Universität der Bundeswehr München
Werner-Heisenberg-Weg 39
85577Neubiberg

Modulhandbuch des Studiengangs

Cyber - Sicherheit
(Master of Science)

an der
Universität der Bundeswehr München

(Version 2022)

Stand: 02. Dezember 2021

Inhaltsverzeichnis

Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022

Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2022

Seminar - CYB 2022

Masterarbeit - CYB 2022

Verpflichtendes Begleitstudium plus

Modulname	Modulnummer
Netzsicherheit	5502

Konto	Pflichtmodule - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Gabi Dreo Rodosek	Pflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10102	VÜ	Netzsicherheit	Pflicht	3
10103	P	Praktikum Netzsicherheit	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Grundlegende Kenntnisse zu Rechnernetzen, wie sie z.B. in der Bachelor-Vorlesung Einführung in Rechnernetze vermittelt werden.

Qualifikationsziele

Die Studierenden lernen in der Vorlesung Netzsicherheit die Gefährdungsaspekte von Netzen und deren Entwicklung detailliert kennen. Nach erfolgreichem Abschluss des Moduls sind die Studierenden befähigt, sicherheitsrelevante Aspekte in vernetzten Strukturen zu erkennen und Betrachtungen von Netzen in Bezug auf Sicherheitsaspekte durchzuführen. Sie werden in die Lage versetzt, Verfahren zum Schutz und der Absicherung der jeweiligen Netze zu identifizieren. Mittels der Vorstellung von aktuellen Geräten und neuer Verfahren werden die Studierenden zusätzlich befähigt, Abschätzungen von Sicherheitsgefährdungen durch neue Technologien zu geben.

Nach dem Praktikum Netzsicherheit sind die Studierenden in der Lage, Maßnahmen zur Abwehr von gängigen Bedrohungen und zur Absicherung von IT-Systemen zu implementieren und deren Wirksamkeit zu verifizieren. Durch die eigenständige Bearbeitung von angeleiteten, praktischen Aufgaben vertiefen und festigen die Studierenden ihre Kenntnisse im Bereich Cyber-Sicherheit.

Inhalt

In der Vorlesung Netzsicherheit erhalten Studierende einen vertieften Einblick in Fragestellungen der Netzsicherheit. Hierbei werden zunächst die Sicherheitsbedrohungen im Wandel von klassischen Angriffen hin zum Cyber War mit Schadsoftware und deren Verbreitung betrachtet, sowie u.a. aktive und passive Angriffe, Blended Attacks, Web Hacking, Spam, Botnetze und Aspekte der Internet-Kriminalität behandelt.

Im weiteren Verlauf stehen sowohl Firewall-Architekturen, -konzepte, -Systeme als auch Intrusion Detection und Prevention Systeme, Honeypots (Low- und High-Interaction), Honeynets sowie Early Warning Systeme im Fokus. Eine vertiefende Auseinandersetzung mit sicherheitsrelevanten Protokollen wie IPsec und den Auswirkungen der breitbandigen Nutzung von IPv6 auf die Netzsicherheit ist ebenso Bestandteil der Vorlesung. Wesentliche Techniken und Besonderheiten neuer Verfahren und Ansätze zur Angriffserkennung im Bereich der mobilen Endgeräte wie Smartphones und Tablet-PCs sowie des Cloud Computings schließen die Thematik ab.

Schwerpunkt im Praktikum Netzsicherheit ist die selbstständige Durchführung von praktischen Aufgaben zu aktuellen Themen und Fragestellungen der Absicherung von IT-Systemen. Zu Beginn werden einfache Angriffe auf den Ebenen 2 bis 4 sowie 7 des ISO/OSI-Referenzmodells vorgestellt, bspw. durch die Manipulation von ARP, Subnetting oder Angriffe gegen Webseiten auf Applikationsebene (z.B. XSS). Entsprechende Gegenmaßnahmen werden untersucht und integriert (z.B. Einrichtung und Betrieb einer Firewall, Absicherung von Webservern, Aufbau und Betrieb von Tunneln). Darauf aufbauend werden weitere, aktuelle Angriffsverfahren behandelt, bspw. Bot-Netz-Attacken oder spezialisierte Angriffe wie z.B. zielgerichtete Angriffe. Hierzu werden ebenfalls geeignete Gegenmaßnahmen entwickelt und praktisch implementiert (z.B. Intrusion Detection/Prevention Systeme, low/high interaction Honeypots/Honeynets).

