h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES
fbi
FACHBEREICH INFORMATIK

Modulbeschreibung

Security Protocols and Infrastructures

Module numbers:	41.4886 [PVL 41.4887]
Language:	english
Study programme:	Dualer Master 2021 - Katalog AS: Anwendungs- und systemorientierte Module Dualer Master 2021 - Vertiefung IS: IT Sicherheit Master 2021 - Katalog AS: Anwendungs- und systemorientierte Module Master 2021 - Vertiefung IS: IT Sicherheit Dualer Master 2013 - Katalog AS: Anwendungs- und systemorientierte Module Dualer Master 2013 - Vertiefung IS: IT-Sicherheit JIM 2013 - Elective Catalogue J Master 2013 - Katalog AS: Anwendungs- und systemorientierte Module Master 2013 - Vertiefung IS: IT-Sicherheit JIM 2006 - Courses Master 2006 - Katalog AS: Anwendungs- und systemorientierte Module Master 2006 - Vertiefung AE: Application Engineering Master 2006 - Vertiefung IS: IT-Sicherheit Master 2006 - Vertiefung TK: Telekommunikation Master 2006 - Vertiefung TS: Technische Systeme MN Data Science 2022/2016 - Katalog M-I_I: Allgemeine Wahlpflicht Informatik
Type of course:	V+Ü+P = Lecture+Exercise+Practical
Weekly hours:	2+1+1
Credit Points:	6
Exam:	written exam (90 min., with tasks from the master task catalog)
PVL (e.g. Practical):	not graded (Defending own solutions to given practical tasks)
Required knowledge:	IT Security; structured and analytical thinking. Further recommended: basic concepts and ways of thinking in the field of cryptography
Learning objectives:	After this course the students • have a deep understanding of design principles of security protocols and security infrastructures. • have knowledge of the basic security goals in cryptography and its relevance to practical use cases. • understand, in which way well-known security protocols (TLS, PACE, EAC) achieve the security goals. • understand the key topics of the wide-spread security infrastructure standards and apply them to practical tasks. • are able to choose suitable protocols for a given use case. • are able to analyse if a security protocol does have the zero knowledge property. • can evaluate the security properties of security protocols and infrastructures.
Content:	• Security goals (CIA) • Network security protocols (TLS) • Security protocols for electronic ID cards • Abstract Syntax Notation 1 (ASN.1) • Certificates and related standards X.509/RFC5280 • Public Key Cryptography Standard Series • Certificate-based security infrastructures (PKI) • Zero knowledge protocols • Practical and theoretical solutions to exercises • Autonomous acquisition of zero knowledge protocols, which will be treated in the exam
Literature:	• Menezes, P. van Oorschoot, S. Vanstone: Handbook ofApplied Cryptography, CRC Press, 1997 • D. Cooper et.al.: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Request for Comments 5280, May 2008 • T. Dierks et.al.: The Transport Layer Security (TLS) Protocol, Version 1.2, Request for Comments 5246, August 2008 • BSI Technical Report TR-03110, www.bsi.bund.de
Lecture style / Teaching aids:	Lecture + exercise + practical course / further reading
Responsibility:	Alex Wiesmaier
Professional competencies:	• formal, algorithmic, mathematical competencies: medium • analytical, design and implementation competencies: medium • technological competencies: medium • capability for scientific work: low
Interdisciplinary competencies:	• project related competencies: low • interdisciplinary expertise: basic technical and natural scientific competence