

MODULHANDBUCH

gemäß der Studiengangsprüfungsordnung 2023

**STUDIENGANG
Internet-Sicherheit (Master)**

Inhaltsverzeichnis

Inhaltsverzeichnis	2
Modulkatalog	3
Ausgewählte Themen aus dem Bereich Internet und Sicherheit	4
Datenschutz und Ethik	6
Internet-Sicherheit A	8
Internet-Sicherheit B	10
Kolloquium zur Masterarbeit Internet-Sicherheit.....	13
Masterarbeit Internet-Sicherheit.....	15
Malware-Analyse und Cyber Threat Intelligence	17
Master-Projekt Internet-Sicherheit.....	19
Master-Seminar Internet-Sicherheit	21
Wissenschaftliche Vertiefung Internet-Sicherheit	23
Programmiermethodik und Sicherheit	25
Software Reverse Engineering	27
Wahlpflichtkatalog	29
Datenbanktheorie	30
Digital Forensics and Incident Response	32
Data Science Principles	34
Emerging Challenges in Cybersecurity Research	36
Future Computing	38
Funktionale Programmierung.....	41
Intelligente Systeme.....	43
Logische Programmierung	45
NOSQL Datenbanken	47
Privacy Enhancing Technologies	49
Weiterführende Konzepte zum Betrieb komplexer verteilter Systeme	52
Übersetzerbau	54

Modulkatalog

Ausgewählte Themen aus dem Bereich Internet und Sicherheit

<i>Kürzel:</i>	ATIS
<i>Untertitel:</i>	
<i>Studiensemester:</i>	3. (Master)
<i>Modulverantwortliche(r):</i>	Prof. Dr. Christian Dietrich
<i>Dozent(in):</i>	Prof. Dr. Christian Dietrich
<i>Sprache:</i>	Deutsch
<i>Zuordnung zum Curriculum:</i>	IN MI IS WI
	- - 3 -
<i>Lehrform / SWS:</i>	2 SWS Vorlesung, 2 SWS Praktikum
<i>Gruppengröße:</i>	Vorlesung: Nicht begrenzt, Praktikum: 20
<i>Arbeitsaufwand:</i>	Kontaktzeit: 60 Zeitstunden Selbststudium: 120 Zeitstunden
<i>Leistungspunkte:</i>	6
<i>Turnus:</i>	Wintersemester und Sommersemester, halbjährlich
<i>Teilnehmerzahl:</i>	Nicht begrenzt
<i>Anmeldungsmodalitäten:</i>	
<i>Voraussetzungen nach Prüfungsordnung:</i>	Keine
<i>Empfohlene Voraussetzungen (Modulprüfungen):</i>	Keine
<i>Angestrebte Lernergebnisse:</i>	<p>Die Studierenden beherrschen fortgeschrittene Konzepte der IT-Sicherheit, insb. System- und Softwaresicherheit, und können sie mit Internet-Technologien kombinieren. Sie gewinnen praktische Erfahrungen über sichere und unsichere IT-Infrastrukturen und Programme. In Teamarbeit soll ein komplexes Problem nach wissenschaftlicher Betrachtung praktisch gelöst werden. Die Teilnehmenden sind in der Lage, ihre Ergebnisse gemessen am Stand der Wissenschaft und Technik einzuordnen und sowohl unter Verwendung von Fachtermini untereinander als auch gegenüber der Hochschulöffentlichkeit darzustellen und zu kommunizieren.</p> <p>Wenn möglich werden über die Teilnahme an kompetitiven, spielerischen Wettbewerben (etwa Capture The Flag) die erworbenen Kompetenzen unter Beweis gestellt.</p>
<i>Inhalt:</i>	Aktuelle praktische oder wissenschaftliche Probleme basierend auf etwa Konferenzbeiträgen zu Top-Tier-Konferenzen und Journals oder durch aktuelle CTF-

	Wettbewerbe • IT-Sicherheit • System- und Softwaresicherheit • Internet- und Netzwerktechnologien und Angriffsmethoden
<i>Studien- / Prüfungsleistungen:</i>	Studienleistungen laut Prüfungsordnung als Voraussetzung zur Prüfungsteilnahme: Keine Prüfungsleistungen: schriftliche Ausarbeitung, Klausur und/oder mündliche Prüfung
<i>Literatur:</i>	Literatur an das aktuelle Thema angepasst <ul style="list-style-type: none">• Diverse aktuelle Konferenz-Publikationen
<i>Bemerkungen:</i>	—

Datenschutz und Ethik

<i>Kürzel:</i>	DSE			
<i>Untertitel:</i>				
<i>Studiensemester:</i>	2. (Master)			
<i>Modulverantwortliche(r):</i>	Prof. Dr. (TU NN) Norbert Pohlmann			
<i>Dozent(in):</i>	Prof. Dr. Alexander Koch (Lehrbeauftragte/r)			
<i>Sprache:</i>	Deutsch			
<i>Zuordnung zum Curriculum:</i>	IN	MI	IS	WI
	-	WP	2	WP
<i>Lehrform / SWS:</i>	2 SWS Vorlesung, 2 SWS Übung (Seminar)			
<i>Gruppengröße:</i>	Vorlesung: Nicht begrenzt, Übung: 40			
<i>Arbeitsaufwand:</i>	Kontaktzeit: 56 Zeitstunden Selbststudium: 124 Zeitstunden			
<i>Leistungspunkte:</i>	6			
<i>Turnus:</i>	Sommersemester, jährlich			
<i>Teilnehmerzahl:</i>	Nicht begrenzt			
<i>Anmeldungsmodalitäten:</i>	Siehe Aushang			
<i>Voraussetzungen nach Prüfungsordnung:</i>	Regelmäßige Anwesenheit bei Präsentationen der Teilnehmerinnen und Teilnehmer			
<i>Empfohlene Voraussetzungen (Modulprüfungen):</i>	Keine			
<i>Angestrebte Lernergebnisse:</i>	<p>Die Studierenden besitzen grundlegende Kenntnisse über Datenschutz und Ethik.</p> <p>Sie haben ein gutes Verständnis über die fundamentalen Gesetze, Verordnungen und Strategien im Datenschutz.</p> <p>Sie erlernen den Sinn und Zweck einer Ethik in der vernetzten Informations- und Wissensgesellschaft.</p>			

<i>Inhalt:</i>	<ul style="list-style-type: none">• Einführung in Datenschutz und Ethik.• Begriffsbestimmungen: personenbezogene Daten, Datenregister, ...• Informationelle Selbstbestimmung, Bundesdatenschutzgesetz, Teledienstedatenschutz, Telekommunikationsgesetz, DSGVO, ...• Rechte der Betroffenen.• Organisatorische und technische Maßnahmen zum Schutz personenbezogene Daten.• Ethik in der vernetzten Informations- und Wissensgesellschaft.
<i>Studien- / Prüfungsleistungen:</i>	Anwesenheitspflicht nach Prüfungsordnung Prüfungsleistung: Ausarbeitung der geforderten Projektergebnisse und Präsentationen
<i>Literatur:</i>	Nach Bekanntgabe in der Veranstaltung Themen werden an Hand von aktueller Primärliteratur behandelt.
<i>Bemerkungen:</i>	-

Internet-Sicherheit A

Kürzel:	ISA
Untertitel:	Konzepte, Architekturen, Prinzipien und Funktionsweisen von IT-Sicherheitskomponenten und – Systemen in Internet-Sicherheitsinfrastrukturen
Studiensemester:	1. (Master)
Modulverantwortliche(r):	Prof. Dr. (TU NN) Norbert Pohlmann
Dozent(in):	Prof. Dr. (TU NN) Norbert Pohlmann
Sprache:	Deutsch
Zuordnung zum Curriculum:	IN MI IS WI
	- WP 1 1
Lehrform / SWS:	2 SWS Vorlesung, 1 SWS Übung, 1 SWS Praktikum
Gruppengröße:	Vorlesung: Nicht begrenzt, Übung: 40, Praktikum: 20
Arbeitsaufwand:	Kontaktzeit: 60 Zeitstunden Selbststudium: 120 Zeitstunden
Leistungspunkte:	6
Turnus:	Wintersemester, jährlich
Teilnehmerzahl:	Nicht begrenzt
Anmeldungsmodalitäten:	Anmeldung über den Moodle-Kurs zu diesem Modul
Voraussetzungen nach Prüfungsordnung:	Keine modulspezifischen Voraussetzungen
Empfohlene Voraussetzungen (Modulprüfungen):	Keine
Angestrebte Lernergebnisse:	<ul style="list-style-type: none"> • Gutes Verständnis von möglichen Angriffen und geeigneten Gegenmaßnahmen im Bereich der Internet-Infrastruktur • Erlangen von Kenntnissen über den Aufbau, die Prinzipien, die Architektur und die Funktionsweise von Sicherheitskomponenten und -systemen im Bereich Frühwarn- und Infrastruktur-Sicherheitssystemen • Sammeln von Erfahrungen bei der Ausarbeitung und Präsentation von neuen Themen aus dem Bereich Internet-Sicherheit • Gewinnen von praktischen Erfahrungen über die Nutzung und die Wirkung von Sicherheitssystemen im Bereich der Internet-Infrastruktur • Erleben der Notwendigkeit und Wichtigkeit der Internet-Sicherheit

<i>Inhalt:</i>	<ul style="list-style-type: none">• Cyber-Sicherheit Frühwarn- und Lagebildsysteme• Firewall-Systeme: Definition, Elemente, Konzepte, praktischer Einsatz, die Wirkung und die Möglichkeiten und Grenzen von Firewall-Systemen• IPSec-Verschlüsselung - VPN-Systeme: Ziele, Anwendungsformen, Konzepte, Mechanismen und Protokolle von VPNs und Anwendungsbeispiele• Transport Layer Security (TLS): Idee, Mechanismen, Protokolle und Umsetzungskonzepte• Cyber-Sicherheitsmaßnahmen-gegen-DDoS-Angriffe• Wirtschaftlichkeit von Cyber-Sicherheitsmaßnahmen• Social-Web-Cyber-Sicherheit• Vertrauen und Vertrauenswürdigkeit
<i>Studien- / Prüfungsleistungen:</i>	Studienleistungen: Erfolgreich absolviertes Praktikum als Vorleistung für die Prüfungszulassung Prüfungsleistungen: Klausur (90 Min.)
<i>Literatur:</i>	<ul style="list-style-type: none">• N. Pohlmann: „Cyber-Sicherheit - Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“ 2. Auflage, Springer Vieweg Verlag, Wiesbaden 2022• Pohlmann, N.: Firewall-Systeme - Sicherheit für Internet und Intranet, E- Mail-Security, Virtual Private Network, Intrusion Detection-System, Personal Firewalls. 5. aktualisierte und erweiterte Auflage; ISBN 3- 8266-0988-3; MITP-Verlag, Bonn 2003• A Campo, M.; Pohlmann, N.: Virtual Private Network (VPN). 2. aktualisierte und erweiterte Auflage, ISBN 3-8266-0882-8; MITP-Verlag, Bonn 2003• D. Petersen, N. Pohlmann: „An ideal Internet Early Warning System“. In “Advances in IT Early Warning”, Fraunhofer Verlag, München 2013
<i>Bemerkungen:</i>	-