Leistungsnachweis
Notenschein, der zwei Teilleistungen umfasst. Zur Vorlesung ist eine schriftliche Prüfung mit 60 Minuten Dauer oder eine mündliche Prüfung mit 20 Minuten Dauer abzulegen; die Prüfungsform wird zu Beginn des Moduls festgelegt. Eine Wiederholmöglichkeit besteht im Sommer (am Ende des FT).
Dauer und Häufigkeit
Das Modul dauert 1 Trimester.

Modulname	Modulnummer
Hardwaresicherheit	5503

Konto	Pflichtmodule - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Ph.D. M.S. (OSU) Klaus Buchenrieder	Pflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10311	VÜ	Eingebettete Systeme	Pflicht	3
55031	VÜ	Embedded Systems Security	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Voraussetzung für alle Modulbestandteile sind Kenntnisse in Rechnerarchitektur. Für Eingebettete Systeme sind zusätzlich Kenntnisse zu Rechnerorganisation notwendig, wie sie im Bachelor-Modul Rechnerorganisation vermittelt werden.

Qualifikationsziele

Die Studierenden vertiefen die Kompetenz, das grundlegende Verhalten und die wesentlichen Aufgaben von hardwarenahen Rechnersystemen in der Praxis zu verstehen und zu bewerten. Sie können Eigenschaften von hardwarenahen Rechnersystemen fachwissenschaftlich einordnen und haben damit die Grundlage, die Verwendbarkeit dieser Konzepte für bestimmte praktische Anwendungen zu bewerten. Die Studierenden wissen, wie eingebettete Systeme hinsichtlich der Übertragung, Verarbeitung und Speicherung von Daten abzusichern sind. Sie kennen technische und physische Angriffsvarianten wie Seitenkanalangriffe und wissen, wie Software-Implementierungen dagegen gehärtet werden können.

Inhalt

In diesem Modulbestandteil erhalten die Studierenden einen umfassenden Überblick über die wesentlichen Grundlagen und Konzepte, die zum Entwurf eingebetteter Systeme notwendig sind. Zu Beginn werden die Kenntnisse über Hardware-Konzepte aus dem Modul "Rechnerorganisation" vertieft und darauf aufbauend Mikro- und spezielle Architekturen entwickelt. Neben den gängigen Prozessorarchitekturen werden digitale Signalprozessoren (DSP) und System-on-Chip Architekturen eingeführt.
Zu Themen der maschinennahen Programmierung von Mikroprozessoren und Mikrokontrollern werden Konzepte und Probleme der Verarbeitung von Events und Daten unter Echtzeitbedingungen behandelt. Nach der Einführung asynchroner Ereignisse und den dazu gehörenden Zeitbedingungen werden grundlegende Verfahren zur Ereignissynchronisation beschrieben und Prozessplanungsverfahren vorgestellt.
Im dritten Abschnitt des Modulbestandteils wird auf die Entwurfsmethodik für die

Konstruktion leistungsfähiger Eingebetteter Systeme eingegangen. In der Übung zur Vorlesung wird hardwarenahe Software in Kleingruppen entwickelt, in Betrieb genommen und getestet.

In der Vorlesung Embedded Systems Security wird nach einem Überblick über typische Architekturen und Eigenschaften von zeitgemäßen eingebetteten Systemen ein Schwerpunkt auf mögliche Angreifer auf solche Systeme gelegt. Ausgehend davon, dass typische Angreifer Hardware-Zugriff haben, werden verschiedene Angriffsmöglichkeiten erläutert und zueinander in Kontext gesetzt. Anhand von typischen Hardware-Chips werden Sicherheitsmechanismen und dedizierte Sicherheitschips besprochen. Danach wird ein Schwerpunkt auf kryptographische Algorithmen und deren Implementierung in eingebetteten Systemen gelegt. Dabei werden die schwerwiegenden sogenannten Seitenkanalangriffe behandelt. Danach wird die Implementierung von Sicherheitsmechanismen gegen vorgestellte Angriffe thematisiert. FPGA Zielplattformen sind in speziellen Einsatzbereichen sehr relevant. Die Informationssicherheit von Systemen auf deren Basis wird eigens behandelt. Schlußendlich wird noch die Kommunikationssicherheit von eingebetteten Systemen erläutert. In der Übung wird ein beispielhaftes eingebettetes µC-System anhand der in der Chip-HW vorhandenen Sicherheitsmechanismen gehärtet. Danach wird eine kryptographische Implementierung auf diesen µC portiert und ein Seitenkanalangriff durchgeführt.

