Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Wahlpflichtmodul-Katalog

der Studiengänge
Advanced IT Security M.Sc.
Business and Security Analytics M.Sc.
Systems Engineering M.Eng.
Fakultät Informatik

StuPO 21.2
Wintersemester 2022/23
Ersteller: Prof. Dr. German Nemirovski, Studiendekan
Verantwortlich: Prof. Dr. German Nemirovski, Studiendekan

Inhaltsverzeichnis

1 Modulbeschreibungen

1.1 Wintersemester

1.1.1 Xxxxx - Advanced Programming

Studiengang: INF
StuPO-Version: 21.2

Semester: WS 2022/23
Letzte Bearbeitung: 14.09.22

Modul: Advanced Programming						
	Workload 75 h	**Modulart** Praktische Arbeit	**Studiensemester** 1	**Dauer** 1 Semester	**Häufigkeit** WS und SS	
1	**Lehrveranstaltung(en)** Advanced Programming		**Sprache** Deutsch	**Kontakt-zeit** 2 SWS/ 30 h	**Selbst-studium** 45h	**Credits (ECTS)** 2,5
2	**Lehrform(en) / SWS:** Praktische Arbeit, Umfang 15x2 = 30 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Kenntnis von Komponenten eingebetteter Systeme und Wissen über Zusammenstellung zu einem Gesamtsystem. *[Wissen, 7]* *Kompetenz Fertigkeiten* Erstellung eines Designs mit Auswahl von Komponenten für eingebettete Systeme. *[Instrumentelle Fertigkeiten, 7]* *Sozialkompetenz* Fragen während Lehrveranstaltung und Klausurvorbereitung. Präsentation der Praktikumsergebnisse vor Publikum. *[Kommunikation, 7]* *Selbstständigkeit* Selbständiges Erlernen der Komponenten und Designmethoden. *[Lernkompetenz, 7]*						
4	**Inhalte*:*** Planung eines über das Netzwerk verteilten Systems. Anwendungsprogrammierung mit Authentifizierung. Sichere Netzwerkkommunikation über Middleware. Einsatz einer Datenbank zur Sicherung von Daten. Integration der Systemkomponenten. Image-Container Programmierung. Empfohlene Literaturangaben					

5	**Teilnahmevoraussetzungen:** Der Studierende muss die Programmiersprache Python oder Java beherrschen (Modul Programmieren I u. II).
6	**Prüfungsformen***:* Laborarbeit, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Der Studierende soll in der Lage sein, ein Authentifizierungsfenster mit GUI programmieren. Der Studierende soll aus einer Reihe von zur Verfügung stehenden Middleware's (MQTT, DDS etc.) ein passendes finden und daraus eine verteiltes System programmieren. Der Studierende soll Daten über das Netzwerk sicher zugreifen und verarbeiten. Der Studierende soll alle programmierten Teilkomponenten zu einer kompletten Lösung integrieren. Der Studierende soll Teilkomponenten seiner Lösung mit Hilfe von Container-Techniken verpacken, um die Installation und Wartbarkeit zu vereinfachen.
8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng., Advanced IT Security M.Sc., Business and Security Analytics M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Derk Rembold Dozenten: Prof. Dr. Rembold
10	***Optionale Informationen:*** keine

1.1.2 51100 – Business Intelligence

Studiengang: INF
StuPO-Version: 21.2

Semester: WS 2022/23
Letzte Bearbeitung: 14.09.22

<table>
<tr><td colspan="7">Modul: Business Inteligence</td></tr>
<tr><td colspan="2">Kennnummer
51100</td><td>Workload
180 h</td><td>Modul-art
WPM</td><td>Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung Business Intelligence
Project Business Intelligence</td><td>Sprache
Deutsch oder Englisch, wenn von den Modul-teilnehmern gewünscht (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung: 2 SWS
Projekt: 2 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden kennen den elementaren Aufbau von Data Warehouse Systemen und sind mit den zentralen Konzepten der Informationsvisualisierung vertraut [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden sind in der Lage, die Konzepte des Data Warehousing in realen Anwendungsszenarien konzeptionell und operativ umzusetzen. Sie können Kennzahlen mittels geeigneter Methoden visualisieren. [Instrumentelle Fertigkeiten, 7]
Sozialkompetenz
Die Studierenden erarbeiten gemeinsam Lösungsansätze zu vorgegebenen Fragestellungen [Mitgestaltung, 7]</td></tr>
<tr><td></td><td colspan="6">Selbstständigkeit
Konzeption und Aufbau von Szenarien zur Erfassung, Aufbereitung und Analyse von Kennzahlen wird in Bezug auf die jeweiligen Anforderungen kritisch diskutiert. [Reflexivität, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Abgrenzung dispositive vs. operative Datenbestände (OLTP / OLAP)
Data Warehouse Architekturen
ETL-Prozesse (Datenqualität, Datenbereinigung, Transformation, etc.
Logische und semantische Datenmodelle für Data Warehouses (Star-/Snowflake-Schema,…)
Implementierung von Data Warehouses (MOLAP, ROLAP,..)
spezielle Aspekte im Zusammenhang mit Data Warehouses (slowly changing dimensions,…)</td></tr>
</table>