Internet-Sicherheit B

<i>Kürzel:</i>	ISB
<i>Untertitel:</i>	Konzepte, Architekturen, Prinzipien und Funktionsweisen von IT-Sicherheitskomponenten und -Systemen in Endgeräte und Anwendungen
<i>Studiensemester:</i>	2. (Master)
<i>Modulverantwortliche(r):</i>	Prof. Dr. (TU NN) Norbert Pohlmann
<i>Dozent(in):</i>	Prof. Dr. (TU NN) Norbert Pohlmann
<i>Sprache:</i>	Deutsch
<i>Zuordnung zum Curriculum:</i>	IN MI IS WI - WP 2 WP
<i>Lehrform / SWS:</i>	2 SWS Vorlesung, 1 SWS Übung, 1 SWS Praktikum
<i>Gruppengröße:</i>	Vorlesung: Nicht begrenzt, Übung: 40, Praktikum: 20
<i>Arbeitsaufwand:</i>	Kontaktzeit: 56 Zeitstunden Selbststudium: 124 Zeitstunden
<i>Leistungspunkte:</i>	6
<i>Turnus:</i>	Sommersemester, jährlich
<i>Teilnehmerzahl:</i>	Nicht begrenzt
<i>Anmeldungsmodalitäten:</i>	Anmeldung über den Moodle-Kurs zu diesem Modul
<i>Voraussetzungen nach Prüfungsordnung:</i>	Keine modulspezifischen Voraussetzungen
<i>Empfohlene Voraussetzungen (Modulprüfungen):</i>	Keine
<i>Angestrebte Lernergebnisse:</i>	<ul style="list-style-type: none"> • Gutes Verständnis von möglichen Angriffen und geeigneten Gegenmaßnahmen im Bereich der Endgeräte und Anwendungen • Erlangen von Kenntnissen über den Aufbau, die Prinzipien, die Architektur und die Funktionsweise von Sicherheitskomponenten und -systemen im Bereich Trusted Computing und PKI- und Blockchain-orientierten Sicherheitssystemen • Sammeln von Erfahrungen bei der Ausarbeitung und Präsentation von neuen Themen aus dem Bereich Internet-Sicherheit • Gewinnen von praktischen Erfahrungen über die Nutzung und die Wirkung von Sicherheitssystemen im Bereich Trusted Computing und PKI- und Blockchain-orientierten Sicherheitssystemen • Erleben der Notwendigkeit und Wichtigkeit der Internet-Sicherheit

Inhalt:

- Digitale Signatur: Gesetzliche Grundlagen, Mechanismen und Prinzipien, Anwendungsbeispiele
- Public-Key-Infrastruktur (PKI): Aufgaben, Komponenten, gesetzlicher Hintergrund, Modelle, Umsetzungskonzepte und praktische Beispiele
- Blockchain-Technologie: Aufgaben, Komponenten und Eigenschaften, Umsetzungskonzepte und praktische Beispiele
- Künstliche Intelligenz für Cyber-Sicherheit: Einordnung und Definitionen, Maschinelles Lernen, Künstliche Neuronale Netze, Anwendungen KI und Cyber-Sicherheit, Angriffe auf maschinelles Lernen und Herausforderungen
- Trusted Computing
 - TPM (Aufbau und Funktionen)
 - TC Funktionen (Trusted Boot, Binding, Sealing, and(Remote) Attestation),
 - Trusted Computing Base
 - Sicherheitsplattform (Idee, Ziele, Methoden, ...)
 - Anwendungsbeispiele
- Trusted Network Connect (TNC)
 - grundsätzliche Idee
 - TNC Architektur
 - T-NAC (Idee, Ziele, Methoden, ...)
- E-Mail-Security: Elemente, Konzepte und praktischer Einsatz
- Anti-Spam-System: Schäden, Quellen; Anti-Spam-Technologien, Kopfzeilenanalyse, Textanalyse, Blacklist, Distributed Checksum Clearinghouse (DCC), Distributed IP Reputation System, usw.
- Botnetze: Malware, Infektionsvektoren, Botnetzen, Schadfunktionen durch Bots und Gegenmaßnahmen

Studien- / Prüfungsleistungen:

Studienleistungen: Erfolgreich absolviertes Praktikum als Vorleistung für die Prüfungszulassung
 Prüfungsleistungen: Klausur (90 Min.)

Literatur:

- N. Pohlmann: „Cyber-Sicherheit - Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“ 2. Auflage, Springer Vieweg Verlag, Wiesbaden 2022
- H. Blumberg, N. Pohlmann: "Der IT-Sicherheitsleitfaden“, 2. aktualisierte und erweiterte

Auflage, ISBN-10: 3-8266-1635-9; 523 Seiten, MITP-Verlag, Bonn 2006

- Pohlmann, N.; Reimer, H.: "Trusted Computing - Ein Weg zu neuen IT- Sicherheitsarchitekturen", ISBN 978-3-8348-0309-2, Vieweg-Verlag, Wiesbaden 2008
- M. Jungbauer, N. Pohlmann: „Integrity Check of Remote Computer Systems - Trusted Network Connect". In Proceedings of the ISSE/SECURE 2007 - Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe/Secure 2007 Conference, Eds.: N. Pohlmann, H. Reimer, W. Schneider; Vieweg Verlag, Wiesbaden 2007

Bemerkungen:

-

Kolloquium zur Masterarbeit Internet-Sicherheit

<i>Kürzel:</i>	KMIS			
<i>Untertitel:</i>	Abschlussprüfung im Master-Studium Internet-Sicherheit			
<i>Studiensemester:</i>	4. (Master)			
<i>Modulverantwortliche(r):</i>	Prof. Dr. (TU NN) Norbert Pohlmann			
<i>Dozent(in):</i>	Alle Professoren des Master-Studiengangs Internet-Sicherheit			
<i>Sprache:</i>	Deutsch			
<i>Zuordnung zum Curriculum:</i>	IN	MI	IS	WI
	-	-	4	-
<i>Lehrform / SWS:</i>	Kolloquium zur Masterarbeit			
<i>Gruppengröße:</i>	Im Regelfall Gruppengröße 1, größere Gruppen möglich (§ 22 MRPO)			
<i>Arbeitsaufwand:</i>	150 Zeitstunden			
<i>Leistungspunkte:</i>	5			
<i>Turnus:</i>	Das Kolloquium zur Masterarbeit ist jederzeit möglich			
<i>Teilnehmerzahl:</i>	Wie Gruppengröße			
<i>Anmeldungsmodalitäten:</i>	Siehe § 16 PO und § 26 MRPO			
<i>Voraussetzungen nach Prüfungsordnung:</i>	Siehe § 16 PO und § 26 MRPO			
<i>Empfohlene Voraussetzungen (Modulprüfungen):</i>	Keine			
<i>Angestrebte Lernergebnisse:</i>	<p>Die/der Studierende ist in der Lage, die Ergebnisse ihrer/seiner Masterarbeit aus der Internet-Sicherheit, ihre fachlichen Grundlagen, ihre Einordnung in den aktuellen Stand der Technik, bzw. der Forschung, ihre fächerübergreifenden Zusammenhänge und ihre außerfachliche Bezüge in begrenzter Zeit in einem Vortrag zu präsentieren.</p> <p>Darüber hinaus kann sie/er Fragen zu inhaltlichen Details, zu fachlichen Begründungen und Methoden sowie zu inhaltlichen Zusammenhängen zwischen Teilbereichen ihrer/seiner Arbeit beantworten. Die/der Studierende kann ihre/seine Masterarbeit auch im Kontext beurteilen und ihre Bedeutung für die Praxis und die Forschung einschätzen und ist in der Lage, auch entsprechende Fragen nach themen- und fachübergreifenden Zusammenhängen zu beantworten.</p>			
<i>Inhalt:</i>	Zunächst wird der Inhalt der Masterarbeit aus der Internet-Sicherheit im Rahmen eines Vortrages präsentiert. Anschließend sollen in einer Diskussion			

Fragen zum Vortrag und zur Masterarbeit beantwortet werden.

Die Prüfer können weitere Zuhörer zulassen. Diese Zulassung kann sich nur auf den Vortrag, auf den Vortrag und einen Teil der Diskussion oder auf das gesamte Kolloquium zur Masterarbeit erstrecken.

Der Vortrag soll die Problemstellung der Masterarbeit, die vergleichende Darstellung alternativer oder konkurrierender Lösungsansätze mit Bezug zum aktuellen Stand der Technik, bzw. Forschung, den gewählten Lösungsansatz, die erzielten Ergebnisse zusammen mit einer abschließenden Bewertung der Arbeit sowie einen Ausblick beinhalten. Je nach Thema können weitere Anforderungen hinzukommen. Die Dauer des Vortrages wird vom Erstprüfer festgelegt und kann zwischen 30 und 40 Minuten betragen.

In der anschließenden Diskussion werden Fragen von den Prüfern gestellt. Fragen der übrigen Zuhörer des Kolloquiums können durch die Prüfer ebenfalls zugelassen werden. Die Dauer der Diskussion wird durch die Prüfer bestimmt und beträgt ca. 30-45 Minuten.

Studien- / Prüfungsleistungen:	Benotung des Vortrages und der anschließenden Diskussion und Fragen durch die Prüfer laut Prüfungsordnung
---------------------------------------	---

<i>Literatur:</i>	<ul style="list-style-type: none">• Kuzbari, R.; Ammer, R.: Der wissenschaftliche Vortrag. Springer-Verlag Wien New York, 2006. ISBN-10 3-211-23525-6• Leopold-Wildburger, U.; Schütze, J.: Verfassen und Vortragen - Wissenschaftliche Arbeiten und Vorträge leicht gemacht. Springer-Verlag Berlin Heidelberg New York, 2002. ISBN 3-540-43027-X
-------------------	---

<i>Bemerkungen:</i>	Keine
---------------------	-------

Masterarbeit Internet-Sicherheit

<i>Kürzel:</i>	MAIS
<i>Untertitel:</i>	Abschlussarbeit des Master-Studiums Internet-Sicherheit
<i>Studiensemester:</i>	4. (Master)
<i>Modulverantwortliche(r):</i>	Prof. Dr. (TU NN) Norbert Pohlmann
<i>Dozent(in):</i>	Alle Professoren des Master-Studiengangs Internet-Sicherheit
<i>Sprache:</i>	Deutsch
<i>Zuordnung zum Curriculum:</i>	IN MI IS WI
	- - 4 -
<i>Lehrform / SWS:</i>	Masterarbeit
<i>Gruppengröße:</i>	Im Regelfall Gruppengröße 1, größere Gruppen möglich (§ 22 MRPO)
<i>Arbeitsaufwand:</i>	750 Zeitstunden
<i>Leistungspunkte:</i>	25
<i>Turnus:</i>	Die Vergabe einer Masterarbeit ist jederzeit möglich.
<i>Teilnehmerzahl:</i>	Wie Gruppengröße
<i>Anmeldungsmodalitäten:</i>	Siehe § 13 und § 14 PO und § 23 MRPO
<i>Voraussetzungen nach Prüfungsordnung:</i>	Siehe § 13 PO und § 23 MRPO
<i>Empfohlene Voraussetzungen (Modulprüfungen):</i>	Keine
<i>Angestrebte Lernergebnisse:</i>	<p>Die/der Studierende ist in der Lage, innerhalb einer vorgegebenen Frist entweder</p> <ul style="list-style-type: none"> • eine schwierige und komplexe praxisorientierte Problemstellung aus der Internet-Sicherheit sowohl in ihren fachlichen Einzelheiten als auch in den themen- und fachübergreifenden Zusammenhängen nach wissenschaftlichen Methoden selbstständig zu bearbeiten und zu lösen <p>oder</p> <ul style="list-style-type: none"> • eine anspruchsvolle Fragestellung aus der aktuellen Forschung auf dem Gebiet der Internet-Sicherheit unter Anleitung eigenständig zu bearbeiten und selbstständig ein neues wissenschaftliches Ergebnis zu entwickeln.
<i>Inhalt:</i>	Es soll eine praxisorientierte Problemstellung oder eine Fragestellung aus der Forschung auf dem Gebiet der Internet-Sicherheit mit den im Studium erworbenen oder während der Masterarbeit neu erlernten

wissenschaftlichen Methoden in begrenzter Zeit mit Unterstützung eines erfahrenen Betreuers gelöst werden.

