Technology
Arts Sciences
TH Köln

Modul
IS - IT Security

Master Communication Systems and Networks 2020

Version: 4 | Letzte Änderung: 05.04.2022 17:33 | Entwurf: 0 | Status: vom Modulverantwortlichen freigegeben | Verantwortlich: Knospe

Allgemeine Informationen

Anerkannte Lehrveranstaltungen	IS Knospe
Modul ist Bestandteil des Studienschwerpunkts	N_S - Networks & Security
Dauer	1 Semester
ECTS	5
Zeugnistext (de)	IT-Sicherheit
Zeugnistext (en)	IT Security
Unterrichtssprache	englisch
abschließende Modulprüfung	Ja

Modulprüfung

Benotet	Ja
Frequenz	Jedes Semester

Prüfungskonzept

Schriftliche Prüfung (Klausur)

Allgemeine Informationen

Inhaltliche Voraussetzungen

KRY -Cryptography	Voraussetzungen, Sicherheitsziele und Anwendung kryptographischer Verfahren: Diskrete Strukturen, Wahrscheinlichkeit, Zahlentheorie und Algebra, symmetrische Verschlüsselung, Blockchiffen, Stromchiffren, Hashverfahren, Message Authentication Codes, Erzeugung von Pseudozufallszahlen, asymmetrische Verschlüsselung, Digitale Signaturen, Schlüsselvereinbarung, Hybride Verschlüsselung, Elliptische-Kurven-Kryptographie.

Kompetenzen

Kompetenz	Ausprägung
kommunikationstechnische Systeme und Prozesse entwerfen	diese Kompetenz wird vermittelt
kommunikationstechnische Systeme und Prozesse analysieren	diese Kompetenz wird vermittelt
kommunikationstechnische Systeme und Prozesse realisieren	diese Kompetenz wird vermittelt
Informationen und wissenschaftliche Literatur beschaffen, analysieren, verstehen und auswerten	diese Kompetenz wird vermittelt
Wissenschaftliche Methoden anwenden	diese Kompetenz wird vermittelt
Gesellschaftliche und ethische Grundwerte anwenden	diese Kompetenz wird vermittelt

Vorlesung / Übungen

Exemplarische inhaltliche Operationalisierung

Introduction to IT Security
- Standards and Guidelines
- Taxonomy
- Security Objectives, Vulnerabilities, Threats, Risk, Attacks, Security Controls

Authentication and Key Establishment
- Authentication Protocols
- Key Exchange
- Kerberos
- Public Key Infrastructures
- Passwords and their Vulnerabilities
- Security Token

Access Control

- Authentication, Authorization, Auditing
- Discretionary and Mandatory Access Control
- Access Matrix, Unix ACL
- Role-Based Access Control
- Multi-Level Security, Bell-LaPadula Model

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

Software Security
- Safety and Security
- Software Vulnerabilities
- Web Security

Security Management
- Information Security Management System
- Security Standards ISO 27001, ISO 27002, BSI Grundschutz
- Privacy Regulations

Separate Prüfung

keine

Praktikum

Exemplarische inhaltliche Operationalisierung

- 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.

Separate Prüfung

Benotet	Nein
Frequenz	Einmal im Jahr

Voraussetzung für Teilnahme an Modulprüfung	Ja

Prüfungskonzept

Individuelle Lernstandsrückmeldung und Testat