	Date Warehouse Projekte (agiles Vorgehen) Aufbau eines Data Warehousing Prozesses mittels SAP BW on HANA Visualisierung von Kennzahlen Konzeption und Aufbau von Dashoards Visual Analytics (Reduktion von Darstellungsdimensionen, Visualisierung von Objekten auf Grundlage von Unähnlichkeitsmaßen…)
	Empfohlene Literaturangaben: Bauer, A, Günzel, H (Hrsg): Data Warehouse Systeme – Architekur, Entwickung, Anwendung, dpunkt verlag, 2013 Müller, R.M., Lenz, H.-J.: Business Intelligence, Springer Vieweg, 2013 Kemper, H. G., Mehanna, W., & Unger, C. : Business Intelligence– Grundlagen und praktische Anwendungen, Vieweg, Wiesbaden, 2004, ISBN:3834807192 Klein, A., Gräf, J.: Reporting und Business Intelligence, Haufe-Lexware, 2014, ISBN: 364804771X Sharda, T. Aronson, King, A.:Business Intelligence: A Managerial Approach, Pearson Verlag, 2008, ISBN: 013610066X Kohlhammer, J., Proff, D.U., Wiener, A.: Visual Business Analytics: Effektiver Zugang zu Daten und Informationen. dpunkt.verlag GmbH, 2014, ISBN: 3864900441
5	**Teilnahmevoraussetzungen:** Empfohlen: Datenbank-Grundlagen
6	**Prüfungsformen***:* Klausur 90 min., benotet Praktische Arbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene schriftliche Modulprüfung; erfolgreiche Bearbeitung der Aufgaben im Praktikum
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc., Advanced IT Security M.Sc., Systems Engineering M.Eng. (Für SE-Studierende ergibt sich durch das Belegen des Moduls ggf. ein höherer Workload als in StuPO vorgesehen)
9	***Modulverantwortliche(r):*** Prof. Dr. Bernd Stauß Dozenten: Prof. Dr. Bernd Stauß, N.N.
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

1.1.3 53160 – Electronic System-Level Design

Studiengang: INF
StuPO-Version: 21.2

Semester: WS 2022/23
Letzte Bearbeitung: 14.09.22

<table>
<tr><td colspan="8">Modul: Electronic System-Level (ESL) Design</td></tr>
<tr><td colspan="2">Kennnummer
53160</td><td>Work-load
150</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
1. Semester</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
LV 53165 ESL Design 1
LV 53166 ESL Design 2</td><td colspan="2">Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
90</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="8">Lehrform(en) / SWS:
Vorlesung + Übung ESL Design 1, Umfang 15 x 2 = 30 SWS
Vorlesung + Übung ESL Design 2, Umfang 15 x 2 = 30 SWS</td></tr>
<tr><td>3</td><td colspan="8">Lernergebnisse (learning outcomes), Kompetenzen:
Kompetenz Wissen
Kenntnis und Verständnis der Entwurfsebene ESL und deren Methoden und Werkzeuge. [Wissen, 7]
Kompetenz Fertigkeiten
Fähigkeit zur Modellierung und Simulation von Systemen unter Anwendung von ESL-Methoden. [Instrumentelle Fertigkeiten, 7]
Sozialkompetenz
Diskussion und Konsolidierung der selbständig erarbeiteten Lösungen der Übungsaufgaben. [Kommunikation, 6]
Selbstständigkeit
Transfer der Vorlesungsinhalte in die praktische Anwendung im Rahmen der Übungen. [Lernkompetenz, 6]</td></tr>
<tr><td>4</td><td colspan="8">Inhalte:
Der Entwurf mikroelektronischer Systeme ist durch einen kontinuierlichen Anstieg der Systemkomplexität einhergehend mit sich stetig verschärfenden Systemanforderungen, etwa hinsichtlich Sicherheit, Zuverlässigkeit oder Performanz, geprägt. Um dieser Entwicklung nachzukommen, wurde in den letzten Jahren eine neue höhere Abstraktionsebene des Systementwurfs mit Bezeichnung "Electronic System-Level" ("ESL") etabliert. Die Lehrveranstaltungen des Moduls "Electronic System-Level Design" liefern eine Einführung in diese neue Systemsicht und geben einen Überblick über deren Entwurfsmethoden und -werkzeuge. Anhand der eng mit der Entwicklung von ESL verwobenen C++-basierten Systembeschreibungssprache SystemC werden die wesentlichen Konzepte und Techniken des ESL Designs vorgestellt und neue Mechanismen dieser Ebene, etwa das Prinzip der transaktionsbasierten Modellierung (Transaction-Level Modeling, TLM), vermittelt (Teil Vorlesung) und im Rahmen von praktischen Übungen am Rechner vertieft (Teil Übung).</td></tr>
</table>

	ESL Design 1: - Einführung in ESL Design - Grundlagen des Systementwurfs - Die Systembeschreibungssprache SystemC ESL Design 2: - Advanced SystemC: Transaction Level Modeling - ESL Entwurfsmethoden
	Empfohlene Literaturangaben: - Kesel F.: Modellierung von digitalen Systemen mit SystemC: Von der RTL- zur Transaction- Level-Modellierung. Oldenbourg Wissenschaftsverlag. - Grötker T., Swan S., Martin G., Liao S.: System Design with SystemC. Springer-Verlag. - Accellera Systems Initiative: SystemC Download-Package (Simulator + Dokumentation). https://www.accellera.org/downloads/standards/systemc - IEEE Standard 1666-2011: Standard SystemC Language Reference Manual. https://ieeexplore.ieee.org/document/6134619
5	**Teilnahmevoraussetzungen:** Grundlagen der Programmierung und Programmentwicklung in C/C++. ESL Design 2 setzt inhaltlich auf ESL Design 1 auf, die beiden Lehrveranstaltungen finden daher innerhalb des Semesters nicht nebenläufig sondern in sequentieller Abfolge statt (ESL Design 1 in der ersten Semesterhälfte, daran anschließend ESL Design 2 in der zweiten Semesterhälfte).
6	**Prüfungsformen***:* ESL Design 1: Klausur 45 Minuten, benotet ESL Design 2: Klausur 45 Minuten, benotet Übungen unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** ESL Design 1: Bestandene Klausur (2,5 ECTS) ESL Design 2: Bestandene Klausur (2,5 ECTS)
8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng., Advanced IT Security M.Sc., Business and Security Analytics M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Joachim Gerlach Dozenten: Prof. Dr. Joachim Gerlach
10	***Optionale Informationen:***

