**Informationssicherheit (Kopie vom Fri May 22 16:52:33 +0200 2020) (deleted:Fri May 22 16:53:53 +0200 2020)**

*Information Security*

Modulnummer:

Bachelor

- Pflicht/Wahl ☒
- Wahlpflicht ☐
- Wahl ☐
- Sonderfall ☐

Modulbereich: Pflicht

| Anzahl der SWS | V | UE | K | S | Prak. | Proj. | Σ |
|---|---|---|---|---|---|---|---|
| | 2 | 2 | 0 | 0 | 0 | 0 | 4 |

Kreditpunkte: 6

Turnus

i. d. R. angeboten alle 2 Semester

Formale Voraussetzungen: -

Inhaltliche Voraussetzungen: Technische Informatik 2

Vorgesehenes Semester: ab 1. Semester

Sprache: Deutsch

Ziele:

- 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.

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

Unterlagen (Skripte, Literatur, Programme usw.):

- (deutschsprachig:) Claudia Eckert: IT-Sicherheit: Konzepte - Verfahren - Protokolle; Oldenbourg 2009; 981 Seiten
- (englischsprachig:) Ross Anderson: Security engineering: a guide to building dependable distributed systems; Wiley 2008; 1040 Seiten

Form der Prüfung:
i.d.R. Bearbeitung von Übungsaufgaben und Fachgespräch oder mündliche Prüfung

| | | |
|---|---|---|
| Arbeitsaufwand | Präsenz | 56 h |
| | Übungsbetrieb/Prüfungsvorbereitung | 124 h |
| | Summe | 180 h |
| Lehrende:<br>Prof. Dr. C. Bormann, Dr. K. Sohr | | Verantwortlich:<br>Prof. Dr. C. Bormann |