22 Hardware-Sicherheit

Hardware Security

Semester	4
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. Oliver Stecklina
Lerngebiet	Informatik
Teilnahmevoraussetzungen	Angewandte Kryptographie
Lernergebnisse	Nach Abschluss des Moduls sind die Studierenden in der Lage • die Effiktivität und Effizienz von hardware-basierten IT-Sicherheitslösungen abzuschätzen. • Anforderungen zur sicheren Bescheinigung von Fähigkeiten von System-Modulen formulieren. • Anwendungsspezifische Lösungen auf der Grundlage von technischen Methoden und Verfahren der Hardware-basierten Sicherheit gestalten. • Methoden und Verfahren physischer Angriffe benennen. • Umsetzung Hardware-basierter Krypto-Funktionen und Zufallszahlengeneratoren beschreiben. • Lösungen für eine manipulationssichere Hardware benennen. • Krypto-Funktionen hinsichtlich ihrer technischen Eignung in Klein- und Kleinstsystemen untersuchen und unterscheiden. • Bedeutung und Gefahren von Klein- und Kleinstsystemen für die moderne Gesellschaft einordnen und erläutern.
Prüfungsvorleistung	Einsendeaufgabe, Präsenzteilnahme, Online-Teilnahme
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Web-Konferenz, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium: ca. 120 h

	Webkonferenzteilnahme: ca. 26 h Präsenzteilnahme: ca. 3 h Die beide Präsenztermine sind wie folgt aufgeteilt: 1 x 90 Minuten, 1 x 180 Minuten
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Chat, Einsendeaufgaben u. a.) sowie Präsenzphasen.
Prüfungsform	Hausarbeit
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte

In diesem Modul werden Kenntnisse zur technischen Umsetzung von Mechanismen und Algorithmen der IT-Sicherheit vermittelt. Der Schwerpunkt des Moduls liegt auf den Hardware-basierten Problemstellungen und Lösungen in Klein- und Kleinstsystemen. Die Studierenden können im Anschluss Fragenstellungen zur Hardware-basierten Umsetzung von Sicherheitsfunktionen hinsichtlich ihrer Anwendungsspezifischen Eignung prüfen bzw. geeignete Lösungsansätze zusammenstellen und deren Effektivität und Effizienz abschätzen.

Lehreinheiten

1. Einführung in Klein- und Kleinstsysteme
2. Methoden und Verfahren physischer Angriffe

- Hardware-Hacking
- Seitenkanal-Angriffe

3. Vertrauenswürdige System-Module

- Hardware-basierte Krypto-Funktionen
- Sichere Zufallszahlen
- Remote Attestation

4. Manipulationssichere Hardware

- Hardware-Verschlüsselung
- Physical Unclonable Functions
- Tamper-Resistenz