1.1.4 XXXXX – Einführung in die Grundlagen der Quantuminformatik

Studiengang: INF
StuPO-Version: 21.2

Semester: WS 2022/23
Letzte Bearbeitung: 14.09.22

Modul: Einführung in die Grundlagen der Quantuminformatik					
Kennnummer XXXX	**Workload** 180	**Modulart** WP	**Studiensemester** 1	**Dauer** 1	**Häufigkeit** WS

1	**Lehrveranstaltung(en)** a. XXX Voerlesung Grundlagen der Quantuminformatik b. XXX Übung. Grundlagen der Quantuminformatik	**Sprache** a.,b., deutsch oder englisch	**Kontakt-zeit** a. 30 b. 30	**Selbst-studium** 120	**Credits (ECTS)** 6
2	**Lehrform(en) / SWS:** a. Vorlesung, b. Übung				
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Beherrschen der Grundlagen der Quanteninformatik: Grundlagen der Quantenmachnik und Ihrer potenziellen Anwendung in der Datenverarbeitung. *[Wissen, 7]* *Kompetenz Fertigkeiten* Fähigkeit die Weiterentwicklung der Quanteninformatik zu verfolgen und die Auswirkungen auf IT-Industrie abschätzen zu können. *[Instrumentelle Fertigkeiten, 7]* *Sozialkompetenz* Nicht relevant *Selbstständigkeit* Sind in der Lage komplexe Fragestellungen selbständig zu Bearbeiten und eigenen Fortschritt adäquat zu bemessen *[Lernkompetenz, 7]*				
4	Inhalte: Grundlagen der Quantentheorie: Postulate der Theorie, Prozess der Messung in Quantenmechanik. Verschränkung. Entropie. Quantum Gates und Schaltungen. Anwendungsbeispiele: Transportation, Cloning, Cryptographie. Typen der Quantumalgorithmen und Beispiele.				

	Empfohlene Literaturangaben: Michael Nielsen, Issak Chuang, Quantum Computation and Quantum Information, Cambridge University Press. Benjamin Schumacher and Mike Westmoreland, Quantum Processes Systems, and Information, Cambridge University Press. Mark M. Wilde, Quantum Information Theory, Cambridge University Press. Thomas Cover, Elements of Information Theory, Wiley.
5	**Teilnahmevoraussetzungen:** Gute Mathematikkentnisse auf dem Niveau der Mathematik für Informatik (Bachelor). Solide Grunkentnisse der komplexen Arithmetik und der linearen Algebra sind wichtig. Der Begriff des Tensorproduktes und die Eigenvektoren werden in der Vorlesung wiederholt. Keine Vorkentnisse der Quantenmechanik werden vorausgesetzt.
6	**Prüfungsformen***:* Mündliche Prüfung 45 min. (Modulprüfung)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene mündliche Prüfung
8	***Verwendbarkeit des Moduls:*** Advanced IT Security M.Sc., Business and Security Analytics M.Sc., Systems Engineering M.Eng. (Für SE-Studierende ergibt sich durch das Belegen des Moduls ggf. ein höherer Workload als in StuPO vorgesehen)
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski Dozent: Dr. Andreas Teshler
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

1.1.5 56000 - Funktionale Programmierung

Studiengang: INF
StuPO-Version: 21.2

Semester: WS 2022/23
Letzte Bearbeitung: 14.09.22

Modul: Funktionale Programmierung						
Kennnummer 56000	**Work-load** 150	**Modulart** WPM	**Studiensemester** 1	**Dauer** 1	**Häufigkeit** WS	
1	**Lehrveranstaltung(en)** Funktionale Programmierung	**Sprache** Deutsch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 90	**Credits (ECTS)** 5	
2	**Lehrform(en) / SWS:** Vorlesung mit Übung					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen funktionale Programmierkonzepte, die Beziehung zu Konzepten der Kategorientheorie (Morphismen) sowie deren Umsetzungen in Haskell *[Wissen, 7]* Weiter haben die Studierenden Kenntnisse der streng statischen Typisierung am Beispiel des Hindley-Millner Typsystems *[Wissen, 7]* Die Studierenden kennen experimentelle forschungslastige Programmierkonzepte und kennen aktuelle Forschungsfragestellungen im Entwurf von Programmiersprachen. *[Wissen, 7]* *Kompetenz Fertigkeiten* Selbständiges entwickeln und schreiben funktionaler Programme unter Einsatz des gewonnenen Wissens *[Instrumentelle Fertigkeiten, 7]* *Sozialkompetenz* Nicht relevant *Selbstständigkeit* Studierende verstehen das Lernen als einen komplexen Prozess, der individuelle sowie auch soziale Kompetenzen umfasst; Sie verfügen über Motivation und Ausdauer, um komplexe Inhalte zu erlernen und verwenden dabei Ansätze des wissenschaftlichen Forschens *[Eigenständigkeit/Verantwortung, 7]*					
4	**Inhalte*:*** - Funktionen (Extensionalität, Currying, Operatoren, Sections, Funktionskomposition) - Datentypen (Aufzählungstypen, Summentypen, Produkttypen, rekursive Datentypen) - Listen (Konkatenation, Homomorphismen und Katamorphismen auf Listen) - Bäume (Homomorphismen und Katamorphismen auf Bäumen) - Typisierung (Typsystem, Typklassen, Konstruktorklassen) - Monaden					

	Empfohlene Literaturangaben: http://book.realworldhaskell.org/
5	**Teilnahmevoraussetzungen:** Grundkenntnisse in Programmierkonzepten und Paradigmen (wie z.B. Iterative oder Objektorientiert Programmierung) Vorlesungen Software Entwicklung, Programmieren I und II
6	**Prüfungsformen***:* Klausur 90 Minuten
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen der Klausur
8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng., Advanced IT Security M.Sc., Business and Security Analytics M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Nemirovski Dozenten: Herr Brettschneider, N.N.
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

