Technology
Arts Sciences
TH Köln

Lehrveranstaltung
EBS - Embedded Security

Version: 3 | Letzte Änderung: 17.10.2019 10:46 | Entwurf: 0 | Status: vom verantwortlichen Dozent freigegeben

Allgemeine Informationen

Langname	Embedded Security
Anerkennende LModule	EBS_MaCSN
Verantwortlich	Prof. Dr. Kerstin Lemke-Rust Professor Hochschule Bonn-Rhein-Sieg
Niveau	Master
Semester im Jahr	Sommersemester
Dauer	Semester
Stunden im Selbststudium	96
ECTS	5
Dozenten	Prof. Dr. Kerstin Lemke-Rust Professor Hochschule Bonn-Rhein-Sieg
Voraussetzungen	- Grundlagen der IT-Sicherheit. - Kenntnisse der angewandten Kryptographie und bekannter kryptographischer Algorithmen (insbesondere DES, AES, RSA, DSA).
Unterrichtssprache	deutsch
separate Abschlussprüfung	Ja

Abschlussprüfung

Details

mündliche Prüfung

Mindeststandard

Regelmässige Anwesenheit bei Praktikum und Bearbeiten von Übungsaufgaben

Prüfungstyp

mündliche Prüfung

Vorlesung / Übungen

Lernziele

Kenntnisse

Diese Lehrveranstaltung behandelt die Grundlagen und fortgeschrittene Themen der Embedded Security, d.h. der in der Implementierung "eingebauten" Sicherheit.
Inhalte:
- Einführung Implementierungssicherheit, Sicherheitsziele Tamper Resistance, Tamper Response, Tamper Evidence und beispielhafte Realisierungen.
- Hardware-Architekturen (Mikrokontroller, FPGAs, ASICs, System-on-Chip) und bekannte Angriffsmöglichkeiten.
- Mikroarchitektur-Seitenkanalangriffe
- Implementierungssicherheit kryptographischer Verfahren (Fehleranalysen: Methoden und Gegenmaßnahmen. Seitenkanalanalysen: Timing Analysis, Simple/Differential Power Analysis, Templates, Kollisionsangriffe und Gegenmaßnahmen.)
- Standards zur IT-Sicherheitszertifizierung von Produkten: FIPS 140, Common Criteria.
- Schwachstellenanalyse von IT-Produkten. Analyse von FIPS 140 Security Policies und Common Criteria Protection Profiles.

Fertigkeiten

Die Studierenden sind befähgt, in aktuellen Forschungsthemen zur Embedded Security mitzuarbeiten.
Die Studierenden sind befähigt, fortgeschrittene Sicherheitsmaßnahmen in sicherheitssensitive Produkte zu implementieren sowie Schwachstellenanalysen durchzuführen und implementierte Sicherheitsmaßnahmen bezüglich ihrer Effektivität zu bewerten.

Aufwand Präsenzlehre

Typ	Präsenzzeit (h/Wo.)
Vorlesung	2
Übungen (ganzer Kurs)	1
Übungen (geteilter Kurs)	0
Tutorium (freiwillig)	0

Separate Prüfung

keine

Praktikum

Lernziele

Fertigkeiten

Die Studierenden sind befähigt, fortgeschrittene Sicherheitsmaßnahmen in sicherheitssensitive Produkte zu implementieren sowie Schwachstellenanalysen durchzuführen und implementierte Sicherheitsmaßnahmen bezüglich ihrer Effektivität zu bewerten.

Aufwand Präsenzlehre

Typ	Präsenzzeit (h/Wo.)
Praktikum	0
Tutorium (freiwillig)	0

Separate Prüfung

keine