TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Module Handbook

TUK MODHB Homapage

Module INF-42-52-M-5

Network Security (M, 4.0 LP)

Module Identification

Module Number	Module Name	CP (Effort)
INF-42-52-M-5	*Network Security*	4.0 CP (120 h)

Basedata

CP, Effort	4.0 CP = 120 h
Position of the semester	1 Sem. irreg. WiSe
Level	[5] Master (Entry Level)
Language	[DE/EN] German or English as required
Module Manager	Schmitt, Jens, Prof. Dr. (PROF | DEPT: INF)
Lecturers	Schmitt, Jens, Prof. Dr. (PROF | DEPT: INF)
Area of study	[INF-VVS] Distributed and Networked Systems
Reference course of study	[INF-88.79-SG] M.Sc. Computer Science
Livecycle-State	[NORM] Active

Courses

Type/SWS	Course Number	Choice in Module-Part	SL	PL	CP	Sem.
2V+1U	INF-42-52-K-5	P	U-Schein	PL1	4.0	irreg. WiSe

- About **[INF-42-52-K-5]**: Title: "Network Security"; Presence-Time: 42 h; Self-Study: 78 h
- About **[INF-42-52-K-5]**: The study achievement **"[U-Schein] proof of successful participation in the exercise classes (ungraded)"** must be obtained.
  - It is a prerequisite for the examination for PL1.

Examination achievement PL1

- Form of examination: **written or oral examination**
- Examination Frequency: each semester
- Examination number: 64257 ("Network Security")

Type of examination will be announced in the lecture. Duration of the examination: ref. examination regulations.

Evaluation of grades

The grade of the module examination is also the module grade.

Contents

From [INF-42-52-K-5] Network Security:

- History of secure communications
- Symmetric cryptography: DES, 3DES, AES
- Asymmetric cryptography: RSA, Diffie-Hellman, El Gamal
- Cryptographic protocols: Needham-Schroeder, Kerberos, X.509
- Security protocols in the link layer: PPP, EAP, PPTP, L2TP
- Security protocols in the network layer: IPSec
- Security protocols in the transport layer: SSL/TLS, SSH
- Security in mobile systems
- Security in WLAN
- Security in wireless sensor networks

Competencies / intended learning achievements

Upon successful completion of the module, students will be able to

- explain the essential features of important cryptographic procedures
- apply cryptographic procedures in wired as well as wireless and mobile systems,
- compare the specifics of the different security protocols
- justify the selection of suitable procedures for securing IT systems
- justify the use of appropriate security measures and protocols at the different network layers

Literature

From [INF-42-52-K-5] Network Security:

- G. Schäfer: Netzsicherheit, dpunkt Verlag, 2003.
- B. Schneier: Applied Cryptography, John Wiley & Sons, 2nd Edition, 1996.
- J. Buchmann: Einführung in die Kryptographie, Springer-Verlag, 1999.

Requirements for attendance of the module (informal)

None

- Notice: Some Courses have informal requirements for attendance:
  - #A: [INF-42-52-K-5] Network Security (2V+1U, 4.0 LP) (P: Obligatory)

Requirements for attendance of the module (formal)

None

References to Module / Module Number [INF-42-52-M-5]

Course of Study	Section	Choice/Obligation
[INF-88.79-SG] M.Sc. Computer Science	[Specialisation] Specialization 1	[WP] Compulsory Elective

Module-Pool	Name
[EIT-AC-MSC-TW-MPOOL-7]	General Elective Modules Master A&C
[INF-SIAK-DT-CS-MPOOL-6]	SIAK Certificate "Digital Transformation" - Modules INF "Computer Science"
[INF-VVS_Ba_V-MPOOL-4]	Specialization Bachelor TA Distributed and Networked Systems