Technology
Arts Sciences
TH Köln

Modulhandbuch 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
Gültig ab	Sommersemester 2021
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
Konzept	mündliche Prüfung zu den in Vorlesung, Übung und Praktikum vermittelten Inhalten
Frequenz	Einmal im Jahr

− Allgemeine Informationen

Inhaltliche Voraussetzungen

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

Handlungsfelder

Algorithmen, Protokolle, Schaltungen und kommunikationstechnische Systeme unter interdisziplinären Bedingungen entwickeln und testen

Wissenschaftlich arbeiten und wissenschaftliche Erkenntnisse anwenden und erweitern

Learning Outcomes

ID	Learning Outcome
LO1	Die Studierenden verstehen die Anforderungen an die Implementierungssicherheit von IT-Sicherheitsprodukten, insbesondere kryptographischen IT-Sicherheitsprodukten, sowohl in der Theorie als auch in der Praxis. Die Studierenden kennen aktuelle Technologien, aktuelle Angriffstechniken auf Sicherheitsfunktionen und geeignete Gegenmaßnahmen in Hardware und Software. Die Studierenden werden an aktuelle Forschungsthemen zur Embedded Security herangeführt. Die Studierenden kennen die Grundlagen und die Anwendung der Common Criteria und FIPS 140 für die IT-Sicherheitszertifizierung von Produkten. Die Studierenden sind befähigt, fortgeschrittene Sicherheitsmaßnahmen in sicherheitssensitive Produkte zu implementieren sowie Schwachstellenanalysen durchzuführen und implementierte Sicherheitsmaßnahmen bezüglich ihrer Effektivität zu bewerten.\nDie Studierenden sind für berufliche Tätigkeiten in hochsicherheitssensitiven Technologiebereichen der Informationstechnik besonders qualifiziert.

Kompetenzen

Kompetenz	Ausprägung
kommunikationstechnische Systeme und Prozesse analysieren	diese Kompetenz wird vermittelt
kommunikationstechnische Systeme und Prozesse prüfen	diese Kompetenz wird vermittelt

kommunikationstechnische Systeme und Prozesse beurteilen	diese Kompetenz wird vermittelt
Komplexe Fragestellungen sinnvoll auftrennen	diese Kompetenz wird vermittelt
Informationen und wissenschaftliche Literatur beschaffen, analysieren, verstehen und auswerten	diese Kompetenz wird vermittelt
Naturwissenschaftliche Phänomene in Realweltproblemen erkennen und deren Auswirkung beurteilen	Voraussetzungen für diese Kompetenz (Wissen,...) werden vermittelt
Erkennen und Verstehen technischer Zusammenhänge	diese Kompetenz wird vermittelt
Wissenschaftliche Methoden anwenden	diese Kompetenz wird vermittelt
Wissenschaftliche Aussagen treffen	diese Kompetenz wird vermittelt

Vorlesung

Typ	Vorlesung
Separate Prüfung	Nein
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.

Übungen

Typ	Übungen
Separate Prüfung	Nein
Exemplarische inhaltliche Operationalisierung	Aufgaben zu den behandelten Themen aus der Vorlesung

Praktikum

Typ	Praktikum
Separate Prüfung	Ja
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

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