TECHNISCHE HOCHSCHULE LÜBECK

Module: Hardware-based IT-Security

Level	Master	**Short Name**	HWS
Responsible Lecturers	Oliver Stecklina, Prof. Dr.		
Department, Facility	Electrical Engineering and Computer Science		
Course of Studies	Applied Information Technology, Master		
Compulsory/elective	Elective	**ECTS Credit Points**	5
Semester of Studies	2	**Semester Hours per Week**	4
Length (semesters)	1	**Workload (hours)**	150
Frequency	WiSe	**Presence Hours**	60
Teaching Language	German/English	**Self-Study Hours**	90

The following section is filled only if there is **exactly one** module-concluding exam.

Exam Type	Project Work	**Exam Language**	German/English
Exam Length (minutes)		**Exam Grading System**	One-third Grades
Learning Outcomes	After successfully completing the event, students will be able to: • estimate and assess the effectiveness and efficiency of hardware-based IT security solutions, • formulate requirements for the provision of security-enhancing capabilities of system modules, • design application-specific solutions for hardware-based security, • implement secure hardware-based crypto functions and random number generators, and develop solutions for tamper-proof hardware.		
Participation Prerequisites			

The previous section is filled only if there is **exactly one** module-concluding exam.

Consideration of Gender and Diversity Issues	✔ Use of gender-neutral language (THL standard) ✘ Target group specific adjustment of didactic methods ✔ Making subject diversity visible (female researchers, cultures etc.)
Applicability	
Remarks	

TECHNISCHE HOCHSCHULE LÜBECK

Module Course: Hardware-based IT Security (Lecture)

(of Module: Hardware-based IT-Security)

Course Type	Lecture	**Form of Learning**	Presence
Mandatory Attendance	no	**ECTS Credit Points**	3
Participation Limit		**Semester Hours per Week**	3
Group Size		**Workload (hours)**	90
Teaching Language	German/English	**Presence Hours**	45
Study Achievements ("Studienleistung", SL)		**Self-Study Hours**	45
SL Length (minutes)		**SL Grading System**	

The following section is filled only if there is a course-specific exam.

Exam Type		**Exam Language**	
Exam Length (minutes)		**Exam Grading System**	
Learning Outcomes			
Participation Prerequisites			

The previous section is filled only if there is a course-specific exam.

Contents

This module imparts knowledge of the technical implementation of mechanisms and algorithms in IT security. The module focuses on hardware-based problems and solutions in small and power-restricted systems. The students can then examine questions regarding the hardware-based implementation of security functions with regard to their application-specific suitability or compile suitable solutions and assess their effectiveness and efficiency.

- Introduction to small and power-restricted systems
- Methods and procedures of physical attacks
  - Hardware Hacking
  - Side channel attacks
- Trustworthy system modules
  - Hardware-based crypto functions
  - Secure random number generation
  - Remote attestation
- Tamper-proof hardware
  - Hardware-based encryption
  - Physical Unclonable Functions
  - Tamper resistance

Literature

[1] Stefan Mangard, Elisabeth Oswald und Thomas Popp; Power Analysis Attacks; Springer 2007

[2] Christof Paar, Jan Palzl; Understanding Cryptography: A Textbook for Students and Practitioners; Springer 2010

	[3] Mohammed Theranipoor, Cliff Wang; Introduction to Hardware Security and Trust; Springer 2012 [4] Christoph Böhm, Maximilian Hofer; Physical Unclonable Functions in Theory and Practice; Springer 2013
Remarks	

Module Course: Hardware-based IT Security (Practical Training)

(of Module: Hardware-based IT-Security)

Course Type		**Form of Learning**	Presence
Mandatory Attendance	no	**ECTS Credit Points**	2
Participation Limit		**Semester Hours per Week**	1
Group Size	12	**Workload (hours)**	60
Teaching Language	English	**Presence Hours**	15
Study Achievements ("Studienleistung", SL)	Practical Training	**Self-Study Hours**	45
SL Length (minutes)		**SL Grading System**	Pass

The following section is filled only if there is a course-specific exam.

Exam Type		**Exam Language**	
Exam Length (minutes)		**Exam Grading System**	
Learning Outcomes			
Participation Prerequisites			

The previous section is filled only if there is a course-specific exam.

Contents	The knowledge of the lecture is to be consolidated in practical examples: • Electromagnetic and / or power analysis of crypto functions in FPGAs and on microcontrollers Setup of tamper-resistant circuits
Literature	Beispiel: Jukic, N. et al.: Database Systems, Prospect Press, 2016
Remarks	