Studien- / Prüfungsleistungen: In der Prüfungsordnung geregelt

Literatur:

- Franck, N.; Stary, J.: Die Technik wissenschaftlichen Arbeitens. UTB-Verlag Stuttgart 2009 (15. Auflage). ISBN-10: 3825207242
- Ebel, H.; Bliefert, C.: Bachelor-. Master- und Doktorarbeit – Anleitungen für den naturwissenschaftlichtechnischen Nachwuchs. Verlag Wiley 2009 (4. Auflage). ISBN-10: 3527324771
- Gockel, T.: Form der wissenschaftlichen Ausarbeitung. Springer-Verlag Berlin 2008. ISBN-10: 3540786139
- Themenspezifische Literatur

Bemerkungen: —

Malware-Analyse und Cyber Threat Intelligence

<i>Kürzel:</i>	MCTI
<i>Untertitel:</i>	
<i>Studiensemester:</i>	2. (Master)
<i>Modulverantwortliche(r):</i>	Prof. Dr. Christian Dietrich
<i>Dozent(in):</i>	Prof. Dr. Christian Dietrich
<i>Sprache:</i>	Deutsch
<i>Zuordnung zum Curriculum:</i>	IN MI IS WI
	- WP 2 -
<i>Lehrform / SWS:</i>	2 SWS Vorlesung, 2 SWS Praktikum
<i>Gruppengröße:</i>	Vorlesung: Nicht begrenzt, Übung: 40, Praktikum: 20
<i>Arbeitsaufwand:</i>	Kontaktzeit: 56 Zeitstunden Selbststudium: 124 Zeitstunden
<i>Leistungspunkte:</i>	6
<i>Turnus:</i>	Sommersemester, jährlich
<i>Teilnehmerzahl:</i>	Nicht begrenzt
<i>Anmeldungsmodalitäten:</i>	
<i>Voraussetzungen nach Prüfungsordnung:</i>	Keine
<i>Empfohlene Voraussetzungen (Modulprüfungen):</i>	Programmierkenntnisse, Software Reverse Engineering
<i>Angestrebte Lernergebnisse:</i>	Die Studierenden vertiefen die Konzepte zur Analyse von Schadsoftware (Malware) und zur Erkennung von Angriffswerkzeugen. Anhand realer Cyber-Angriffe wenden sie aktuelle Methoden zur technischen Analyse der Artefakte wie Schadsoftware-Samples oder Netzwerkmitschnitten an. Sie erkennen auf diese Weise die Limitierungen aktueller Methoden und entwickeln eigene Forschungsfragen. Darüber hinaus eignen sie sich selbst neues Wissen über das Studium bestehender Berichte zu vergangenen Vorfällen an und lernen Bewertungskriterien zur Einschätzung der Berichte zu entwickeln und anzuwenden sowie kritisch zu hinterfragen. Methode zur Attribution von Akteuren hinter Cyber-Angriffen müssen angewendet werden und eine geopolitische Einordnung wird betrachtet. Im Rahmen der Veranstaltung wird abschließend anhand eines realen Cyber-Angriffs die Analyse und die Kommunikation der Analyse-Ergebnisse in Form eines

	Threat Intelligence Berichts sowie einer dazugehörigen Präsentation vertieft.
<i>Inhalt:</i>	Malware-Analyse • Malware-Erkennung und -Klassifikation • Signaturen • Exploit-Dokumente • Shellcode • Unpacking und Speicherabzüge • Anti-Analyse-Verfahren von Malware • Cyber kill chain • Cyber Threat Intelligence • Analysis of Competing Hypothesis • Angriffsvektoren • Netzwerkkommunikation • Attribution • Threat Actor
<i>Studien- / Prüfungsleistungen:</i>	Studienleistungen laut Prüfungsordnung als Voraussetzung zur Prüfungsteilnahme: Keine Prüfungsleistungen: schriftliche Ausarbeitung und Präsentation
<i>Literatur:</i>	<ul style="list-style-type: none">• Timo Steffens: Auf der Spur der Hacker - Wie man die Täter hinter der Computer-Spionage enttarnt• Michael Sikorski and Andrew Honig: Practical Malware Analysis• Russinovich, M./Solomon, D./Ionescu, A.: <i>Windows Internals</i>, Part 1 & 2; Microsoft Press, 6. Edition• Diverse aktuelle Konferenz-Publikationen
<i>Bemerkungen:</i>	—

Master-Projekt Internet-Sicherheit

<i>Kürzel:</i>	MPIS
<i>Untertitel:</i>	Master-Projekt Internet-Sicherheit
<i>Studiensemester:</i>	1. und 2. (Master)
<i>Modulverantwortliche(r):</i>	Prof. Dr. (TU NN) Norbert Pohlmann
<i>Dozent(in):</i>	Alle Professoren des Master-Studiengangs Internet-Sicherheit
<i>Sprache:</i>	Deutsch
<i>Zuordnung zum Curriculum:</i>	IN MI IS WI - - 1+2 -
<i>Lehrform / SWS:</i>	1 SWS Praktikum (Projekt)
<i>Gruppengröße:</i>	Standard, i.d.R. Projektteams von 6 bis 8 Studierenden
<i>Arbeitsaufwand:</i>	Kontaktzeit: 56 Zeitstunden Selbststudium: 304 Zeitstunden
<i>Leistungspunkte:</i>	12
<i>Turnus:</i>	Wintersemester, jährlich
<i>Teilnehmerzahl:</i>	Nicht begrenzt
<i>Anmeldungsmodalitäten:</i>	Anmeldung über den Moodle-Kurs zu diesem Modul
<i>Voraussetzungen nach Prüfungsordnung:</i>	Regelmäßige Anwesenheit bei Projektbesprechungen
<i>Empfohlene Voraussetzungen (Modulprüfungen):</i>	Keine
<i>Angestrebte Lernergebnisse:</i>	Die Studierenden sind in der Lage, ihre bisher erworbenen speziellen Kenntnisse, Fertigkeiten und Lösungsstrategien aus der Informatik und der Internet-Sicherheit auf interdisziplinäre Problemstellungen anzuwenden.
<i>Inhalt:</i>	<ul style="list-style-type: none"> • Im Master-Projekt Internet-Sicherheit wird besonders die interdisziplinäre Komponente des Masterstudiengangs Internet-Sicherheit in den Mittelpunkt gerückt. • Während der Projektarbeit sollen die Studierenden vor allem ihre speziellen Kenntnisse, Fertigkeiten

und Lösungsstrategien aus der Informatik auf interdisziplinäre Problemstellungen anwenden.

- Interdisziplinäre Projekte können mit den anderen Master-Studiengängen koordiniert werden. Beispiele sind:
 - Wirtschaftsinformatik (Return of Security Investment (RoSI), Mehrwerte von Internet-Sicherheit, ...) oder
 - Technische Informatik (Sicherheit bei „Internet der Dinge“, Industrie 4.0, ...) oder
 - Medieninformatik (Vertrauenswürdige Gestaltung von Oberflächen, Darstellung von sicherheitsrelevanten Ereignissen auf eine intuitive Weise, ...) oder
 - Praktische Informatik (Integration von IT-Sicherheit in Anwendungen, ...).
- Die Projektteams haben dabei die Verantwortung für die genaue Ausgestaltung und das Zeitmanagement.

Studien- / Prüfungsleistungen: Prüfungsleistung: Ausarbeitung der geforderten Projektergebnisse und Präsentationen

Literatur: Projektspezifisch, wird zu Veranstaltungsbeginn bekannt gegeben

Bemerkungen: Das Master-Projekt wird über zwei Semester durchgeführt.

Master-Seminar Internet-Sicherheit

<i>Kürzel:</i>	MSIS
<i>Untertitel:</i>	Fachseminar zu aktuellen Themen der Internet-Sicherheit
<i>Studiensemester:</i>	3. (Master)
<i>Modulverantwortliche(r):</i>	Prof. Dr. (TU NN) Norbert Pohlmann
<i>Dozent(in):</i>	Alle Professoren des Master-Studiengangs Internet-Sicherheit
<i>Sprache:</i>	Deutsch
<i>Zuordnung zum Curriculum:</i>	IN MI IS WI
	- - 3 -
<i>Lehrform / SWS:</i>	2 SWS Übung (Seminar)
<i>Gruppengröße:</i>	Standard, i.d.R. Projektteams von 3 bis 6 Studierenden
<i>Arbeitsaufwand:</i>	Kontaktzeit: 30 Zeitstunden Selbststudium: 150 Zeitstunden
<i>Leistungspunkte:</i>	6
<i>Turnus:</i>	Zu jedem Semester
<i>Teilnehmerzahl:</i>	Nicht begrenzt
<i>Anmeldungsmodalitäten:</i>	Anmeldung über den Moodle-Kurs zu diesem Modul
<i>Voraussetzungen nach Prüfungsordnung:</i>	Regelmäßige Anwesenheit
<i>Empfohlene Voraussetzungen (Modulprüfungen):</i>	Keine
<i>Angestrebte Lernergebnisse:</i>	<p>Die Studierenden besitzen die folgenden Fähigkeiten:</p> <ul style="list-style-type: none"> • Sie sind in der Lage zur selbstständigen Einarbeitung in aktuelle Forschungsfragen zur Internet-Sicherheit auf der Basis von Primärliteratur (Publikationen in Fachzeitschriften sowie Tagungsbeiträgen); • Sie können Informationsrecherchen zu forschungsorientierten Fragestellungen durchführen und sind in der Lage, dazu eine strukturiert schriftliche Aufbereitung des aktuellen Stands der Forschung zu erarbeiten; • Sie können eine zusammengefasste Darstellung der Ergebnisse zu einer Fragestellung präsentieren sowie in der Diskussion mit allen Seminar teilnehmern sich ergebende Fragen beantworten und aufgestellte Thesen verteidigen.
<i>Inhalt:</i>	<ul style="list-style-type: none"> • Im Rahmen dieses Projekts bearbeiten die Studierenden aktuelle Themen aus dem Bereich der

Internet-Sicherheit. Die Themen orientieren sich z.B. an den Forschungsthemen des Instituts für Internet-Sicherheit -if(is).