1.1.6 55541 – IT-Sicherheit und IT-Angriffe

Studiengang: INF
StuPO-Version: 21.2

Semester: WS 2022/23
Letzte Bearbeitung: 14.09.222

Modul: IT-Sicherheit und IT-Angriffe						
Kennnummer	**Work-load** 90 h	**Modulart** WPF	**Studiensemester** 1	**Dauer** 1 Semester	**Häufigkeit** WS	
1	**Lehrveranstaltung(en)** Vorlesung IT-Sicherheit und IT-Angriffe		**Sprache** Deutsch	**Kontakt-zeit** 2 SWS / 30 h	**Selbst-studium** 60 h	**Credits (ECTS)** 3
2	**Lehrform(en) / SWS:** Vorlesung: 2 SWS					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden Kennen die Kategorien der Schadsoftware und deren Auswirkung *[Wissen, 7]* *Kompetenz Fertigkeiten* Die Studierenden Kennen die Kategorien der Schadsoftware und deren Auswirkung /Kompetenzausprägung wählen *7]* *Sozialkompetenz* Die Studierenden Kennen die Kategorien der Schadsoftware und deren Auswirkung *[Team-/Führungsfähigkeit, 7]* *Selbstständigkeit* Die Studierenden sind in der Lage größere Aufgaben, deren Bearbeitung auch mehrere Tage in Anspruch nimmt, verantwortungsvoll zu erfüllen, realistische Ziele zu definieren und diese konsequent zu verfolgen /Kompetenzausprägung wählen *7]*						
4	**Inhalte***:* • Grundlagen der IT-Sicherheit • IT-Bedrohungen und Abwehrmaßnahmen • Schadsoftware (Computerviren, Würmer, Trojanisches Pferd) • Angriff über Pufferüberlauf (Mechanismen, Manipulation des Programmablaufes, Erstellen von Schadcode, Überlegungen zur Abwehr von Schadcode) • Bedrohungen im Rechnernetz und Abwehrmaßnahmen • Angriffe auf Schicht 2, 3, und 4) und Abwehrmaßnahmen • Bedrohungen aus dem Internet und Abwehrmaßnahmen • Angriff auf einen Browser • E-Mail-Client Angriffe • Spam-Mails und Phishing-Mails						

	• DoS und DDoS • Python-Hacks (Kelogger, Ransomware, WLAN-Probe-Requeststst, Passwortangriff)
	Empfohlene Literaturangaben: Alan J White (Autor), Ben Clark: Blue Team Field Manual. Create Space Independent Publishing Platform (2017); Cameron H. Malin, Eoghan Casey, James M. Aquilina: Malware Forensics Guide for Windows Systems, Digital Forensics Field Guides. Elsevier (2012) Claudia Eckert. IT-Sicherheit - Konzepte - Verfahren - Protokolle. Oldenbourg Verlag, München, überarbeitete und erweiterte Auflage edition, 2008a. ISBN 978-3-486-70687-1. Klein, T. (2003): Buffer Overflows und Format-String-Schwachstellen: Funktionsweisen, Exploits und Gegenmaßnahmen; Heidelberg: dpunkt-Verlag Weitere Literatur, insbesondere aktuelle wissenschaftliche Artikel, warden in der Vorlesung bekannt gegeben.
5	Teilnahmevoraussetzungen: Die Studierenden besitzen Kenntnisse, Fertigkeiten und Erfahrungen in • Betriebssysteme • Netzwerke • Netzwerksicherheit • Programmierung in einer Hochsprache und einer Skriptsprache
6	**Prüfungsformen***:* Klausur 60 Min; benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandenes Referat und bestandene Praktische Arbeit
8	***Verwendbarkeit des Moduls:*** Systems Endineering M.Eng.; Business and Security Analytics M.Sc., Advanced IT Security M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Rieger Dozenten: Prof. Dr. Rieger
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

1.1.7 51700 - Incident Response and Malware Defence

Semester: WS 2022/23

Studiengang: INF
StuPO-Version: 21.2

Letzte Bearbeitung: 14.09.22

<table>
<tr><td colspan="7">Modul: Incident Response und Malware Defense</td></tr>
<tr><td colspan="2">Kennnummer
52700</td><td>Workload
150 h</td><td>Modulart
P</td><td colspan="2">Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Vorlesung Incident Response und Malware Defense
Praktikum Incident Response und Malware Defense</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
60 SWS / 4 h</td><td>Selbst-studium
90</td><td>Credits (ECTS)
5</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung: 2 SWS
Praktikum: 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden Kennen die Kategorien der Schadsoftware und deren Auswirkung. [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden können Methoden entwickeln und anwenden um IT-Angriffe zu erkennen, zu analysieren, einzudämmen und zu beseitigen
[Systemische Fertigkeiten, 7]
Sozialkompetenz
Die Studierenden sind in der Lage, sich mittels dem spezifischen Vokabular auszudrücken, sich verständlich zu machen und andere zu verstehen [Kommunikation, 7]
Selbstständigkeit
Die Studierenden sind in der Lage größere Aufgaben, deren Bearbeitung auch mehrere Tage in Anspruch nimmt, verantwortungsvoll zu erfüllen, realistische Ziele zu definieren und diese konsequent zu verfolgen [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:

1. Der Incident Response Prozess: Preparation, Detection, Analysis, Containment, Recovery, Post Incident Activity
Veranschaulichung und Vertiefung der Phasen an Beispielen
2. Klassifikation und Taxonomie von Incidents
3. Systemsicherung: Sicherung systemwichtiger Daten
4. Spurensicherung: Netzbasierte Spuren (Netzwerkmitschnitte und Netzwerk-Komponenten), Host-basierte Spuren (persistente und nicht persistente Spuren,</td></tr>
</table>

