Technology
Arts Sciences
TH Köln

Modul
EBS - Embedded Security

Master Communication Systems and Networks 2020

Version: 1 | Letzte Änderung: 17.10.2019 11:14 | Entwurf: 0 | Status: vom Modulverantwortlichen freigegeben | Verantwortlich: Lemke-Rust

Allgemeine Informationen

Anerkannte Lehrveranstaltungen	EBS Lemke-Rust
Modul ist Bestandteil des Studienschwerpunkts	N_S - Networks & Security
Dauer	1 Semester
ECTS	5
Zeugnistext (de)	Embedded Security
Zeugnistext (en)	Embedded Security
Unterrichtssprache	deutsch oder englisch
abschließende Modulprüfung	Ja

Modulprüfung

Benotet	Ja
Frequenz	Einmal im Jahr

Prüfungskonzept

mündliche Prüfung zu den in Vorlesung, Übung und Praktikum vermittelten Inhalten

Allgemeine Informationen

Inhaltliche Voraussetzungen

IS -IT Security	Grundlagen der IT-Sicherheit. \nKenntnisse der angewandten Kryptographie und bekannter kryptographischer Algorithmen (insbesondere DES, AES, RSA, DSA).

Kompetenzen

Kompetenz	Ausprägung
kommunikationstechnische Systeme und Prozesse analysieren	Vermittelte Kompetenzen
kommunikationstechnische Systeme und Prozesse prüfen	Vermittelte Kompetenzen
kommunikationstechnische Systeme und Prozesse beurteilen	Vermittelte Kompetenzen
Komplexe Fragestellungen sinnvoll auftrennen	Vermittelte Kompetenzen
Informationen und wissenschaftliche Literatur beschaffen, analysieren, verstehen und auswerten	Vermittelte Kompetenzen
Naturwissenschaftliche Phänomene in Realweltproblemen erkennen und deren Auswirkung beurteilen	Vermittelte Voraussetzungen für Kompetenzen
Erkennen und Verstehen technischer Zusammenhänge	Vermittelte Kompetenzen
Wissenschaftliche Methoden anwenden	Vermittelte Kompetenzen
Wissenschaftliche Aussagen treffen	Vermittelte Kompetenzen

Vorlesung

Exemplarische inhaltliche Operationalisierung

Vermittlung der Inhalte zum Fach Embedded Security
Dies sind die Grundlagen und fortgeschrittene Themen der Embedded Security, d.h. der in der Implementierung “eingebauten” Sicherheit wie z.B.:
1.Einführung Implementierungssicherheit, Sicherheitsziele Tamper Resistance, Tamper Response, Tamper Evidence und beispielhafte Realisierungen.
2. Hardware-Architekturen (Mikrokontroller, FPGAs, ASICs, System-on-Chip) und bekannte Angriffsmöglichkeiten.
3. Zufallszahlengeneratoren: physikalische Zufallszahlengeneratoren, Pseudo-Zufallszahlengeneratoren. Funktionalitätsklassen und Evalulierungsmethologie nach BSI AIS20 und AIS.
4. Implementierungssicherheit kryptographischer Verfahren
- Fehleranalysen: Methoden und Gegenmaßnahmen.

- Seitenkanalanalysen: Timing Analysis, Simple/Differential Power Analysis, Templates, Kollisionsangriffe und Gegenmaßnahmen.
5. Standards zur IT-Sicherheitszertifizierung von Produkten: FIPS 140, Common Criteria.
6. Schwachstellenanalyse von IT-Produkten. Analyse von FIPS 140 Security Policies und Common Criteria Protection Profiles.

Separate Prüfung

keine

Übungen

Exemplarische inhaltliche Operationalisierung

Aufgaben zu den behandelten Themen aus der Vorlesung

Separate Prüfung

keine

Praktikum

Exemplarische inhaltliche Operationalisierung

Bearbeitung der Praktikumsaufgaben., dazu wird eine regelmäßige Anwesenheit vorausgesetzt.

Separate Prüfung

Benotet	Nein
Frequenz	Einmal im Jahr
Voraussetzung für Teilnahme an Modulprüfung	Ja

Prüfungskonzept

Die Studiernden müssen die im Praktikum gestellten Aufgaben selbstständig lösen und die Ergebnisse vorführen. Dise werden dann diskutiert und bewertet.