

Modul: Security Engineering

Lern- und Qualifikationsziele:

Inhalt: Aufgaben des Security Engineerings, Protokolle, Kryptographie, sichere Dokumente, Digitale Unterschriften und digitale Zertifikate (PKI), Authentifizierung, Realisierung von Zugangsbeschränkungen (Access Control), Überwachungs-Systeme; Biometrie, Netzwerkattacken und Schutzmassnahmen dagegen. Im Praktikum werden kryptographische Algorithmen implementiert und analysiert, sowie Attacken gegen Experimentalsysteme ausprobiert.

Qualifikationsziele: Verständnis, welche Fragen bei der Sicherheit komplexer Systeme bedacht werden müssen. Kenntnis bekannter Attacken sowie der derzeit besten Methoden sich dagegen zu wehren.

ggf. Voraussetzungen für die Teilnahme am Modul:

Abschluss des Grundstudiums in Informatik

Lehrveranstaltungen	SWS	SP und Beschreibung der Arbeitsleistung, auf deren Grundlage die SP vergeben werden
VL + PR	4 + 2	8 SP: Vorlesung (4 SWS) mit begleitendem Praktikum (2 SWS), Selbststudium, bewertete Hausaufgaben / Praktikumsaufgaben. Kurze, unangekündigte Klausur(en) im Semester. Eine Mindestpunktzahl beim Praktikum und den Klausuren ist Voraussetzung für die Teilnahme an der Prüfung.
Voraussetzung für die Vergabe von Studienpunkten		Für Leistungen in den Klausuren sowie für die korrekte Bearbeitung der Hausaufgaben / Praktikumsaufgaben werden Punkte vergeben. Eine Mindestpunktzahl ist die Voraussetzung für die Zulassung zur Prüfung am Ende des Semesters. Bei bestandener Prüfung werden Studienpunkte vergeben.
Prüfung (Prüfungsform, Umfang/Dauer, SP)		Mündliche oder schriftliche Prüfung (wird jeweils am Semesterbeginn festgelegt)
Häufigkeit des Angebots		Mindestens jedes zweite Wintersemester
Dauer des Moduls		1 Semester