	Arbeitsspeicher) 5. Spurenanalyse: Netzbasierte Spuren (Netzwerkmitschnitte, Log-Dateien), Host-basierte Spuren (Arbeitsspeicher, Log-Dateien, Dateisysteme) 6. Detektion: Signatur-basierte und Regel-basierte Methoden 7. Methoden zur Einschränkung der Schadwirkung: Sandbox, Zugriffsschutz, Rechteüberwachung, Firewall, Proxy, Netzwerksegmentierung 8. Wiederherstellung: Backup und Systemsicherung anwenden 9. Statische Malware-Analyse: Aufbau der Malware, verwendete Bibliotheken, maliziöse Funktionen und Strukturen 10. Dynamische Malware-Analyse: Wirkungsweise der Malware, Schadwirkung lokalisieren 11. Reporting zur Malware-Analyse: Wirkungsweise, Schadenspotential, potentielle Quellen 12. Reporting zum Incident Response-Prozess 13. Post Incident Aktivitäten: Maßnahmen zur Verbesserung der Sicherheit treffen; Training von Incidents Beispiele für Projekte • Aufsetzen einer Signaturbasierten Detektion in einem System. Angriff auf das System. Incident behandeln • Aufsetzen eines Systems mit Schwachstellen (z. B. offene USB-Anschlüsse oder Mail-Clients ohne Makrovirenschutz); Eintragen einer Malware; Incident Response Prozess ausführen • Entwicklung einer Malware, die vermutete Systemschwächen ausnutzt (z. B. Keylogger, DLL-Injektor); Erproben der Malware an einem System mit Malware-Schutz; Incident Respons anwenden
	Empfohlene Literaturangaben: Alan J White (Autor), Ben Clark: Blue Team Field Manual. Create Space Independent Publishing Platform (2017) Gerard Johansen: Digital Forensics and Incident Response.Packt (2012 Johansen, Gerard. Digital Forensics and Incident Response: A practical guide to deploying digital forensic techniques in response to cyber security incidents (Kindle-Positionen14-15). Packt Publishing. Kindle-Version. Cameron H. Malin, Eoghan Casey, James M. Aquilina: Malware Forensics Guide for Windows Systems, Digital Forensics Field Guides. Elsevier (2012) Weitere Literatur, insbesondere aktuelle wissenschaftliche Artikel, werden in der Vorlesung bekannt gegeben.
5	**Teilnahmevoraussetzungen:** Die Studierenden besitzen Kenntnisse, Fertigkeiten und Erfahrungen in • Betriebssysteme • Netzwerke • Netzwerksicherheit • Programmierung in einer Hochsprache und einer Skriptsprache
6	**Prüfungsformen***:* Referat 20 min. mit Ausarbeitung, benotet Praktische Arbeit mit Präsentation 20 min. und Handout, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandenes Referat und bestandene Praktische Arbeit
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, Advanced IT Security Pflichtmodul in Systems Engineering - Security Systems!

9	***Modulverantwortliche(r):*** Prof. Dr. Rieger Dozenten: Prof. Dr. Rieger
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

1.1.8 Xxxxx – Netzwerksicherheit

Studiengang: INF
StuPO-Version: 21.2

Semester: WS 2022/23
Letzte Bearbeitung: 14.09.22

<table>
<tr><td colspan="8">Modul: Netzwerksicherheit</td></tr>
<tr><td colspan="2">Kennnummer
XXX</td><td>Work-load
75</td><td>Modulart
WPM</td><td>Studiensemester
1. Semester</td><td>Dauer
1 Semester</td><td colspan="2">Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Vorlesung/Übungen
Netzweksicherheit</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
2 SWS / 30 h</td><td>Selbst-studium
45 h</td><td>Credits (ECTS)
2,5</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung + Übung Netzweksicherheit, Umfang 15 x 2 = 30 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:
Kompetenz Wissen
Grundsätze der Sicherheit von Rechnernetzen • Wirkung von Netzwerkkomponenten • Wirkungsweisen von Schadsoftware im Rechnernetz • Sensoren zur Aufzeichnung von Netzwerkverkehr • Möglichkeiten der Netzwerkanalyse • Szenarien bekannter Netzwerkangriffe. [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden können
• Zielgenaue Netzwerkaufzeichnungen anfertigen• Netzwerkaufzeichnungen auswerten • Vorgänge im rechnernetz analysieren• Mit Netzwerkkomponenten und geeigneter Software Netzwerk absichern• Penetrationstests auf Rechnernetz ausführen [Instrumentelle Fertigkeiten, 7]
Die Studierenden sind fähig
• Prinzipien sicherer Rechnernetze umzusetzen
• Methoden der Netzwerkforensik anwenden
[Systemische Fertigkeiten, 7]
Sozialkompetenz
Diskussion und Konsolidierung der selbständig erarbeiteten Lösungen der Übungsaufgaben. [Kommunikation, 6]
Selbstständigkeit
Transfer der Vorlesungsinhalte in die praktische Anwendung im Rahmen der Übungen. [Lernkompetenz, 6]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
• Netzwerkpläne lesen, verstehen und optimieren
• Netzwerkscan ausführen und auswerten
• Geräte im Netzwerk erkennen
• Angriffe im Netzwerk
• Sichere Protokolle und Verfahren
• Netzwerkabsicherung mit Firewall usw.
• Network Security Monitoring: Mitschnitt, Detektion, Analyse</td></tr>
</table>

	• Auswertung aktiver Netzwerkkomponenten • Auswertung von Serverdiensten (Webserver, Proxy usw.)
	Empfohlene Literaturangaben: - Chris Sanders and Jason Smith. Applied Network Security Monitoring - Collection, Detection, and Analysis. Syngress, 2014. Eckert: IT-Sicherheit, Verlag: De Gruyter Oldenbourg; Auflage: 9., aktualisierte Auflage (26. September 2014) Schwenk: Sicherheit und Kryptographie im Internet. Verlag: Springer Vieweg; Auflage: 4., überarb. u. erw. Aufl. 2014 (27. August 2014) O'Conner: Violent Python. Verlag: Syngress (20. Dezember 2012)
5	**Teilnahmevoraussetzungen:** Grundlagen der Programmierung und Programmentwicklung in C/C++. ESL Design 2 setzt inhaltlich auf ESL Design 1 auf, die beiden Lehrveranstaltungen finden daher innerhalb des Semesters nicht nebenläufig sondern in sequentieller Abfolge statt (ESL Design 1 in der ersten Semesterhälfte, daran anschließend ESL Design 2 in der zweiten Semesterhälfte).
6	**Prüfungsformen***:* Klausur 60 min, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur 60 min, benotet
8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng., Advanced IT Security M.Sc., Business and Security Analytics M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Martin Rieger Dozent: Prof. Dr. Martin Rieger
10	***Optionale Informationen:***