Die Rahmenbedingungen für das Projekt werden von den Lehrenden vorgegeben, die Ausgestaltung und die Verantwortung liegen aber bei den einzelnen Projektteams des Institutes.

- Dadurch sollen die Studierenden das selbstständige und zielorientierte Bearbeiten von wissenschaftlichen Problemstellungen über einen längeren Zeitraum erlernen.
- Ein Schwerpunkt dieses Seminars bildet die eigenständige Bearbeitung wissenschaftlicher Fragestellungen.

Studien- / Prüfungsleistungen: Prüfungsleistung: Ausarbeitung der geforderten Projektergebnisse und Präsentationen

Literatur: Projektspezifisch, wird zu Veranstaltungsbeginn bekannt gegeben

Bemerkungen: —

Wissenschaftliche Vertiefung Internet-Sicherheit

Kürzel:	MVIS
Untertitel:	Wissenschaftliche Vertiefung Internet-Sicherheit
Studiensemester:	3. (Master)
Modulverantwortliche(r):	Prof. Dr. (TU NN) Norbert Pohlmann
Dozent(in):	Alle Professoren des Master-Studiengangs Internet-Sicherheit
Sprache:	Deutsch
Zuordnung zum Curriculum:	IN MI IS WI
	- - 3 -
Lehrform / SWS:	2 SWS Seminar
Gruppengröße:	Standard, i.d.R. Projektteams von 3 bis 6 Studierenden
Arbeitsaufwand:	Kontaktzeit: 30 Zeitstunden Selbststudium: 330 Zeitstunden
Leistungspunkte:	12
Turnus:	Wintersemester, jährlich
Teilnehmerzahl:	Nicht begrenzt
Anmeldungsmodalitäten:	Anmeldung über den Moodle-Kurs zu diesem Modul
Voraussetzungen nach Prüfungsordnung:	Keine modulspezifischen Voraussetzungen
Empfohlene Voraussetzungen (Modulprüfungen):	Keine
Angestrebte Lernergebnisse:	Die Studierenden sind in der Lage, wissenschaftlich anspruchsvolle Problemstellungen selbstständig und zielorientiert zu bearbeiten.
Inhalt:	<ul style="list-style-type: none"> • Im Rahmen dieses Projekts bearbeiten die Studierenden aktuelle Themen aus dem Bereich der Internet-Sicherheit. Die Themen orientieren sich z.B. an den Forschungsthemen des Instituts für Internet-Sicherheit -if(is). • Die Rahmenbedingungen für das Projekt werden von den Lehrenden vorgegeben, die Ausgestaltung und die Verantwortung liegen aber bei den einzelnen Projektteams des Institutes. • Dadurch sollen die Studierenden das selbstständige und zielorientierte Bearbeiten von wissenschaftlichen Problemstellungen über einen längeren Zeitraum erlernen. • Ein Schwerpunkt dieses Seminars bildet die eigenständige Bearbeitung wissenschaftlicher

	Fragestellungen. Idealerweise entsteht daraus ein Artikel, die veröffentlicht werden kann.
<i>Studien- / Prüfungsleistungen:</i>	In der Prüfungsordnung geregelt
<i>Literatur:</i>	Projektspezifisch, wird zu Veranstaltungsbeginn bekannt gegeben
<i>Bemerkungen:</i>	Keine

Programmiermethodik und Sicherheit

<i>Kürzel:</i>	PRMS
<i>Untertitel:</i>	
<i>Studiensemester:</i>	1. (Master)
<i>Modulverantwortliche(r):</i>	Prof. Dr. Christian Dietrich
<i>Dozent(in):</i>	Prof. Dr. Christian Dietrich
<i>Sprache:</i>	Deutsch
<i>Zuordnung zum Curriculum:</i>	IN MI IS WI
	- - 1 -
<i>Lehrform / SWS:</i>	2 SWS Vorlesung, 2 SWS Praktikum
<i>Gruppengröße:</i>	Vorlesung: Nicht begrenzt, Praktikum: 20
<i>Arbeitsaufwand:</i>	Kontaktzeit: 60 Zeitstunden Selbststudium: 120 Zeitstunden
<i>Leistungspunkte:</i>	6
<i>Turnus:</i>	Wintersemester, jährlich
<i>Teilnehmerzahl:</i>	Nicht begrenzt
<i>Anmeldungsmodalitäten:</i>	
<i>Voraussetzungen nach Prüfungsordnung:</i>	Keine
<i>Empfohlene Voraussetzungen (Modulprüfungen):</i>	Kenntnisse in Software-Entwicklung auf Bachelor-Niveau
<i>Angestrebte Lernergebnisse:</i>	Die Studierenden beherrschen die grundlegenden Konzepte der Speichersicherheit (Memory Safety) und kennen Methoden und Techniken, um effizient zuverlässige Software hoher Qualität für sich schnell ändernde und wachsende Anforderungen zu erstellen. Dies gilt insbesondere für Anwendungen mit hohen Anforderungen an Sicherheit und Verlässlichkeit. Beispielhafte Umsetzungen erfolgen mit modernen Programmiersprachen, etwa Rust. Darüber hinaus wenden sie Techniken zum Aufbau von sicheren IT-Infrastrukturen an.
<i>Inhalt:</i>	Test-Driven Design • Memory Safety • Inversion of Control • Convention over Configuration • Programming by Contract • Nebenläufige Programmierung • Software-Schwachstellen durch Speicherschutzverletzungen • System-Schutzmechanismen • Type Safety • Speicherzugriffsfehler • Garbage Collection • Generische Programmierung • Fehlerbehandlung

Studien- / Prüfungsleistungen: Studienleistungen laut Prüfungsordnung als Voraussetzung zur Prüfungsteilnahme: Keine Prüfungsleistungen: Klausur (90 Min.) oder mündliche Prüfung

- Literatur:*
- The Rust Programming Language, Steve Klabnik and Carol Nichols, August 2019, <https://doc.rust-lang.org/book/>
 - Software Security: Principles, Policies, and Protection (SS3P), Mathias Payer, v0.37, <https://nebelwelt.net/SS3P/softsec.pdf>
 - Diverse aktuelle Konferenz-Publikationen
-

- Bemerkungen:* -
-

Software Reverse Engineering

<i>Kürzel:</i>	SRE
<i>Untertitel:</i>	
<i>Studiensemester:</i>	1. (Master)
<i>Modulverantwortliche(r):</i>	Prof. Dr. Christian Dietrich
<i>Dozent(in):</i>	Prof. Dr. Christian Dietrich
<i>Sprache:</i>	Deutsch
<i>Zuordnung zum Curriculum:</i>	IN MI IS WI
	- - 1 -
<i>Lehrform / SWS:</i>	2 SWS Vorlesung, 2 SWS Praktikum
<i>Gruppengröße:</i>	Vorlesung: Nicht begrenzt, Übung: 40, Praktikum: 20
<i>Arbeitsaufwand:</i>	Kontaktzeit: 60 Zeitstunden Selbststudium: 120 Zeitstunden
<i>Leistungspunkte:</i>	6
<i>Turnus:</i>	Wintersemester, jährlich
<i>Teilnehmerzahl:</i>	Nicht begrenzt
<i>Anmeldungsmodalitäten:</i>	Keine
<i>Voraussetzungen nach Prüfungsordnung:</i>	Keine
<i>Empfohlene Voraussetzungen (Modulprüfungen):</i>	Kenntnisse in Betriebssystemen und Programmierkenntnisse auf Bachelor-Niveau
<i>Angestrebte Lernergebnisse:</i>	Die Studierenden beherrschen die grundlegenden Konzepte des Software Reverse Engineering und können einige statische und dynamische Methoden zur Programmanalyse zur Lösung überschaubarer, praktischer Aufgaben sicher anwenden. Sie kennen gewisse Elemente von Maschinensprachen, insb. Intel x86, amd64 oder ARM, sowie zur Umsetzung gewisser Hochsprachen-Idiome in Maschinencode-Entsprechungen. Durch exemplarische Anwendung der Methoden werden praktische Erfahrungen zur Schadsoftware-Analyse gesammelt und ein grundlegendes Verständnis zur Vorgehensweise von Cyber-Angrifern erlangt. Darüber hinaus erfahren sie die Grenzen der Programmanalyse beispielsweise bei obfuscatedem Binärcode und können abstrakte Repräsentationen von Programmen, etwa in Kontrollflussgraphen, erstellen und zur Problemlösung nutzen. Gegebenenfalls werden die Kenntnisse im Rahmen eines Capture-The-Flag-Wettbewerbs angewendet und vertieft.

<i>Inhalt:</i>	Maschinensprache und Assemblersprache für die Intel x86-Architektur • Wiederholung wichtiger Betriebssystemaspekte am Beispiel von Windows oder Linux • Methoden zur statischen Code-Analyse • Disassembly • Erkennung von C-Hochsprachenkonzepten in Maschinencode • Kontrollflusskonstrukte und Kontrollflussgraphen • Dekompilation • Abbildung von C++-Hochsprachenkonzepten (Vererbung, Virtual Function Calls) in Maschinencode • Methoden zur dynamischen Code-Analyse • Debugging • Hooking • Binary Instrumentation • Emulation • Grundlagen der Schadsoftware-Analyse
<i>Studien- / Prüfungsleistungen:</i>	Studienleistungen laut Prüfungsordnung als Voraussetzung zur Prüfungsteilnahme: Keine Prüfungsleistungen: Klausur (90 Min.) oder mündliche Prüfung
<i>Literatur:</i>	<ul style="list-style-type: none">• Eilam, E.: <i>Reversing: Secrets of Reverse Engineering</i>; John Wiley & Sons, 1. Auflage• Dang, B./Gazet, A.: <i>Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation</i>; John Wiley & Sons, 1. Auflage• Russinovich, M./Solomon, D./Ionescu, A.: <i>Windows Internals, Part 1 & 2</i>; Microsoft Press, 6. Edition• Diverse aktuelle Konferenz-Publikationen
<i>Bemerkungen:</i>	-

