Industrielle und anwendungsbezogene Sicherheit

Allgemeine Angaben

Kürzel	M_IAS
Modulverantwortliche	Prof. Dr. Koch
Dozenten	Prof. Dr. Koch, Prof. Dr. Stehr, Dr. Loeser, Dr. Speth
Lehrsprache	Deutsch
Semester	3
ECTS-Punkte	5
Kontaktstunden	40
Selbststudium	85
Dauer	1 Semester
Art	Pflicht im Rahmen der Spezialisierung
Häufigkeit	jedes Studienjahr
Gewichtung	5/120
Prüfungsleistung	RS

Stichwörter

- Mobile Sicherheit
- Cloud Security
- Trusted Computing
- Sicherheit im Bereich IoT/Industrie 4.0

Zugangsvoraussetzungen

- Grundlagen im Bereich IT-Sicherheit und Riskmanagement sind vorhanden, Sicherheitsanalytik, Identitäts- und Zugriffsmanagement.

Verwendbarkeit

- Masterthesis und ggf. weiterführende Arbeiten für Forschungsprojekte und möglicherweise eine Promotion/DBA; verwendbar in weiteren Spezialisierungsmodulen Cyber Security.

Qualifikations- und Kompetenzziele

Die Studierenden sind in der Lage sich in unterschiedlichste Themen und Anwendungsfelder der Informationstechnik (IT) einzuarbeiten und die dafür erforderlichen Sicherheitsanalysen und Risikobetrachtungen durchzuführen. Sie verstehen die besonderen Sicherheitsanforderungen im Bereich der Mobile Security, Cloud Security und in industriellen Anwendungsfeldern und können entsprechende Sicherheitslösungen konzipieren und integrieren. Sie kennen die Unterschiede zwischen IT und OT (Operational Technology) und die Notwendigkeiten, die sich daraus für das Thema Cyber Security im industriellen Umfeld ergeben. Sie verstehen die besonderen Merkmale und Voraussetzungen von Trusted Computing und können Trusted Computing in typischen Anwendungen konzeptionell integrieren.

Lehr- und Lernmethoden

Vorlesung, Gruppenarbeiten, Fallstudien, Seminaristischer Vortrag, Übungen.

Inhalte

Die verschiedenen Themen und Anwendungsbereiche werde beleuchtet und unter dem Blickwinkel der Cyber Security betrachtet. Hierbei werden die spezifischen Anforderungen betrachtet und daraus spezielle Konzepte und Lösungen für die Anwendungsszenarien entwickelt.

- Sicherheit im industriellen Umfeld (Cyber Physical Systems / IoT / I4.0)
  - Automatisierung und Vernetzung
  - Neue Geschäftsmodelle

    - M2M-Kommunikation
    - Neue Angriffsszenarien
- Weitere möglichen Themengebiete sind:
    - Sicherheit von Trusted Computing Systemen
    - Sicherheit mobiler Systeme, Netze und Endgeräte
    - Sicherheit im Cloud-Computing
    - Sicherheit im Internet und Web
    - Sicherheit kritischer Infrastrukturen
    - Sicherheit im Bereich der Künstlichen Intelligenz
    - etc,
- Vertiefung ausgewählter Anwendungen, je nach aktueller Relevanz der Anwendung

Grundlegende Literaturhinweise

Schwenk, J.: Sicherheit und Kryptographie im Internet: Theorie und Praxis, Springer Vieweg, 2020
Pinnow, C. und Schäfer, St.: Industrie 4.0 – Safety and Security, Beuth Verlag, 2017
Westhoff, D.: Mobile Security: Schwachstelle verstehen und Angriffsszenarien nachvollziehen, Springer Vieweg, 2020

Weitere Literatur je nach Anwendungsfeld, wie z.B.
Dotson, Chr.: Practical Cloud Security: A Guide for Secure Design and Deployment, O'Reilly UK Ltd.,2019
Hoffmann, A.: Web Application Security: Exploitation and Countermeasures for Modern Web Applications, O'Reilly UK Ltd., 2020