1.1.9 51600 – Open Source Intelligence

Studiengang: INF
StuPO-Version: 21.2

Semester: WS 2022/23
Letzte Bearbeitung: 14.09.22

<table>
<tr><td colspan="8">Modul: Open Source Intelligence</td></tr>
<tr><td colspan="2">Kennnummer
51600</td><td>Workload
180 h</td><td>Modulart
WPM</td><td>Studiensemester
1</td><td>Dauer
1 Semester</td><td colspan="2">Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung Open Source Intelligence
Praktikum Open Source Intelligence</td><td>Sprache
Deutsch oder Englisch (Literaturstudium in Deutsch und Englisch erforderlich)</td><td>Kontakt-zeit
60 SWS / 4 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung, Übungen, Seminar: 3 SWS
Praktikum: 1 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden verfügen über ein breites Wissen über die technischen, gesellschaftlichen und rechtlichen Rahmenbedingungen für einen OSINT Einsatz, [Wissen, 6]
Die Studierenden verfügen über ein tiefes Wissen im Bereich von OSINT Terminologien, Methoden und Techniken, [Wissen, 7]

Kompetenz Fertigkeiten
Können einen OSINT Einsatz konzeptionell strukturieren und geeignete Methoden und Werkzeuge auswählen [Instrumentelle Fertigkeiten, 7]

Können die Leistungsfähigkeit vorhandener OSINT Werkzeuge beurteilen und selbstständig neue OSINT Verfahren und Werkzeuge entwickeln [Systemische Fertigkeiten, 7]

Können per OSINT ermittelte Daten hinsichtlich ihrer technischen und juristischen Verwertbarkeit beurteilen und ihren Informations- und Intelligence Gehalt einschätzen [Beurteilungsfähigkeit, 7]

Sozialkompetenz
Studierende können sich auf tiefer Expertenebene mit der Fachcommunity unterhalten, Erkenntnisse und Methoden diskutieren und ihr Expertenwissen auch Fachabteilungen vermitteln [Kommunikation, 7]

Selbstständigkeit
Studierende können neue OSINT Anwendungen eigenständig identifizieren und erforschen sowie mit der Fachcommunity diskutieren [Eigenständigkeit/Verantwortung, 7]</td></tr>
</table>

	Aktuelle Aufgabenstellungen und Probleme aus dem OSINT Bereich können eigenständig anhand der aktuellen Forschung im Print- und Preprintbereich erschlossen werden *[Lernkompetenz, 7]*
4	**Inhalte*:*** Vorlesung, Seminar, Praktikum • Auffrischung relevanter Grundlagen der IT Sicherheit, Digitalen Forensik und Internettechnologien • Anonymisierung und De-Anonymisierung im Surface-, Deep- und Darknet • Ermittlungstaktisches- / nachrichtendienstliches Vorgehen • OSINT Grundlagen, Terminologien, Taxonomien • OSINT Methoden, Tools, Techniken • Legaler, moralischer und ethischer Rahmen • Analyse und Bewertung von OSINT Erkenntnissen • Praktische Anwendungen • Wissenschaftliche Recherche, Arbeit und Forschung im OSINT Bereich • Relevante wissenschaftliche Konferenzen, Journals und Plattformen
	Empfohlene Literaturangaben: Akhgar, B., Bayerl, P.S., Sampson, F.S.: OpenSource Intelligence Investigation – From Strategy to Implementation, Springer, 2017 Bazzell, M.: Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information, 5. Auflage, CreateSpace Independent Publishing Platform, 2016 U.S.Army: NATO OpenSource Intelligencehandbook, online, http://www.au.af.mil/au/awc/awcgate/nato/osint_hdbk.pdf Attrill, A.: Cyberpsychology, 2015, Oxford University Press Gollmann, D.: Computer Security, 3. Auflage, Wiley, 2012 Tavani, H.T.: Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing, 4. Auflage, Wiley, 2013 Spinello, R.: Cyberethics: Morality and Law in Cyberspace 6th Edition, Jones & Bartlett Learning, 2016 A Gift of Fire: Social, Legal, and Ethical Issues for Computing Technology, 5th Edition, Pearson, 2017 Biskup, J.: Security in Computing Systems, Springer, 2010 Ausgewählte Literatur bekannter Top-Tier Konferenzen im OSINT Bereich Weitere Literatur wird in der Vorlesung vorgestellt.
5	**Teilnahmevoraussetzungen:** Grundlagen Betriebssysteme und Netzwerke, Grundlagen IT Sicherheit und Digitaler Forensik, Programmierung in einer Skriptsprache
6	**Prüfungsformen*:*** Referat 20 min. inkl. wissenschaftlicher Ausarbeitungen und Poster, Diskussion, benotet Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Ausreichend bewertetes Referat erfolgreiche Teilnahme am Praktikum

8	***Verwendbarkeit des Moduls:*** Business and Security Analytics M.Sc., Systems Engineering M.Eng. Pflichtmodul in Advanced ITS
9	***Modulverantwortliche(r):*** Prof. Morgenstern Dozenten: Prof. Dr. Fein
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