Wahlpflichtkatalog

Datenbanktheorie

<i>Kürzel:</i>	DBT			
<i>Untertitel:</i>	-			
<i>Studiensemester:</i>	(Master)			
<i>Modulverantwortliche(r):</i>	Prof. Dr. Katja Zeume			
<i>Dozent(in):</i>	Prof. Dr. Katja Zeume			
<i>Sprache:</i>	Deutsch			
<i>Zuordnung zum Curriculum:</i>	IN WP	MI WP	IS WP	WI WP
<i>Lehrform / SWS:</i>	2 Vorlesung, 2 SWS Übung			
<i>Gruppengröße:</i>	Vorlesung: nicht begrenzt, Übung: 30			
<i>Arbeitsaufwand:</i>	Kontaktzeit: 56 Zeitstunden Selbststudium: 124 Zeitstunden			
<i>Leistungspunkte:</i>	6			
<i>Turnus:</i>	Sommersemester (nach Bedarf)			
<i>Teilnehmerzahl:</i>	Nicht begrenzt			
<i>Anmeldungsmodalitäten:</i>	Anmeldung über den Moodle-Kurs zu diesem Modul			
<i>Voraussetzungen nach Prüfungsordnung:</i>	Keine modulspezifischen Voraussetzungen			
<i>Empfohlene Voraussetzungen (Modulprüfungen):</i>	keine			
<i>Angestrebte Lernergebnisse:</i>	In der heutigen Zeit enthalten große IT-Landschaften oft komplexe Datenarchitekturen, die auf verschiedene Datenbankformate zurückgreifen und Daten effizient dazwischen integrieren. Die Studierenden lernen in der Veranstaltung die Grenzen von Datenbanken im Allgemeinen (hauptsächlich formatunabhängig) kennen.			
Dabei lernen sie die theoretische Analyse von Daten-basierten Problemen kennen. Die gewonnenen Kenntnisse werden auf praktische Probleme umgesetzt.				
<i>Inhalt:</i>	<ul style="list-style-type: none"> - Überblick über aktuelle Datenarchitekturen, aus Sicht der verwendeten Datenbanken (mit verschiedenen Formaten) und aus Sicht der Datenmodellierung bzw. Integration 			

-
- Formalisierung von Datenformaten und Anfragen (Kalkül vs. Algebra)
 - Ausdrucksstärke von Anfragesprachen für verschiedene Formate (z.Bsp. SQL, SPARQL, Key-Value)
 - Überblick und Einführung in die Auswertungskomplexität von Anfragen allgemein
 - (Wahlweise) Aktuelle verwandte Themen und deren Anwendung in der Praxis (z. Bsp. CAP Theorem, Ontologien, Knowledge Graphs)
-

Studien- / Prüfungsleistungen: Klausur oder mündliche Prüfung

Literatur: Leskovec, Rajaraman, Ullman. Mining of Massive Datasets

Foundations of Databases, Serge Abiteboul, Rick Hull, Victor Vianu, 1995.

Bemerkungen: -

Digital Forensics and Incident Response

<i>Kürzel:</i>	DFIR
<i>Untertitel:</i>	
<i>Studiensemester:</i>	(Master)
<i>Modulverantwortliche(r):</i>	Prof. Dr. Christian Dietrich
<i>Dozent(in):</i>	Prof. Dr. Christian Dietrich
<i>Sprache:</i>	Deutsch
<i>Zuordnung zum Curriculum:</i>	IN MI IS WI
	- - WP -
<i>Lehrform / SWS:</i>	2 SWS Vorlesung, 2 SWS Praktikum
<i>Gruppengröße:</i>	Vorlesung: Nicht begrenzt, Übung: 40, Praktikum: 20
<i>Arbeitsaufwand:</i>	Kontaktzeit: 56 Zeitstunden Selbststudium: 124 Zeitstunden
<i>Leistungspunkte:</i>	6
<i>Turnus:</i>	Sommersemester, jährlich
<i>Teilnehmerzahl:</i>	Nicht begrenzt
<i>Anmeldungsmodalitäten:</i>	
<i>Voraussetzungen nach Prüfungsordnung:</i>	Keine
<i>Empfohlene Voraussetzungen (Modulprüfungen):</i>	Programmierkenntnisse, Software Reverse Engineering
<i>Angestrebte Lernergebnisse:</i>	<p>Die Studierenden können die Terminologie forensischer Arbeit verstehen und anwenden. Sie sind in der Lage, die Qualität und Manipulierbarkeit digitalforensischer Spuren insb. auf Festspeicherdatenträgern einzuschätzen und kennen Anwendungen, mit Hilfe derer Spuren untersucht werden können. In einer Gruppe Studierender kommunizieren Studierende unter Verwendung von Fachtermini. Sie zeigen, dass sie digitalforensische Spuren aus Installationen des Betriebssystems Windows sachkundig erheben, analysieren, auswerten und dokumentieren können, um künftig bei der Aufklärung von Vorfällen mitwirken zu können. Moderne Entwicklungen zur Beobachtung von Systemen unter Verwendung von Virtualisierung können sie wiedergeben und erarbeiten Limitierungen bestehender Lösungen. Darüber hinaus verstehen sie architekturelle Gegebenheiten von Android-basierten Smartphones im Hinblick auf die digitalforensische Bedeutung.</p>

<i>Inhalt:</i>	Methodische Fundierung der digitalen Forensik und forensischen Informatik • Dokumentation von forensischen Untersuchungen • Analyse forensischer Berichte • digitalforensische Spuren in Windows-Installationen • Endpunktbasierter Erkennung und Reaktion (EDR) • Einbruchserkennung • Hypervisor • Smartphone-Forensik
<i>Studien- / Prüfungsleistungen:</i>	Studienleistungen laut Prüfungsordnung als Voraussetzung zur Prüfungsteilnahme: Keine Prüfungsleistungen: schriftliche Ausarbeitung
<i>Literatur:</i>	<ul style="list-style-type: none">• Andreas Dewald, Felix C. Freiling: Forensische Informatik. Books on demand, 2. Auflage 2015• Alexander Geschonneck: Computer Forensik, dpunkt Verlag, 2. Auflage, 2006• Diverse aktuelle Konferenz-Publikationen
<i>Bemerkungen:</i>	-

Data Science Principles

<i>Kürzel:</i>	DSC
<i>Untertitel:</i>	
<i>Studiensemester:</i>	1. (Master)
<i>Modulverantwortliche(r):</i>	Prof. Dr. Laura Anderle
<i>Dozent(in):</i>	Prof. Dr. Laura Anderle
<i>Sprache:</i>	deutsch oder englisch
<i>Zuordnung zum Curriculum:</i>	IN WP MI WP IS WP WI 1
<i>Lehrform / SWS:</i>	2 SWS Vorlesung, 2 SWS Übung
<i>Gruppengröße:</i>	Vorlesung: Nicht begrenzt, Übung: 40
<i>Arbeitsaufwand:</i>	Kontaktzeit: 60 Zeitstunden Selbststudium: 120 Zeitstunden
<i>Leistungspunkte:</i>	6
<i>Turnus:</i>	Wintersemester, jährlich
<i>Teilnehmerzahl:</i>	Nicht begrenzt
<i>Anmeldungsmodalitäten:</i>	Anmeldung über den Moodle-Kurs zu diesem Modul
<i>Voraussetzungen nach Prüfungsordnung:</i>	Keine modulspezifischen Voraussetzungen
<i>Empfohlene Voraussetzungen (Modulprüfungen):</i>	Kenntnisse auf Bachelor niveau zu Statistik und linearer Algebra
<i>Angestrebte Lernergebnisse:</i>	<ul style="list-style-type: none"> • Die Studierenden haben ein fundiertes Verständnis der theoretischen Hintergründe, Grenzen und Einsatzszenarien von datenwissenschaftlichen Verfahren und können diese Fachwissenschaftler*innen und Fachfremden erläutern. • Sie sind in der Lage, den Einsatz datenwissenschaftlicher Verfahren kritisch zu hinterfragen und gewissenhaft zu planen. • Dadurch sind sie in der Lage, datenwissenschaftliche Verfahren sinnvoll zur Problemlösung in verschiedenen Anwendungsszenarien einzubringen und einzusetzen.
<i>Inhalt:</i>	<p>Theoretische Grundlagen und Anwendung verschiedener</p> <ul style="list-style-type: none"> • Regressionsverfahren • Klassifikationsverfahren

-
- Clustering-Verfahren
 - Bootstrap- und Kreuzvalidierungsverfahren
 - Gütekriterien für die Ergebnisse datenwissenschaftlicher Verfahren
-

Studien- / Prüfungsleistungen: Klausur und/oder mündliche Prüfung und/oder schriftliche Ausarbeitung

Literatur:

- G. James, D. Witten, T. Hastie, R. Tibshirani: An Introduction to Statistical Learning with Applications in R, Springer (2021)
- J.M. Philipps: Mathematical Foundations for Data Analysis, Springer (2021)
- M. Plaue: Data Science: Grundlagen, Statistik und maschinelles Lernen, Springer (2021)
- Weitere Literatur wird in der Veranstaltung bekannt gegeben.

Bemerkungen: ---

Emerging Challenges in Cybersecurity Research

<i>Kürzel:</i>	ECCR			
<i>Untertitel:</i>	Emerging Challenges in Cybersecurity Research			
<i>Studiensemester:</i>	2. (Master)			
<i>Modulverantwortliche(r):</i>	Prof. Dr. Tobias Urban			
<i>Dozent(in):</i>	Prof. Dr. Tobias Urban			
<i>Sprache:</i>	Deutsch oder Englisch			
<i>Zuordnung zum Curriculum:</i>	IN WP	MI -	IS WP	WI -
<i>Lehrform / SWS:</i>	2 SWS Vorlesung 2 SWS Praktikum			
<i>Gruppengröße:</i>	Vorlesung: Nicht begrenzt Praktikum: 20			
<i>Arbeitsaufwand:</i>	Kontaktzeit: 56 Zeitstunden Selbststudium: 124 Zeitstunden			
<i>Leistungspunkte:</i>	6			
<i>Turnus:</i>	Sommersemester, jährlich			
<i>Teilnehmerzahl:</i>	Nicht begrenzt			
<i>Anmeldungsmodalitäten:</i>	Anmeldung über den Moodle-Kurs zu diesem Modul			
<i>Voraussetzungen nach Prüfungsordnung:</i>	Keine modulspezifischen Voraussetzungen			
<i>Empfohlene Voraussetzungen (Modulprüfungen):</i>	Keine			
<i>Angestrebte Lernergebnisse:</i>	<p>Die Studierenden arbeiten sich in aktuelle und zukunftsweisende Forschungsthemen im Bereich der IT-Sicherheit und des Datenschutzes ein. Dazu wird in jedem Semester ein anderes Schwerpunktthema, in welches sich die Studierenden einarbeiten, den aktuellen Stand der Technik verstehen und den Stand der Forschung sukzessive erarbeiten. Dabei sollen die Studierenden über Kenntnisse, ein Verständnis und Wissen in den folgenden Themenkomplexen.</p> <ul style="list-style-type: none"> • Eigenständige Erarbeitung von vertieften Kenntnissen über aktuelle Forschungsthemen in der IT-Sicherheit und des Datenschutzes (Basierend auf Primärliteratur). • Kritische Auseinandersetzung mit dem aktuellen wissenschaftlichen Diskurs bzw. neuen Erkenntnissen in dem gewählten Themenkomplex • Identifikation von komplexen Sicherheitsproblemen und Entwicklung von innovativen Lösungen bzw. Methodiken. 			

-
- Präzise Präsentation und Kommunikation von Forschungsergebnissen.
-

Inhalt:

- Die Studierenden lernen den Prozess wie in der Wissenschaft in der Regel Publikationen bewertet und veröffentlicht werden (peer-review) kennen.
- Definition und Vorstellung eines Themenkomplexes, der innerhalb der Veranstaltung von den Studierenden vertieft und aus unterschiedlichen Blickwinkeln bearbeitet wird. Die Definition der Themen soll dabei entlang aktueller Veröffentlichungen auf führenden wissenschaftlichen Konferenzen und Journals zum Thema IT-Sicherheit und Privatheit erfolgen.
- Die Studierenden stellen aktuelle wissenschaftliche Veröffentlichungen in dem Themenkomplex der Gruppe vor
- Die Studierenden diskutieren in der Gruppe die vorgestellten Arbeiten und können diese so im größeren Rahmen des gesamtthemenkomplexes setzen und interpretieren.
- Die Studierenden fertigen eigene Experimente an, um die vorgestellten Ergebnisse zu demonstrieren.

Studien- / Prüfungsleistungen:

- Prüfungsleistungen: Kombinationsprüfung aus 2 Teilleistungen
- Präsentationen (50%)
 - Schriftliche Ausarbeitung (50%)

Literatur:

Aktuelle wissenschaftliche Veröffentlichungen zu dem jeweiligen Thema der Vorlesung (wird zu Veranstaltungsbeginn bekannt gegeben).

Bemerkungen:

Future Computing

<i>Kürzel:</i>	FCO
<i>Untertitel:</i>	Neue Rechnerkonzepte
<i>Studiensemester:</i>	(Master)
<i>Modulverantwortliche(r):</i>	Prof. Dr. Dieter Hannemann
<i>Dozent(in):</i>	Prof. Dr. Dieter Hannemann
<i>Sprache:</i>	deutsch
<i>Zuordnung zum Curriculum:</i>	IN WP IS WP MI WP WI WP
<i>Lehrform / SWS:</i>	2 SWS Vorlesung, 2 SWS Übung
<i>Gruppengröße:</i>	Nicht begrenzt
<i>Arbeitsaufwand:</i>	Kontaktzeit: 60 Zeitstunden Selbststudium: 120 Zeitstunden
<i>Leistungspunkte:</i>	6
<i>Turnus:</i>	Wintersemester, jährlich
<i>Teilnehmerzahl:</i>	Nicht begrenzt
<i>Anmeldungsmodalitäten:</i>	Anmeldung per Email: Prof@DieterHannemann.de
<i>Voraussetzungen nach Prüfungsordnung:</i>	keine
<i>Empfohlene Voraussetzungen (Modulprüfungen):</i>	Mathematik und Physik auf Bachelor-Niveau. Fehlende Physikkenntnisse können durch ein eLearning-Modul nachgeholt werden.
<i>Angestrebte Lernergebnisse:</i>	<p>Aufbauend auf Schulkenntnissen aus dem Bereich der Naturwissenschaften verstehen die Studierenden nach dem Studium dieses Moduls, welche Bedeutung neuere Rechnerkonzepte für die moderne Informatik haben. Durch die Beschäftigung mit der naturwissenschaftlichen Methodik wurde gleichzeitig die logisch, analytische Denkweise verbessert und Problemlösungskompetenz entwickelt.</p> <p>Dieses Modul trägt dazu bei, die Absolventen ganz allgemein zu wissenschaftlicher Arbeit und verantwortlichem Handeln bei der beruflichen Tätigkeit und in der Gesellschaft zu befähigen.</p> <p>Insbesondere werden durch dieses Modul die folgenden Fertigkeiten und Kompetenzen der Absolventen gestärkt:</p> <p>Sie sind in der Lage, komplexe Aufgabenstellungen aus einem neuen oder in der Entwicklung begriffenen Bereich zu abstrahieren und zu formulieren sowie Konzepte und Lösungen zu komplexen, zum Teil auch</p>

unüblichen Aufgabenstellungen – ggf. unter Einbeziehung anderer Disziplinen – zu entwickeln.

Sie haben die Kompetenz, sich systematisch und in kurzer Zeit in neue Systeme und Methoden einzuarbeiten, neue und aufkommende Technologien zu untersuchen und zu bewerten sowie Wissen aus verschiedenen Bereichen methodisch zu klassifizieren und systematisch zu kombinieren.

Sie wissen, auf welchen Grundprinzipien Quantencomputer beruhen und wie man mit dem Erbgut – der DNA – rechnen kann. Dabei wird die Biologie – im Bereich der Lebensinformatik – vor allem verstanden als die Wissenschaft von den komplexesten Systemen der Informations-verarbeitung, die es nur in der Natur gibt und deren Übertragung in die Informatik von großer Bedeutung ist.

Inhalt:

- Einführung
 - Lernhinweise
 - Informationen
 - Intelligenz
- Molecular Computing
 - BioPhysik
 - Molekulargenetik
 - Epigenetik
 - Molekulares Rechnen
- Computational Intelligence
 - Neurobiologie
 - Neuroinformatik
 - Neuromorphie
 - Fuzzy-Logik
- Neue Technologien
 - Quanten
 - Quanteninformatik
 - Diverses

Studien- / Prüfungsleistungen: Prüfungsleistungen: Klausur (90 Min.)

Literatur:

- Hannemann, D.: "Physik Smart-Book", ISBN 978-3-920088-52-5
- Bostrom Nick, 2014: "Superintelligenz" Surkamp, eISBN 978-3-518-73900-6
- Kurzweil, Ray, 2014: "Menschheit 2.0" Die Singularität naht, ISBN 978-3-944203-08-9
- Human Brain Project, 2022:
<https://www.humanbrainproject.eu/>
- Homeister, Matthias, 2018: "Quantum Computing verstehen", ISBN 978-3-658-10455-9
- Hinze, Th., M. Sturm, 2004: "Rechnen mit DNA" ISBN 3-486-27530-5
- Sackmann, E. & Merkel, R. 2010: "Lehrbuch der Biophysik"
- Thompson, R.F., 2001: "Das Gehirn", ISBN: 978-3-662-53349-9
- Diverse Forschungsberichte zu folgenden Themen:
 - Neuromorphes Computing
 - Quanten-Computer, -Internet, -Information
 - Photonische Chips

Bemerkungen:

Die Lernmaterialien werden nach der Anmeldung zum Modul vollständig zur Verfügung gestellt: multimediales Online-Lernmaterial (Animationen, Simulationen, Videos, etc.). Weitere Informationen: <http://future-computing.dieterhannemann.de/>

Funktionale Programmierung

<i>Kürzel:</i>	FPR			
<i>Untertitel:</i>				
<i>Studiensemester:</i>	(Master)			
<i>Modulverantwortliche(r):</i>	Prof. Dr. Marcel Luis			
<i>Dozent(in):</i>	Prof. Dr. Marcel Luis			
<i>Sprache:</i>	Deutsch			
<i>Zuordnung zum Curriculum:</i>	IN WP	MI WP	IS WP	WI WP
<i>Lehrform / SWS:</i>	2 SWS Vorlesung, 1 SWS Übung, 1 SWS Praktikum			
<i>Gruppengröße:</i>	Vorlesung: Nicht begrenzt, Übung: 40, Praktikum: 20			
<i>Arbeitsaufwand:</i>	Kontaktzeit: 56 Zeitstunden Selbststudium: 124 Zeitstunden			
<i>Leistungspunkte:</i>	6			
<i>Turnus:</i>	Sommersemester, jährlich			
<i>Teilnehmerzahl:</i>	Nicht begrenzt			
<i>Anmeldungsmodalitäten:</i>				
<i>Voraussetzungen nach Prüfungsordnung:</i>	Keine			
<i>Empfohlene Voraussetzungen (Modulprüfungen):</i>	Objektorientierte Programmierung sowie Algorithmen und Datenstrukturen auf Bachelor-Niveau			
<i>Angestrebte Lernergebnisse:</i>	Die Studierenden beherrschen die grundlegenden Konzepte der funktionalen Programmierung (FP) und können diese für kleine Aufgabenstellungen (in der Lehrsprache Haskell) sicher anwenden. Sie kennen die in FP möglichen Realisierungsmuster, z.B. in Verbindung mit unendlichen Datenstrukturen oder Monaden. Sie verstehen, dass FP für eine Vielzahl von Problemen eine elegante, fehlervermeidende und produktive Form der Programmierung ist. Durch Termersetzung als Auswertungsmodell gewinnen die Studierenden einen Einblick in symbolisches Rechnen und erweiterten zudem ihre Sicht auf den Begriff der Berechnung. Durch Seitenblicke auf die Sprache Java erkennen die Studierenden schließlich, dass viele Konzepte von FP auch in originär nicht funktionalen Sprachen angewendet werden können. Dadurch verbessern sie ihre Produktivität und Qualität bei der Software-Entwicklung in solchen Sprachen.			
<i>Inhalt:</i>	Ausdrücke, Reduktion und Reduktionsstrategien • Typen und Typklassen • Currying und Funktionen höherer Ordnung • Listen, rekursive Datentypen • Fold			

	für Listen, laws of fold • Unendliche Datenstrukturen • Programmieren mit lazy evaluation • Monaden • Praxisbeispiele
<i>Studien- / Prüfungsleistungen:</i>	Studienleistungen laut Prüfungsordnung als Voraussetzung zur Prüfungsteilnahme: Keine Prüfungsleistungen: Klausur (90 Min.) oder mündliche Prüfung
<i>Literatur:</i>	<ul style="list-style-type: none">• Richard Bird: Introduction to Functional Programming using Haskell. Prentice Hall, 2002.• Richard Bird: Thinking Functionally with Haskell. Cambridge University Press, 2014.
<i>Bemerkungen:</i>	-

Intelligente Systeme

<i>Kürzel:</i>	INT			
<i>Untertitel:</i>	---			
<i>Studiensemester:</i>	(Master)			
<i>Modulverantwortliche(r):</i>	Prof. Dr. Wolfram Conen			
<i>Dozent(in):</i>	Prof. Dr. Wolfram Conen			
<i>Sprache:</i>	Deutsch			
<i>Zuordnung zum Curriculum:</i>	IN WP	MI WP	IS WP	WI -
<i>Lehrform / SWS:</i>	2 SWS Vorlesung, 1 SWS Übung, 1 SWS Praktikum			
<i>Gruppengröße:</i>	Standard			
<i>Arbeitsaufwand:</i>	Kontaktzeit: 60 Zeitstunden Selbststudium: 120 Zeitstunden			
<i>Leistungspunkte:</i>	6			
<i>Turnus:</i>	Wintersemester, jährlich			
<i>Teilnehmerzahl:</i>	Nicht begrenzt			
<i>Anmeldungsmodalitäten:</i>	Anmeldung über den Moodle-Kurs zu diesem Modul			
<i>Voraussetzungen nach Prüfungsordnung:</i>	Keine modulspezifischen Voraussetzungen			
<i>Empfohlene Voraussetzungen (Modulprüfungen):</i>	KI im Bachelorstudiengang Informatik			
<i>Angestrebte Lernergebnisse:</i>	<p>Die Studierenden kennen grundlegende Methoden und Strukturen aus ausgewählten Kapiteln der künstlichen Intelligenz und können diese zur Konstruktion intelligenter Systeme anwenden.</p> <p>Sie sind insbesondere in der Lage, durch Abstraktion und Modellbildung Problemstellungen zu analysieren, Zusammenhänge zu vorhandenem Wissen zu erkennen und entsprechende Lösungsansätze zu identifizieren und umzusetzen.</p> <p>Sie sind mit der Problematik der Interpretation von Modellen und den Risiken ihres Einsatzes vertraut und können Ansätze, diese Risiken zu bewerten und zu minimieren, analysieren und kritisch hinterfragen.</p>			
<i>Inhalt:</i>	<p>Einführendes: Geschichte der KI, ausgewählte aktuelle Forschungsansätze.</p> <p>Grundlegendes: Problemlösung mit exakter und heuristischer Suche, Constraint Satisfaction/Optimization. Problemmodellierung und -lösung mit Logik und Wahrscheinlichkeiten.</p>			

	Lernen und intelligente Informationsanalyse: klassische Verfahren (Kategorisierung, Clustering: u.a. Naive Bayes, Decision Trees, EM), stochastische Verfahren (Hidden Markov, POMDP), naturanaloge Verfahren (NN, Deep-NN). Optimierung von Handlungssequenzen: Adversarial Search, DP und Reinforcement Learning, inkl. Deep-RL. Interpretierbarkeit von Modellen, ethische und gesellschaftliche Konsequenzen des Einsatzes von intelligenten Systemen.
<i>Studien- / Prüfungsleistungen:</i>	Klausur
<i>Literatur:</i>	<ul style="list-style-type: none">• Russell, Norvig: Artificial Intelligence, A Modern Approach, Pearson, in aktueller Auflage (4. derzeit)• Ausgewählte grundlegende und aktuelle Forschungspapiere und Vorträge.
<i>Bemerkungen:</i>	---

Logische Programmierung

Kürzel:	LPR			
Untertitel:	Theoretische Grundlagen, Konzepte und Anwendungen			
Studiensemester:	(Master)			
Modulverantwortliche(r):	Prof. Dr. Ulrike Griefahn			
Dozent(in):	Prof. Dr. Ulrike Griefahn			
Sprache:	Deutsch			
Zuordnung zum Curriculum:	IN WP	MI WP	IS WP	WI -
Lehrform / SWS:	3 SWS Vorlesung, 1 SWS Übung			
Gruppengröße:	Vorlesung: Nicht begrenzt, Übung: 40, Praktikum: 20			
Arbeitsaufwand:	Kontaktzeit: 60 Zeitstunden Selbststudium: 120 Zeitstunden			
Leistungspunkte:	6			
Turnus:	Sommersemester, unregelmäßig			
Teilnehmerzahl:	Nicht begrenzt			
Anmeldungsmodalitäten:	Anmeldung über den Moodle-Kurs zu diesem Modul			
Voraussetzungen nach Prüfungsordnung:	Keine modulspezifischen Voraussetzungen			
Empfohlene Voraussetzungen (Modulprüfungen):	Kenntnisse in Logik, Theoretischer Informatik, Algorithmen und Datenstrukturen auf Bachelor-Niveau			
Angestrebte Lernergebnisse:	<p>Die Studierenden kennen die Konzepte der logischen Programmierung. Sie sind in der Lage, Probleme deklarativ zu beschreiben und hierfür logische Programme mit der Programmiersprache Prolog zu entwickeln.</p> <p>Sie kennen die Theorie der logischen Programmierung und können sowohl die deklarative als auch die prozedurale Semantik logischer Programme im Detail erläutern. Sie können die Unterschiede der prozeduralen Semantik zur Auswertungsstrategie von Prolog benennen und begründen, wie diese Abweichungen zustande kommen.</p> <p>Mit Kenntnissen der logischen Programmierung sind die Teilnehmer später besser in der Lage, Probleme auf einem höheren Abstraktionsniveau zu beschreiben und damit die Problemanalyse vom Entwurf einer Problemlösungsstrategie besser zu trennen.</p>			
Inhalt:	Während in der imperativen Programmierung mit Programmen alle Schritte festgelegt werden, die der Computer in der angegebenen Reihenfolge			

auszuführen hat, wird in der logischen Programmierung das zu lösende Problem nur beschrieben und die Lösungsfindung einem Auswertungssystem überlassen. Inhalte der Vorlesung sind:

- Problemlösen mit Prolog: Auswertungsstrategie, Unifikation, Backtracking.
- Programmietechniken: Generate & Test, Relationen, Datenstrukturen als Fakten, Musterorientierte Wissensrepräsentation
- Theorie der logischen Programmierung: Prädikatenlogik 1. Ordnung, Deklarative Semantik, SLD-/SLDNF-Resolution
- Nicht-logische Bestandteile von Prolog: Negation und Cut
- Sprachverarbeitung in Prolog: Grammatiken und Parsergenerierung
- Ausblick Constraint-logische Programmierung

Studien- / Prüfungsleistungen:	Studienleistungen laut Prüfungsordnung als Voraussetzung zur Prüfungsteilnahme: Keine Prüfungsleistungen: Klausur (90 Min.) oder mündliche Prüfung (30 Min.) Die Studierenden können durch die Teilnahme am Praktikum Bonuspunkte für die Klausur erwerben. Einzelheiten zum Erwerb der Bonuspunkte werden in der 1. Vorlesungsstunde bekannt gegeben.
---------------------------------------	--

Literatur:	<ul style="list-style-type: none"> • William F. Clocksin, Christopher S. Mellish: Programming in Prolog. Using the ISO Standard. 5th Ed., Springer, 2003, 299 Seiten, ISBN 978-3540006787 • Ivan Bratko: Prolog Programming for Artificial Intelligence (4th Ed.). Addison-Wesley, 2011, 696 Seiten, ISBN: 978-0321417466 • Ulf Nilsson, Jan Maluszynski: Logic, Programming, and Prolog (2nd Ed.). John Wiley, 1995, 294 Seiten, vom Verlag nicht mehr erhältlich, dafür online unter http://www.ida.liu.se/~ulfni/lpp (last updated: 2012-05-07) • Patrick Blackburn, Johan Bos, Kristina Striegnitz, Learn Prolog Now! College Publications, 2006, 284 Seiten, ISBN 978-1904987178 oder freie Online-Version http://www.learnprolognow.org.
-------------------	---

Bemerkungen:	---
---------------------	-----

NOSQL Datenbanken

<i>Kürzel:</i>	NSQ
<i>Untertitel:</i>	-
<i>Studiensemester:</i>	1. (Master)
<i>Modulverantwortliche(r):</i>	Prof. Dr. Katja Zeume
<i>Dozent(in):</i>	Prof. Dr. Katja Zeume
<i>Sprache:</i>	Deutsch
<i>Zuordnung zum Curriculum:</i>	IN WP MI WP IS WP WI 1
<i>Lehrform / SWS:</i>	2 Vorlesung, 1 SWS Übung, 1 SWS Praktikum
<i>Gruppengröße:</i>	Vorlesung: nicht begrenzt, Übung: 40, Praktikum: 20
<i>Arbeitsaufwand:</i>	Kontaktzeit: 60 Zeitstunden Selbststudium: 120 Zeitstunden
<i>Leistungspunkte:</i>	6
<i>Turnus:</i>	Wintersemester, jährlich
<i>Teilnehmerzahl:</i>	Nicht begrenzt
<i>Anmeldungsmodalitäten:</i>	Anmeldung über den Moodle-Kurs zu diesem Modul
<i>Voraussetzungen nach Prüfungsordnung:</i>	Keine modulspezifischen Voraussetzungen
<i>Empfohlene Voraussetzungen (Modulprüfungen):</i>	keine
<i>Angestrebte Lernergebnisse:</i>	<p>Die Studierenden beherrschen den theoretischen und praktischen Umgang mit verschiedenen Datenbankformaten und deren Anfragesprachen.</p> <p>Die Studierenden sind in der Lage, NOSQL-Datenbanken unter Einsatz des entsprechenden DB-Supports zu benutzen und zu entwickeln.</p>
<i>Inhalt:</i>	<ul style="list-style-type: none"> • Aktuelle Datenbankformate (über das relationale DB-Modell hinaus) und deren Anwendungsfälle in der Praxis • Überblick nicht-relationale / NOSQL Datenbanken und deren Anfragesprachen • Vor- und Nachteile der verschiedenen Formate • Wahlweise eines oder mehrerer der folgenden Themenkomplexe: Information Retrieval, Graphdatenbanken, Ontologien, Grenzen von Datenbanken, wichtige Ergebnisse der DB-Theorie
<i>Studien- / Prüfungsleistungen:</i>	Prüfungsleistung: Klausur (75min)

-
- Literatur:*
- Leskovec, Rajaraman, Ullman. Mining of Massive Datasets
 - Foundations of Databases, Serge Abiteboul, Rick Hull, Victor Vianu, 1995.
-

- Bemerkungen:* -
-

Privacy Enhancing Technologies

<i>Kürzel:</i>	PETS
<i>Untertitel:</i>	Privacy Enhancing Technologies
<i>Studiensemester:</i>	2. (Master)
<i>Modulverantwortliche(r):</i>	Prof. Dr. Tobias Urban
<i>Dozent(in):</i>	Prof. Dr. Tobias Urban
<i>Sprache:</i>	Deutsch oder Englisch
<i>Zuordnung zum Curriculum:</i>	IN WP MI - IS WP WI WP
<i>Lehrform / SWS:</i>	2 SWS Vorlesung 2 SWS Praktikum
<i>Gruppengröße:</i>	Vorlesung: Nicht begrenzt Praktikum: 20
<i>Arbeitsaufwand:</i>	Kontaktzeit: 60 Zeitstunden Selbststudium: 120 Zeitstunden
<i>Leistungspunkte:</i>	6
<i>Turnus:</i>	Wintersemester, jährlich
<i>Teilnehmerzahl:</i>	Nicht begrenzt
<i>Anmeldungsmodalitäten:</i>	Anmeldung über den Moodle-Kurs zu diesem Modul
<i>Voraussetzungen nach Prüfungsordnung:</i>	Keine modulspezifischen Voraussetzungen
<i>Empfohlene Voraussetzungen (Modulprüfungen):</i>	Keine
<i>Angestrebte Lernergebnisse:</i>	<p>Die Studierenden lernen verschiedene Ansätze kennen, wie Technologien entwickelt und eingesetzt werden können, um die Privatsphäre von Nutzerinnen und Nutzern zu steigern bzw. zu schützen. Außerdem werden Konzepte vorgestellt, wie Technologien privatsphärenfreundlich entwickelt werden können („Privacy-by-Design“). In dem Modul sollen die Studierenden Kenntnisse, Verständnis und Wissen in den folgenden Themenkomplexen erlernen</p> <ul style="list-style-type: none"> • Weltweite rechtliche Rahmenbedingungen bezüglich der Sammlung, Verarbeitung und Speicherung von personenbezogenen Daten. • Verständnis der grundlegenden Konzepte und Techniken zur Verbesserung der Privatsphäre. • Fähigkeit zur Bewertung und Implementierung von PET in verschiedenen Kontexten.

-
- Gängige Methoden und Gegenmaßnahmen zur Verfolgung („user tracking“) von Nutzerinnen und Nutzern im Internet.
 - Methodiken zur anonymen Kommunikation und zur Verarbeitung von verschlüsselten Daten.
 - Eigenständige Entwicklung von „Privacy Enhancing Technologies“ basierend auf aktuellen Forschungsthemen (basierend auf Primärliteratur).

Inhalt:**Grundlagen**

- Gesetzliche Rahmenbedingungen (z.B. DSGVO, CCPA/CPRA)
- Ethische Aspekte des Datenschutzes
- Definition von Grundbegriffen (z.B. Anonymität oder Pseudonymität)

User Tracking im Internet

- Third-party Tracking Methoden: Cookie-basiertes Tracking, Browser-Fingerprinting, u.Ä.
- First-Party Tracking: Server-side Tracking, CNAME Cloaking, u.Ä.
- Einwilligungserklärungen: Methodiken zur Verwaltung von Einwilligungserklärungen, gängige Praktiken zur Einholung von Einwilligungserklärungen, u.Ä.
- Privatheit im Web messen: Generelle Ansätze zur Messung des Webs, Design von Messtudien für Webanwendungen und Testen von Webseiten

Anonyme Kommunikation

- Das Tor-Netzwerk: Architektur und Funktionsweise, Erläuterung der verschiedenen Knotenarten (Entry Node, Relay Node, Exit Node), Onion Routing, Sicherheitsmerkmale und Schwachstellen
- Mixnets: Erläuterung des Konzepts von Mixnets und deren Unterschiede zu Tor, Mix-Kaskaden, Analyse der Sicherheitsmerkmale und Anonymitätsgarantien von Mixnets, typische Anwendungen und Einsatzmöglichkeiten von Mixnets
- Traffic-Analyse: Durchführung und Auswertung von Traffic-Analysen zur Untersuchung der Anonymität, Testen der Verbindung über das Tor-Netzwerk

Privacy by Design

- Prinzipien und Best Practices des Datenschutzes durch Design
- Datenschutzfreundliche Architektur, Datenschutz-Folgenabschätzung (PIA), Auditing

Kryptographische Ansätze

-
- Homomorphe Verschlüsselung: Grundlagen der homomorphen Verschlüsselung; Arten und Anwendungen (insb. teilweise homomorphe Verschlüsselung und voll homomorphe Verschlüsselung)
 - Secure Multi-Party Computation (SMPC): Konzepte und Protokolle der sicheren Mehrparteienberechnung (z.B. Yao's Garbled Circuits oder Secret Sharing)

Studien- / Prüfungsleistungen:**Prüfungsleistungen:**

Schriftliche Prüfung oder mündliche Prüfung oder Kombinationsprüfung (50% Klausur (60 Minuten) und 50% schriftliche Ausarbeitung). Die konkrete Prüfungsleistung wird zu Beginn der Veranstaltung festgelegt.

Literatur:

- Adams, Carlisle. Introduction to Privacy Enhancing Technologies. 1st ed. Cham, Switzerland: Springer Nature, 2021. <https://doi.org/10.1007/978-3-030-81043-6>.
- Jarmul, Katharine. Practical Data Privacy. O'Reilly Media, 2023.
- Dennedy, Michelle, Jonathan Fox, and Tom Finneran. The Privacy Engineer's Manifesto. PDF. 1st ed. Berlin, Germany: APress, 2014. <https://doi.org/10.1007/978-1-4302-6356-2>.
- Aktuelle wissenschaftliche Veröffentlichungen

Bemerkungen:

Weiterführende Konzepte zum Betrieb komplexer verteilter Systeme

<i>Kürzel:</i>	WKV
<i>Untertitel:</i>	---
<i>Studiensemester:</i>	(Master)
<i>Modulverantwortliche(r):</i>	Prof. Dr. Andreas Cramer
<i>Dozent(in):</i>	Prof. Dr. Andreas Cramer
<i>Sprache:</i>	Deutsch
<i>Zuordnung zum Curriculum:</i>	IN MI IS WI WP - WP WP
<i>Lehrform / SWS:</i>	2 SWS Vorlesung, 2 SWS Praktikum
<i>Gruppengröße:</i>	Vorlesung: nicht begrenzt, Praktikum: 20
<i>Arbeitsaufwand:</i>	Kontaktzeit: 56 Zeitstunden Selbststudium: 124 Zeitstunden
<i>Leistungspunkte:</i>	6
<i>Turnus:</i>	Sommersemester, jährlich
<i>Teilnehmerzahl:</i>	Nicht begrenzt
<i>Anmeldungsmodalitäten:</i>	Anmeldung über den Moodle-Kurs zu diesem Modul
<i>Voraussetzungen nach Prüfungsordnung:</i>	Keine modulspezifischen Voraussetzungen
<i>Empfohlene Voraussetzungen (Modulprüfungen):</i>	Betrieb komplexer verteilter Systeme, Betriebssysteme, Rechnernetze
<i>Angestrebte Lernergebnisse:</i>	Die Studierenden lernen unterschiedliche Technologien, Konzepte und Verfahren kennen, die für den Betrieb großer IT-Infrastrukturen wichtig sind. Sie bekommen erste Erfahrungen im Umgang mit diesen Technologien und Verfahren. Die Fähigkeit neue Technologien in diesem Umfeld schnell begreifen, einordnen und bewerten zu können wird erlangt. Die Studierenden lernen komplexe Rechnersysteme zu analysieren und mit Hilfe von formalen Methoden zu bewerten um Verbesserungen der Systeme vornehmen zu können.
<i>Inhalt:</i>	<ul style="list-style-type: none"> • Leistungsbewertung • Monitoring, Software, Hardware, hybrid Modellierung, funktionale und zeitbehaftete Petri-Netze • Zusammenhang zwischen Messung und Modellierung • Fehlertoleranz

-
- Rechner-Cluster
 - ITIL
 - IT-Controlling
-

Studien- / Prüfungsleistungen: Studienleistungen laut Prüfungsordnung als Voraussetzung zur Prüfungsteilnahme: erfolgreiche Teilnahme am Praktikum
Prüfungsleistungen: mündliche Prüfung oder Klausur

Literatur: Wird in der Vorlesung bekannt gegeben

Bemerkungen: ---

Übersetzerbau

<i>Kürzel:</i>	ÜSB
<i>Untertitel:</i>	---
<i>Studiensemester:</i>	(Master)
<i>Modulverantwortliche(r):</i>	Prof. Dr. Ulrike Griefahn
<i>Dozent(in):</i>	Prof. Dr. Ulrike Griefahn
<i>Sprache:</i>	Deutsch
<i>Zuordnung zum Curriculum:</i>	IN WP MI WP IS WP WI -
<i>Lehrform / SWS:</i>	2 SWS Vorlesung, 1 SWS Übung, 1 SWS Praktikum
<i>Gruppengröße:</i>	Vorlesung: nicht begrenzt, Übung: 40
<i>Arbeitsaufwand:</i>	Kontaktzeit: 60 Zeitstunden Selbststudium: 120 Zeitstunden
<i>Leistungspunkte:</i>	6
<i>Turnus:</i>	Wintersemester, jährlich
<i>Teilnehmerzahl:</i>	Nicht begrenzt
<i>Anmeldungsmodalitäten:</i>	keine
<i>Voraussetzungen nach Prüfungsordnung:</i>	Keine modulspezifischen Voraussetzungen
<i>Empfohlene Voraussetzungen (Modulprüfungen):</i>	Kenntnisse in Theoretischer Informatik, Algorithmen und Datenstrukturen, Objektorientierter und/oder Prozeduraler Programmierung auf Bachelor-Niveau
<i>Angestrebte Lernergebnisse:</i>	<p>Die Studierenden kennen die Phasen der Übersetzung von Programmiersprachen in Maschinensprache, wobei der Schwerpunkt der Vorlesung auf dem Front-End (Analysephase und Zwischencode-Erzeugung) liegt, da eine Kenntnis der dort angewendeten Methoden und Konzepte für die spätere Berufspraxis von größerem Nutzen ist.</p> <p>Die Studierenden sind in der Lage, eigene formale Sprachen für spezielle Anwendungen oder komplexe Datenformate zu definieren. Sie können für diese Sprachen mit Hilfe von Scanner- und Parser-Generatoren entsprechende Scanner und Parser konstruieren. Sie sind in der Lage, geeignete interne Repräsentationen als (Zwischen-)Übersetzungsziele zu entwickeln.</p> <p>Sie können die Konstruktion von Scannern aus regulären Ausdrücken und von Top-Down- und Bottom-Up-Parsern aus kontextfreien Grammatiken im Detail erklären und implementieren. Sie können mit Hilfe</p>

	syntaxgesteuerter Definitionen als Ergebnis der Übersetzung abstrakte Syntaxbäume konstruieren oder Zwischencode erzeugen.
<i>Inhalt:</i>	<p>In der Vorlesung werden alle Phasen der Übersetzung behandelt. Der Schwerpunkt liegt auf der Analysephase und der Zwischencode-Erzeugung.</p> <ul style="list-style-type: none"> • Einführung: Programmiersprachen, Übersetzer, Interpreter • Lexikalische Analyse: Reguläre Ausdrücke, endliche Automaten, Scanner-Generatoren • Syntaktische Analyse: Kontextfreie Sprachen, Top-Down- und Bottom-Up-Analyse, Parser-Generatoren • Syntaxgesteuerte Übersetzung: abstrakte Syntaxbäume • Semantische Analyse: Typprüfung • Zwischencodeerzeugung: Drei-Adress-Code • Ausblick zu Codeoptimierung und Codeerzeugung <p>In den Übungen wird u.a. ein durchgängiges Projekt zum Übersetzerbau bearbeitet.</p>
<i>Studien- / Prüfungsleistungen:</i>	<p>Studienleistungen laut Prüfungsordnung als Voraussetzung zur Prüfungsteilnahme: Keine Prüfungsleistungen: Klausur (120 Min.) oder mündliche Prüfung (30 Min.)</p> <p>Die Studierenden können durch die Teilnahme am Übersetzerbauprojekt Bonuspunkte für die Klausur erwerben. Einzelheiten zum Erwerb der Bonuspunkte werden in der 1. Vorlesungsstunde bekannt gegeben.</p>
<i>Literatur:</i>	<ul style="list-style-type: none"> • Aho, A., Lam, M., Sethi, R., Ullman, J.: Compilers: Principles, Techniques & Tools. Addison Wesley, 2. Auflage, 2013, 942 Seiten, ISBN: 978-1292024349 oder die deutsche Übersetzung der 1. Auflage: • Compiler: Prinzipien, Techniken und Werkzeuge, Pearson Studium, 2. Auflage, 2008, ISBN-13: 978-3827370976 • Appel, A.W.: Modern Compiler Implementation in Java. 2. Auflage, Cambridge University Press, 2002, 512 Seiten ISBN: 978-0521820608
<i>Bemerkungen:</i>	---
