Technology
Arts Sciences
TH Köln

Lehrveranstaltungshandbuch IS

IT-Sicherheit

Version: 3 | Letzte Änderung: 05.04.2022 17:30 | Entwurf: 0 | Status: vom verantwortlichen Dozent freigegeben

Allgemeine Informationen

Langname	IT-Sicherheit
Anerkennende LModule	IS_MaCSN, IS_MaTIN
Verantwortlich	Prof. Dr. Heiko Knospe Professor Fakultät IME
Gültig ab	Wintersemester 2020/21
Niveau	Master
Semester im Jahr	Wintersemester
Dauer	Semester
Stunden im Selbststudium	78
ECTS	5
Dozenten	Prof. Dr. Heiko Knospe Professor Fakultät IME
Voraussetzungen	Voraussetzungen, Sicherheitsziele und Anwendung kryptographischer Verfahren: symmetrische Verschlüsselung, Hashverfahren, Message Authentication Codes, Erzeugung von Pseudozufallszahlen, asymmetrische Verschlüsselung, Signaturen, Schlüsselvereinbarung.

Literatur

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.

Abschlussprüfung

Details	Klausur
Mindeststandard	Bestehen der Klausur

Unterrichtssprache	englisch
separate Abschlussprüfung	Ja

Prüfungstyp	Klausur

− Vorlesung / Übungen

Lernziele

Zieltyp	Beschreibung
Kenntnisse	Introduction to IT Security - Standards and Guidelines - Taxonomy - Security Objectives, Vulnerabilities, Threats, Risk, Attacks, Security Controls
Kenntnisse	Authentication and Key Establishment - Authentication Protocols - Key Exchange - Kerberos - Public Key Infrastructures - Passwords and their Vulnerabilities - Security Token
Kenntnisse	Access Control - Authentication, Authorization, Auditing - Discretionary and Mandatory Access Control - Access Matrix, Unix ACL - Role-Based Access Control - Multi-Level Security, Bell-LaPadula Model
Kenntnisse	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
Kenntnisse	Software Security - Safety and Security - Software Vulnerabilities - Web Security
Kenntnisse	Security Management - Information Security Management System - Security Standards ISO 27001, ISO 27002, BSI Grundschutz - Privacy Regulations

Besondere Voraussetzungen

keine

Begleitmaterial	Lecture Slides, Online course "Cisco CyberOps"
Separate Prüfung	Nein

Aufwand Präsenzlehre

Typ	Präsenzzeit (h/Wo.)
Vorlesung	2
Übungen (ganzer Kurs)	1
Übungen (geteilter Kurs)	0
Tutorium (freiwillig)	0

− Praktikum

Lernziele

Zieltyp	Beschreibung
Fertigkeiten	- 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.

Aufwand Präsenzlehre

Typ	Präsenzzeit (h/Wo.)
Praktikum	1
Tutorium (freiwillig)	0

Besondere Voraussetzungen

keine

Begleitmaterial	-, -
Separate Prüfung	Ja

Separate Prüfung

Prüfungstyp	praxisnahes Szenario bearbeiten (z.B. im Praktikum)
Details	Testat und individuelle Lernstandsrückmeldung
Mindeststandard	Erfolgreiche Bearbeitung der aller Praktikumsaufgaben

© 2022 Technische Hochschule Köln