1.1.10 Xxxxx - Post-Quantum Cryptography and Quantum Key Distribution

Studiengang: INF
StuPO-Version:.21.2

Semester: WS 2022/23
Letzte Bearbeitung: 12.09.2022

<table>
<tr><td colspan="7">Modul: Post-Quantum Cryptography and Quantum Key Distribution</td></tr>
<tr><td colspan="2">Kennnummer
z.B. 15100</td><td>Work-load
180 h</td><td>Modulart
WP</td><td colspan="2">Studiensemester
1. Semester</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
a. Vorlesung, Praktikum Post-Quantum Cryptography
b. Vorlesung Quantum Key Distribution</td><td>Sprache
Englisch (Literaturstudium in Deutsch und Englisch erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung, Praktikum Post-Quantum Cryptography: 3 SWS
Vorlesung Quantum Key Distribution: 1 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden können die Gefahren von Quantencomputern für etablierte kryptographische Verfahren erklären und quantensichere Verfahren aufzählen, die nicht betroffen sind. [Wissen, 7]

Die Studierenden können Funktionsweise, Voraussetzungen und Vor- und Nachteile von Quantum Key Distribution aufzählen. [Wissen, 7]

Kompetenz Fertigkeiten
Die Studierenden können quantensichere kryptographische Verfahren für eine Anwendung auswählen und implementieren. [Instrumentelle Fertigkeiten, 7]

Die Studierenden können die Eignung von Quantum Key Distribution für eine Anwendung bewerten. [Beurteilungsfähigkeit, 7]

Sozialkompetenz
Die Studierenden können sich auf Expertenebene mit der Fachcommunity über Post-Quatum Cryptography und Quantum Key Distribution unterhalten, Erkenntnisse und Methoden diskutieren und ihr Expertenwissen auch Fachabteilungen vermitteln [Kommunikation, 7]

Die Studierenden können mögliche gesellschaftliche Auswirkungen von aktuellen und neuen Entwicklungen im Quantencomputing für die IT-Sicherheit erkennen, bewerten und mit Laien- und Fachpublikum diskutieren. [Kommunikation, 7]</td></tr>
</table>

	Selbstständigkeit Die Studierenden können neue Anwendungen für Post-Quatum Cryptography und Quantum Key Distribution selbstständig identifizieren und erforschen sowie mit der Fachcommunity diskutieren. /Kompetenzausprägung wählen /Niveaustufe wählen Die Studierenden können neue Aufgabenstellungen und Probleme aus den Bereichen Post-Quatum Cryptography und Quantum Key Distribution selbstständig anhand der aktuellen Forschungsergebnisse erarbeiten. /Kompetenzausprägung wählen /Niveaustufe wählen
4	**Inhalte*:*** Vorlesung, Praktikum Post-Quantum Cryptography: • Auffrischung relevanter Grundlagen der Kryptologie, IT Sicherheit und Mathematik • Einführung in Quantum Computing • Gefahren durch Quantencomputer für etablierte Verschlüsselungsverfahren • Prinzipien für Post-Quantum Cryptography • Implementierung konkreter Post-Quatum-Verschlüsselungsverfahren Vorlesung Quantum Key Distribution: • Auffrischung relevanter Grundlagen der Kryptologie und IT Sicherheit • Grundlagen der Quantenmechanik • Quantum Key Distribution • Angriffsszenarien
	Empfohlene Literaturangaben: Empfohlene Literaturangaben
5	**Teilnahmevoraussetzungen:** Grundlagen der Kryptologie (insbesondere Public Key Cryptography), IT-Sicherheit, Programmierkenntnisse
6	**Prüfungsformen***:* Wissenschaftliche Ausarbeitung inkl. Kurzpräsentation, benotet Referat 20 min., Diskussion, benotet
7	**Voraussetzungen für die Vergabe von Kreditpunkten:** Ausreichend bewertete Ausarbeitung Ausreichend bewertetes Referat
8	**Verwendbarkeit des Moduls:** Advanced IT Security M.Sc., Business and Security Analytics M.Sc., Systems Engineering M.Eng. (Für SE-Studierende ergibt sich durch das Belegen des Moduls ggf. ein höherer Workload als in StuPO vorgesehen)
9	**Modulverantwortliche(r):** Prof. Dr. Henrich Dozent: Prof. Dr. Jungk
10	**Optionale Informationen:** Studiengangsspezifische, zusätzliche Informationen zum Modul

1.1.11 51400 – Semantic Web

Studiengang: INF
StuPO-Version: 21.2

Semester: WS 2022/23
Letzte Bearbeitung: 14.09.22

Modul: Semantic Web					
Kennnummer 51400	**Workload** 180	**Modulart** WP	**Studiensemester** 1	**Dauer** 1	**Häufigkeit** WS

1	**Lehrveranstaltung(en)** a. 51405 Semantic Web b. 51420 Proj. Semantic Web	**Sprache** a.,b., deutsch oder englisch	**Kontakt-zeit** a. 30 b. 30	**Selbst-studium** 120	**Credits (ECTS)** 6
2	**Lehrform(en) / SWS:** a. Vorlesung, b. Projektarbeit				
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Vertieftes verstehen Formaler Logiken und Reasoning-Aufgaben *[Wissen, 7]* Vertieftes Verstehen von Semantic Web -Technologien als Instrument für interoperable Wissensbeschreibung *[Wissen, 7]* *Kompetenz Fertigkeiten* Können Ontologien mit Hilfe von Tools wie Editoren und Reasoner entwickeln und Anwenden *[Instrumentelle Fertigkeiten, 6]* Können Wissensstrukturen von Komplexen Wissensdomains analysieren und formal beschreiben *[Systemische Fertigkeiten, 7]* *Sozialkompetenz* Sind in der Lage komplexe Formalismen zu kommunizieren und Diskussion auf Grundlage der Formalismen und mit Anwendung des formallogischen Vokabular zu führen *[Kommunikation, 7]* *Selbstständigkeit* Sind in der Lage komplexe Fragestellungen selbständig zu Bearbeiten und eigenen Fortschritt adäquat zu bemessen *[Lernkompetenz, 7]*				
4	Inhalte: Die Grundlagen: - Definition und Begriffsklärung - Security Analytics Use Cases - Data Sourcess und Methoden der Datensammlung - Real time Data Harvesting - Anwendung der Security Analytics Ergebnissen und ihr Impact - Basic Security Analytics Costs - Advanced persistent threats - Security Analytics und Digitale Forensics				

