorlesung, Praktikum, Studentische Arbeit	
Modulverantwortlicher	P. Felke	
Qualifikationsziele		
Die Studierenden kennen Schwachstellen und Angriffsmethoden auf IT-Infrastrukturen und mobile Kommunikationsnetzwerke. Durch die Analyse und Bewertung der Schwachstellen können Angriffe und Gegenmaßnahmen identifiziert werden, die dann unter Anwendung ausgewählter Werkzeuge und unter Berücksichtigung rechtlicher Rahmenbedingungen implementiert werden. Die Grenze zwischen technischer Machbarkeit und sozialer Verantwortung ist den Studierenden bewusst.		
Lehrinhalte		
Es werden Schwachstellen von mobilen und Computernetzwerken vorgestellt, sowie Gegenmaßnahmen behandelt. Den Studierenden werden Angriffe und Sicherheitslösungen vorgestellt, die im Praktikum analysiert, bewertet und implementiert werden.		
Literatur		
Schwenk, J.: Sicherheit und Kryptographie im Internet, Springer 2014 Eckert, C.: IT-Sicherheit, Oldenbourg-Verlag, 2008 Forsberg, D.: LTE-Security, Wiley John+Sons, 2012		
Lehrveranstaltungen		
Dozent	Titel der Lehrveranstaltung	SWS
P. Felke	Angriffsszenarien und Gegenmaßnahmen	2
P. Felke	Praktikum Angriffsszenarien und Gegenmaßnahmen	2