03-IBAP-ISEC	Informationssicherheit
	Information Security

Lehrform *(teaching format)* / **SWS** *(hours per week)*: 2VL + 2UE

Kreditpunkte *(credit points)*: 6

Turnus *(frequency)*: i.d.R. jedes WiSe

Inhaltliche Voraussetzungen *(content-related prior knowledge/skills)*: Grundlagen Betriebssysteme, Nebenläufigkeit, Rechnernetze

Sprache *(language)*: Deutsch

Lehrende *(teaching staff)*: AG Rechnernetze (Prof. Dr. Carsten Bormann, PD Dr. Karsten Sohr u.a.)

Studiengang *(degree program)*	Module	Semester
Informatik (Bachelor VF)	IBAP (SQ)	ab 5. Sem.
Informatik (Bachelor KF)	KINF-A1/A2	ab 5. Sem.
Digitale Medien (Bachelor)	DMB-MI–9	ab 5. Sem.
Wirtschaftsinformatik (Bachelor)	WI-IM-WP	ab 5. Sem.
Systems Engineering (Bachelor)	V07-ESS-V	ab 5. Sem.
Informatik (Master)	*General Studies*	ab 1. Sem.
Systems Engineering II (Master)	M07-AM-INF	1. Sem.
(Industr.)Mathematics (Master)	Anwendungsfach Informatik	
Zertifikatsstudium DiMePäd	DM in Lernumgebungen	ab 1.Sem.

Lernergebnisse:

- Grundkonzepte der Informationssicherheit kennen;
- Die gängigsten Sicherheitsprobleme in heutigen IT-Infrastrukturen und deren Ursachen kennen;
- Notwendigkeit für den Einsatz von Sicherheitstechnik erkennen;
- Grenzen der im Einsatz befindlichen Technologien einschätzen können;
- Verschiedene Bereiche von Sicherheitstechnik einordnen können;
- Modelle und Methoden zur systematischen Konstruktion sicherer Systeme kennen.

Learning Outcome:

Inhalte:

- Grundbegriffe der IT-Sicherheit, Bedrohungen und Sicherheitsprobleme: Vertraulichkeit, Integrität, Verfügbarkeit etc.; Viren, Würmer, Trojanische Pferde etc.
- Kryptografie (Symmetrisch, Asymmetrisch, Hash, PRF): DES, 3DES, AES; RSA, DSA; MD5, SHA1; TLS-PRF, PBKDF2
- Mechanismen zur Authentisierung und Integritätsprüfung digitaler Signaturen, Zertifikate, PKI
- Zugriffskontrolle, Autorisierung, Rollen
- Sicherheitsprotokolle, z.B. Schlüsselaustausch Diffie-Hellman, TLS (SSL), Kerberos
- Probleme mit Protokollen, Angriffe (fehlende Bindung, Replay, …)

- Netzsicherheit (Firewalls/IDS, VPN, Anwendungssicherheit)
- Sicherheit in Layer 2 (GSM, WLAN, …)
- Software-Zertifizierung: Common Criteria
- Mobiler Code
- Smart Cards, Trusted Computing Platform
- Security Engineering
- Organisationelle Sicherheit; Security: The Business Case

Contents:

Hinweise *(remarks)*:

- In der Tabelle sind nur die primären/spezifischsten Module aufgelistet, denen diese Veranstaltung zugeordnet ist.
- *Informationssicherheit* wird als Vorbereitung auf den Schwerpunkt SQ (*Sicherheit und Qualität*) im Master-SG Informatik empfohlen.