	Security Analytics Tools and Services, u.a.: - Blue Coat Security Analytics Platform, - Lancope Stealth Watch System - JuniperNetworks JSA Series Secure Analytics - EMC RSASecurity Analytics NetWitness - FireEye Threat Analytics Platform - Arbor Networks Security Analytics - Click Security Click Commander - Hexis Cyber Solutions' NeatBeat MON - Sumo Logics' cloud service. - Security Onion - Splunk - Elastic Stack
	Empfohlene Literaturangaben: Lehto, Martti, and Pekka Neittaanmäki, eds. Cyber security: Analytics, technology and automation. Vol. 78. Springer, 2015. Talabis, Mark, et al. Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data. Syngress, 2014. THOMAS, TONY P. VIJAYARAGHAVAN, Athira P. Vijayaraghavan, and Sabu Emmanuel. MACHINE LEARNING APPROACHES IN CYBER SECURITY ANALYTICS. SPRINGER VERLAG, SINGAPOR, 2020.
5	**Teilnahmevoraussetzungen:** Kenntnisse in IT Security (DQR 6), Praktische Fertigkeiten in Netzwerken und Programmierung (DQR 6)
6	**Prüfungsformen***:* Klausur 90 Min. (Modulprüfung)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur
8	***Verwendbarkeit des Moduls:*** Advanced IT Security M.Sc., Business and Security Analytics M.Sc., Systems Engineering M.Eng.(Für SE-Studierende ergibt sich durch das Belegen des Moduls ggf. ein höherer Workload als in StuPO vorgesehen)
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski Dozent: Prof. Dr. German Nemirovski
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

1.1.12 55541 – Smart Home: Entwurf und IT-Sicherheit

Studiengang: Systems Engineering, Advanced IT Security
Semester: WiSe 2022/2023
StuPO-Version: 18.1 / Version 1.0
Letzte Bearbeitung: 14.09.22

Modul: Smart Home: Entwurf und IT-Sicherheit					
	Work-load 180 h	**Modulart** WPF	**Studiensemester** 1	**Dauer** 1 Semester	**Häufigkeit** WS

1	**Lehrveranstaltung(en)**	**Sprache**	**Kontakt-zeit**	**Selbst-studium**	**Credits (ECTS)**
	Smart Home: Entwurf und IT-Sicherheit	Deutsch	80 h	100 h	6

2	**Lehrform(en) / SWS:** Vorlesung: 2 SWS Praktikum: 2 SWS

3	**Lernergebnisse (learning outcomes), Kompetenzen:**
	Kompetenz Wissen Die Studierenden kennen die Methoden und Komponenten eines Smart Home Systems *[Wissen, 7]*
	Kompetenz Fertigkeiten Die Studierenden sind in der Lage ein Smart Home-System zu entwerfen und auf Funktionalität, IT-Sicherheit und forensische Spuren zu analysieren *7]*
	Sozialkompetenz Die Studierenden können verantwortlich mit Aspekten von Smart Home umgehen, die dir Persönlichkeitssphäre betreffen und sind sich über die Wichtigkeit der damit verbundenen digitalen Beweise bewusst. *[Team-/Führungsfähigkeit, 7]*
	Selbstständigkeit Die Studierenden sind in der Lage größere Aufgaben, deren Bearbeitung auch mehrere Tage in Anspruch nimmt, verantwortungsvoll zu erfüllen, realistische Ziele zu definieren und diese konsequent zu verfolgen *[Eigenständigkeit/Verantwortung, 7]*

4	**Inhalte*:*** A Vorlesung 1 Einleitung Motivation und Zielsetzung, Stand der Technik 2 Grundlagen Internet of Things, Smart Home, Kommunikationsprotokolle, Message Queuing Telemetry Transport MQTT Open Home Automation Bus (OpenHAB) Alternativen zu OpenHAB Werkzeuge der digitalen Forensik

	3 OpenHAB Systembeschreibung von OpenHAB Einrichtung von OpenHAB Installation von Things Datenfluss von Sensorinformationen 4 Forensische Analyse Bestandsaufnahme am Tatort Identifikation und Kategorisierung der Spuren Analysemöglichkeiten von OpenHAB Automatisierte Extraktion der Spuren 4 Manipulation und Schwachstellen Sicherheit der Gesamtarchitektur Daten- und Datenbankmanipulationen Physische Manipulationen Schwachstellen in Protokollen Grenzen forensischer Massnahmen B Praktikum 1 Konzeption des Gesamtsystems Auswahl der Komponenten Beschaffung der Komponenten 2 Konfiguration Einrichtung von OpenHAB Installation von Things 3 Test Test der Komponenten Test von OpenHAB 4 Szenarien Erstellen eines "Drehbuchs" zur Nutzung des Gesamtsystems Umsetzung des "Drehbuchs" zur Nutzung des Gesamtsystems Spurenanalyse 5 IT-Sicherheit des Gesamtsystems Schwachstellenanalyse des Gesamtsystems Angriffe auf das Gesamtsystem Maßnahmen zur Verbesserung der IT-Sicherheit
	Empfohlene Literaturangaben: Empfohlene Literaturangaben
5	**Teilnahmevoraussetzungen:** • Die Studierenden besitzen Kenntnisse, Fertigkeiten und Erfahrungen in Betriebssystemen • Programmierung in einer Hochsprache und einer Skriptsprache

6	**Prüfungsformen***:* Hausarbeit mit Referat; benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur
8	***Verwendbarkeit des Moduls:*** Masterstudiengäng in INF
9	***Modulverantwortliche(r):*** Prof. Dr. Rieger Dozenten: Prof. Dr. Rieger
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul