E490 ITS IT-Sicherheit

Studiengang:	Bachelor: ET/IT/MT
Kategorie:	technisches Wahlpflichtfach
Semester:	4.-6. Semester
Häufigkeit:	Jedes Semester
Voraussetzungen:	keine
Vorkenntnisse:	Rechnernetze
Modulverantwortlich:	Prof. Dr. Norbert Schultes
Lehrende(r):	Prof. Dr. Norbert Schultes
Sprache:	Deutsch
ECTS-Punkte/SWS:	5 / 4 SWS
Leistungsnachweis:	Prüfungsleistung: Klausur (60 min, 2,5CP) Studienleistung: Hausarbeit oder Praktikum (2,5CP), wird in der Vorlesung bekannt gegeben
Lehrformen:	Vorlesung (3 SWS) mit Übungen (1 SWS)
Arbeitsaufwand:	50 Stunden Präsenzzeit, 50 Stunden für Vor- und Nachbereitung des Lehrstoffes, 50 Stunden fur die Hausarbeit incl. Präsentation
Medienformen:	Tafel, Rechner mit Beamer, Experimente, Simulationen

Anerkennbare praxisbezogene Leistungen/Kompetenzen in Dualen Studiengängen: keine

Das Modul besteht aus zwei Teilen, die in aufeinander folgenden Semestern angeboten und gehört werden können. Die Reihenfolge der beiden Teile ist beliebig.
Die Abschlussklausur über beide Teile wird jedes Semester angeboten.

Lernziele, Kompetenzen, Schlüsselqualifikationen:

- In der seminaristischen Vorlesung werden moderne Sicherheitsrisiken und Sicherungsverfahren exemplarisch besprochen. Wegen der hohen Dynamik der Sicherheitsanforderungen spielen Lernstrategien, Analyse- und Abstraktionsfähigkeit eine wichtige Rolle um aktuelle Risiken zu erfassen (Methoden-Kompetenz). Die Übungen stärken die Fähigkeit der Studierenden durch Kommunikation und Kooperation zu Lösungen zu gelangen (soziale Kompetenz). In der Hausarbeit sollen die Studierenden eigenstandig, mit Unterstützung ein Teilgebiet des Problemraumes bearbeiten. Die Präsentation der Hausarbeiten für die anderen Studierenden im Kurs stärkt die Kommunikations-Kompetenz.

Inhalte:

- Sicherheitsprobleme: Data at Rest, Data in Motion, Data in use
- Charakterisierung Malware: Angriffstypen / Systemschwächen / Gefährdungen
- Side channel Angriffe, down-grading und Mitigation-Strategien
- typische Implementierungsfehler von Krypto-Methoden in embedded devices
- Symmetrische und asymmetrische Kryptographie (AES, RSA, DH), Stromchiffrierung
- Daten-Integrität und -Authentifikation (SHA-2, SHA-3, HMAC)
- Zufallszahlen (RNG, TRNG, PRNG, PUF)
- Einführung elliptische Kurven
- Layer 2 Kryptoprotokolle (PPP, PPTP, VPN)
- Layer 3 Kryptoprotokolle (IPSEC, IKE)
- Layer 4 Kryptoprotokolle (TLS, SSH, DNSSec)
- Lightweight Protokolle für IoT-Devices, pseudonymisierte Abfrage
- Authentifizierungs- und Privacy-Probleme im Internet of Things
- Implementierungs-Restriktionen von Kryptographie in IoT-Devices
- Implementierungen mit und ohne Betriebssystem
- Bewertung von Kryptobibliotheken und Krypto-Code-Audits
- Patch-Management / Key-Management von embedded devices
- WLAN-Sicherheit (WPA2)
- Mitigation Antivirus, Firewalls, IDS-Systeme, Forensik

Literatur:

- Schäfer, Netzsicherheit, dPunkt Verlag 2014
- Paar, Understanding Cryptography, Springer 2010
- Eckert, IT-Sicherheit: Konzepte – Verfahren – Protokolle, De Gruyter Oldenbourg 2014
- B.Schneier, Angewandte Kryptographie, Addison Wesley , Bonn, 1996
- Busch, Netzwerksicherheit, Spektrum Akad.Verlag, Heidelberg, 2002
- Schwenk, Sicherheit und Kryptographie im Internet, Vieweg, Braunschweig, 2014
- Schmeh, Kryptographie, d-punkt-Verlag, 2016
- Aktuelle wissenschaftliche Veröffentlichungen