Technology
Arts Sciences
TH Köln

Course Manual IS

IT Security

Version: 3 | Last Change: 05.04.2022 17:30 | Draft: 0 | Status: vom verantwortlichen Dozent freigegeben

General information

Long name	IT Security
Approving CModule	IS_MaCSN, IS_MaTIN
Responsible	Prof. Dr. Heiko Knospe Professor Fakultät IME
Valid from	winter semester 2020/21
Level	Master
Semester in the year	winter semester
Duration	Semester
Hours in self-study	78
ECTS	5
Professors	Prof. Dr. Heiko Knospe Professor Fakultät IME
Requirements	Rquirements, objectives and application of cryptographic mechanisms: symmetric encryption, hashes, message authentication codes, random number generation, asymmetric encryption, signatures, key establishment
Language	English
Separate final exam	Yes

Literature

M. Bishop, Computer Security: Art and Science. Addision-Wesley.

C. Eckert, IT-Sicherheit. Konzepte-Verfahren-Protokolle. Oldenbourg Verlag

D. Gollmann, Computer Security. Wiley & Sons

N. Pohlmann, Cyber-Sicherheit. Springer Vieweg

J. Pieprzyk, T. Hardjono, J. Seberry, Fundamentals of Computer Security. Springer

O. Santos, Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide, Cisco Press.

G. Schäfer, M. Roßberg, Netzsicherheit. dpunkt

J. Schwenk, Sicherheit und Kryptographie im Internet. Springer Vieweg

W. Stallings, L. Brown, Computer Security. Principles and Practice. Prentice Hall.

P. C. van Oorschot, Computer Security and the Internet, Springer.

Final exam

Details	Written exam
Minimum standard	Passing the exam

Exam Type	EN Klausur

− Lecture / Exercises

Learning goals

Goal type	Description
Knowledge	Introduction to IT Security - Standards and Guidelines - Taxonomy - Security Objectives, Vulnerabilities, Threats, Risk, Attacks, Security Controls
Knowledge	Authentication and Key Establishment - Authentication Protocols - Key Exchange - Kerberos - Public Key Infrastructures - Passwords and their Vulnerabilities - Security Token
Knowledge	Access Control - Authentication, Authorization, Auditing - Discretionary and Mandatory Access Control - Access Matrix, Unix ACL - Role-Based Access Control - Multi-Level Security, Bell-LaPadula Model
Knowledge	Network Security - Threat Model - LAN and WLAN Security - IP Security, IPsec - TCP Security, TLS, SSH - Virtual Private Networks - IDS and IPS - Firewalls and UTM - DNS Security
Knowledge	Software Security - Safety and Security - Software Vulnerabilities - Web Security
Knowledge	Security Management - Information Security Management System - Security Standards ISO 27001, ISO 27002, BSI Grundschutz - Privacy Regulations

Special requirements

none

Accompanying material	Lecture Slides, Online course "Cisco CyberOps"
Separate exam	No

Expenditure classroom teaching

Type	Attendance (h/Wk.)
Lecture	2
Exercises (whole course)	1
Exercises (shared course)	0
Tutorial (voluntary)	0

− Practical training

Learning goals

Goal type	Description
Skills	- Generation of key pairs, certificates and setting up a public-key infrastructure (PKI). - Implementation of a secure socket connection and analysis of a TLS handshake. - Implementation and analysis of a VPN. - Penetration testing of web applications using open source tools. - Perform SQL injection, XSS and CSRF attacks against test systems. - Reconnaissance, exploitation and infiltration in a lab environment. - Interpret DNS and HTTP data to analyze an attack.

Expenditure classroom teaching

Type	Attendance (h/Wk.)
Practical training	1
Tutorial (voluntary)	0

Special requirements

none

Accompanying material	Online course "Cybersecurity Essentials", Online course "CCNA Cybersecurity Operations"
Separate exam	Yes

Separate exam

Exam Type	EN praxisnahes Szenario bearbeiten (z.B. im Praktikum)
Details	-
Minimum standard	-