Leistungsnachweis

Schriftliche Prüfung mit 60 Minuten Dauer, mündliche Prüfung mit 30 Minuten Dauer oder Notenschein. Die Prüfungsform wird zu Beginn des Moduls festgelegt.

Dauer und Häufigkeit

Das Modul dauert 2 Trimester.

Modulname	Modulnummer
Datenschutz und Privacy	5504

Konto	Pflichtmodule - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Arno Wacker	Pflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55041	VÜ	Datenschutz	Pflicht	3
55042	VÜ	Privacy Enhancing Technologies	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Grundlegende Kenntnisse der Informatik, wie sie im Bachelor-Studium vermittelt werden.

Qualifikationsziele

Die Studierenden kennen die Ziele und Grundbegriffe des Datenschutzes. Sie können erkennen, welche Vorgänge datenschutzrelevant sind und welche gesetzlichen und branchenspezifischen Regelungen dabei berücksichtigt werden müssen. Sie können Folgeabschätzungen für neue Technologien und Verfahren vornehmen und aktuelle technische Schutzmaßnahmen anwenden. Die Studierenden können die Datenschutzrelevanz passiver und aktiver Angriffe wie Verkehrsanalysen beurteilen und Abwägungen zwischen hoher Schutzwirkung und anderen Merkmalen wie Kosten, Bandbreite und Latenz treffen. Sie kennen Ansätze wie Differential Privacy, Multi-Party-Computation und Homomorphe Verschlüsselung und können deren Anwendungsgebiete voneinander abgrenzen

Inhalt

Ziel der Vorlesung "Datenschutz" ist es, verstehen und begründen zu können, was Privacy ist und warum sie sowohl für Einzelne als auch für demokratische Gesellschaften von Bedeutung ist. Es wird ein kurzer Überblick über die Entwicklung der Privatheit in der menschlichen Geschichte gegeben und gezeigt, was die aktuelle rechtliche Lage insbesondere in Deutschland und der EU bezüglich Datenschutzes ist. Der Fokus wird dabei auf der Datenschutz-Grundverordnung der EU (DSGVO) liegen. Es werden u.a. Grundbegriffe des Datenschutzes erläutert und die Datenschutz-Grundsätze vorgestellt. Ein Schwerpunkt dieser Vorlesung werden verschiedene technische Maßnahmen zur Umsetzung des Datenschutzes sein, z.B. technische Umsetzung des Rechts auf Löschen.

Der Fokus der Vorlesung "Privacy Enhancing Technologies" (PETs) liegt auf der technischen Unterstützung sowie Umsetzung von Datenschutz und Privatheit. Es werden zunächst die Prinzipien von PETs sowie die grundlegenden Ansätze zu deren Umsetzung, wie z.B. Privacy by Design, Kryptographie oder Multi-Party Computation, vorgestellt und analysiert. Anschließend werden sowie theoretische Konzepte als auch bereits die in der Praxis umgesetzte Konzepte, Methoden und Werkzeuge der PETs betrachtet, z.B. Funktionsweise und Einsatzgebiete von Blockchain oder der ePass. Um das Wissen über verschiedene Möglichkeiten zum Schutz der eigenen Daten in deren gesamten Lebenszyklus anschaulich zu vermitteln, werden Daten in sechs verschiedene Bereichen eingeteilt und getrennt betrachtet: (1) Authentifizierung, (2) Daten auf lokalen Systemen (Data-at-Rest), (3) Daten in Übertragung (Data-in-Motion), (4) Daten Online/ im Web, (5) Online-Banking und anonymes Bezahlen, (6) Privatheit auf mobilen Geräten. Für jeden dieser Bereiche werden zunächst die Risiken für die Privatheit analysiert und anschließend mögliche Methoden und Techniken für Gegenmaßnahmen vorgestellt und diskutiert.
Leistungsnachweis
Schriftliche Prüfung mit 60 Minuten Dauer oder mündliche Prüfung mit 30 Minuten Dauer oder Notenschein. Die Prüfungsform wird zu Beginn des Moduls festgelegt.
Dauer und Häufigkeit
Das Modul dauert 1 Trimester.

Modulname	Modulnummer
Systemsicherheit	5505

Konto	Pflichtmodule - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Gunnar Teege	Pflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10104	VÜ	IT-Forensik	Pflicht	3
55051	VÜ	Betriebssystemsicherheit	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Grundlegende Kenntnisse zu Betriebssystemen, wie sie z.B. im Bachelor-Modul Einführung in die Technische Informatik vermittelt werden.

Qualifikationsziele

Die Studierenden lernen die wesentliche Rolle kennen, die das Betriebssystem für die Absicherung von Computersystemen spielt und die dabei verwendeten Vorgehensweisen und nötigen Hardware-Voraussetzungen, aber auch die Grenzen rein technischer Maßnahmen. Damit sind sie in der Lage, die Wirksamkeit von Sicherheitsmaßnahmen einzuordnen und Sicherheitseigenschaften von Betriebssystemen abhängig von der Einsatzumgebung zu bewerten. Sie erhalten eine erste Orientierung zum Vorgehen bei der Absicherung von IT-Systemen durch Auswahl und Konfiguration des Betriebssystems und den Einsatz spezieller Sicherheitsmechanismen.

Die Studierenden entwickeln ein Verständnis für die Prinzipien und Vorgehensweisen bei der Untersuchung von Sicherheitsvorfällen. Sie kennen die grundlegenden Schritte eines Computerforensikers und können diese auf konkrete Angriffsszenarien anwenden. Insbesondere verstehen sie die verschiedenen Analysemethoden und sind in der Lage, diese in Form einer gerichtsverwertbaren Aufarbeitung anwenden zu können. Ferner beherrschen sie die forensische Analyse einer Festplatte mittels Open-Source-Tools sowie die Erarbeitung von Konzepten zur Sicherheitsüberprüfung komplexer Systeme.

Inhalt

Zu den Sicherheitsaspekten von IT-Systemen, die typischerweise durch das Betriebssystem implementiert werden, gehören klassischerweise die Zugangs- und Zugriffskontrolle und die Bildung verschiedener Schutzbereiche zur Ausführung von Anwendungen. In der Veranstaltung Betriebssystemsicherheit werden zuerst die wesentlichen Mechanismen zur Absicherung von Software, insbesondere des Betriebssystems selbst vorgestellt (secure boot, Festplattenverschlüsselung,

Hauptspeicherverschlüsselung). Anschließend werden Maßnahmen zur Herstellung von Vertraulichkeit innerhalb eines Rechners betrachtet und Angriffe darauf (Verdeckte Kanäle, Seitenkanäle). Im zweiten Teil der Veranstaltung werden Autorisierungssysteme vorgestellt. Dabei wird ihre Struktur betrachtet, allgemeine Eigenschaften und Grenzen (Safety-Problem) und der Umgang mit diesen Systemen (Sicherheitsmodelle, mandatory / discretionary access control). Abschließend werden Bewertungskriterien für die Sicherheit von Rechensystemen behandelt mit Schwerpunkt auf dem Common Criteria Standard.

IT-Forensik beschäftigt sich mit der Untersuchung von Vorfällen (Incidents) von IT-Systemen. Durch Erfassung, Analyse und Auswertung digitaler Spuren in Computersystemen werden nach Möglichkeit sowohl der Tatbestand als auch der oder die Täter festgestellt. Im Rahmen der Veranstaltung erhalten die Studenten zunächst einen grundlegenden Überblick über die Thematik IT-Forensik. Im nächsten Schritt erfolgt ein vertiefender Einblick in den Aufbau von Speichermedien (Festplatten, Flashspeicher, Magnetbänder) sowie Arten, Standards, Schnittstellen (Aufbau und Analyse von Standarddateisystemen, bspw. FAT, NTFS, ext4fs). Darauf aufbauend erfolgt eine Klassifikation von Datenträgern, Partitionierungsverfahren sowie prinzipiellen Analysemöglichkeiten (z.B. vor dem Hintergrund einer Verschlüsselung von Dateien). Als nächstes werden typische Angriffsmethoden untersucht, bevor am praktischen Beispiel einer forensischen Post-Mortem-Analyse ein konkretes Szenario bearbeitet wird. Hierbei wird u.a. ein spezieller Fokus auf die Einbeziehung von Behörden im Sinne einer gerichtsverwertbaren Auswertung gelegt.

Literatur

Zur Vorlesung Betriebssystemsicherheit: Es gibt kein Lehrbuch, das genau den Vorlesungs-Inhalt abdeckt. In den folgenden Büchern werden Themen aus der Vorlesung behandelt, sie sind als vertiefende Literatur verwendbar:

- Andrew S. Tanenbaum: Moderne Betriebssysteme, Pearson Studium, 3. Auflage, 2009
- Claudia Eckert: IT-Sicherheit, DeGruyter, Oldenbourg, 9. Auflage, 2014
- Trent Jaeger: Operating Systems Security, Morgan & Claypool, 2008
- Joachim Biskup: Security in Computing Systems, Springer, 2009.

Leistungsnachweis

Schriftliche Prüfung mit 60 Minuten Dauer.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester.

Modulname	Modulnummer
Kryptologie	5506

Konto	Pflichtmodule - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Arno Wacker	Pflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55061	VÜ	Einführung in die Kryptographie	Pflicht	3
55062	VÜ	Kryptoanalyse	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Grundkenntnisse in Mathematik, im Algorithmenentwurf und in der Algorithmenanalyse, wie sie in einführenden Lehrveranstaltungen zur Mathematik (Mathematische Strukturen, Lineare Algebra, Analysis) und zur Informatik vermittelt werden.

Qualifikationsziele

Die Studierenden kennen die wichtigsten grundlegenden kryptographischen Verfahren. Sie kennen ihre Vor- und Nachteile und ihre Stärken und Schwächen und können beurteilen, in welchen Situationen welche Verfahren eingesetzt werden können.
Sie kennen verschiedene Anwendungsgebiete kryptographischer Verfahren wie Geheimhaltung, Authentizität von Nachrichten und digitale Signaturen. Ferner kennen Sie die wichtigsten Methoden der Kryptoanalyse.

Inhalt

Die Grundbegriffe der Kryptographie sollen zuerst an klassischen symmetrischen Verschlüsselungsverfahren erläutert werden. Es werden zum Beispiel Stromchiffren und Blockchiffren (DES - Data Encryption Standard, AES - Advanced Encryption Standard) behandelt. Ein Schwerpunkt der einführenden Lehrveranstaltung werden allerdings asymmetrische Public-Key-Verschlüsselungsverfahren sein, zum Beispiel das RSA-Verfahren, die Diffie-Hellman-Schlüsselvereinbarung, El-Gamal-Systeme und weitere Verfahren. Auch Zero-Knowledge-Protokolle sollen behandelt werden. Neben der reinen Nachrichtenverschlüsselung sollen auch andere Anwendungen behandelt werden, zum Beispiel Signatur-Verfahren, Authentizität von Nachrichten sowie Authentifikation von Kommunikationsteilnehmern.

Unter Kryptoanalyse versteht man die Analyse von kryptographischen Verfahren mit dem Ziel, ihre Sicherheit zu beweisen und zu quantifizieren, oder mit dem Ziel, Schwachstellen

aufzudecken und ggf. Gegenmaßnahmen zu ergreifen. In der Vorlesung "Kryptoanalyse" wird die Kryptoanalyse hauptsächlich von den Verfahren behandelt, mit denen die Studierenden in der Vorlesung "Kryptographie" bereits vertraut gemacht wurden:

- Kryptoanalyse der Enigma als Beispiel zur historischen Kryptographie;
- Kryptoanalyse von RSA (Low-Exponent-Angriffe, Common-Modulus-Angriffe, Angriffe auf das Padding, Faktorisierungsalgorithmen/quadratisches Sieb)
- Kryptoanalyse von Verfahren, die auf dem diskreten Logarithmus in der multiplikativen Gruppe eines endlichen Körpers oder in einer elliptischen Kurve beruhen (Algorithmus von Silver-Polig-Hellman, Rho-Verfahren von Pollard, Baby-Step-Giant-Step-Verfahren von Shanks, Indexcalculus in der multiplikativen Gruppe);
- Die Algorithmen von Shor zur Kryptoanalyse mit dem Quantencomputer;
- Kryptoanalyse von Verfahren, die immun gegen Angriffe mit dem Quanten-Computer zu sein scheinen. Als Beispiel wird das auf linearen Codes beruhende McEliece-Verfahren behandelt.

Neben der Diskussion der theoretischen Grundlagen wird auch auf ganz praxisnahe und konkrete Angriffsszenarien, wie zum Beispiel Logjam oder den Heartbleed-Bug, eingegangen.

Leistungsnachweis

Schriftliche Prüfung mit 60 Minuten Dauer oder mündliche Prüfung mit 30 Minuten Dauer oder Notenschein. Die Prüfungsform wird zu Beginn des Moduls festgelegt.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester.

Modulname	Modulnummer
Anwendungssicherheit	5507

Konto	Pflichtmodule - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. rer. nat. Wolfgang Hommel	Pflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10107	VÜ	Sichere vernetzte Anwendungen	Pflicht	3
55071	VL	Language-based Security	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Gute Kenntnisse in den Bereichen Programmiersprachen, Compiler und systemnahe Programmierung werden vorausgesetzt.

Qualifikationsziele

Es wird die Kompetenz vermittelt, grundlegende Designfehler, weit verbreitete Sicherheitslücken und typische Implementierungsfehler auf Quelltextebene zu erkennen und zu vermeiden. Studierende lernen praxisrelevante Penetration-Testing-Ansätze, ausgewählte wichtige Software-Härtungsmaßnahmen und Bausteine sicherer vernetzter Anwendungen samt ihren betrieblichen Aspekten kennen.

Studierende erwerben fundierte Kenntnisse zu aktuellen Angriffen und Verteidigungstechniken. Behandelte Techniken werden sowohl theoretisch als auch praktisch behandelt, sodass Studierende neben Faktenwissen zu den jeweiligen Techniken auch jene Methodenkompetenzen erwerben, die es ihnen erlaubt, Sicherheitsfragestellungen aus Programmiersprachen-Sicht kompetent zu beantworten.

Inhalt

Die Vorlesung Entwicklung und Betrieb sicherer vernetzter Anwendungen betrachtet Methoden, Konzepte und Werkzeuge zur Absicherung von verteilten Systemen über deren gesamten Lebenszyklus. Anhand von Webanwendungen und anderen serverbasierten Netzdiensten werden zunächst Angreifer-, Bedrohungs- und Trustmodelle sowie typische Design-, Implementierungs- und Konfigurationsfehler und deren Zustandekommen analysiert. Auf Basis dieser Grundlagen wird ein systematisches Vorgehen bei der Entwicklung möglichst sicherer vernetzter Anwendungen erarbeitet. Nach einem Überblick über die Besonderheiten der auf IT-Sicherheitsaspekte angepassten Entwicklungsprozesse werden ausgewählte Methoden und Werkzeuge, u.a. zur statischen bzw. dynamischen Code-Analyse und für Penetration Tests, und ihr Einsatz in den einzelnen Phasen des Softwarelebenszyklus mit den Schwerpunkten

Implementierung und operativer Einsatz vertieft. Am Beispiel von Authentifizierungs- und Autorisierungsverfahren u.a. auf Basis von LDAP, SAML, XACML und OAuth wird die Integration klassischer und moderner Access-Control-Modelle in neu entwickelte Systeme und Legacy-Anwendungen mit ihren betrieblichen Aspekten, u.a. Management und Skalierbarkeit, diskutiert. Nach einem Überblick über aktuelle Härtungs- und Präventionsansätze in Compilern, Betriebssystemen und Libraries werden ausgewählte Ansätze zur Analyse von Exploits und Malware behandelt. Unter dem Stichwort Ethical Hacking werden abschließend Vorgehensweisen bei der Responsible Disclosure identifizierter Schwachstellen diskutiert, die zu einer kontinuierlichen Verbesserung der Sicherheitseigenschaften komplexer Anwendungen führen.

Ziel der Vorlesung Language-based Security ist es, Grundlagen aus der sprach-basierten Sicherheit aus praktischer und theoretischer Sicht zu vermitteln. Konkret wird fundamentales Wissen zu aktuellen Angriffstechniken, z.B. Code-Injection und Code-Reuse Angriffe, vermittelt. Die jeweiligen Angriffstechniken werden danach sukzessive in ihre Bestandteile zerlegt und aus der Perspektive der sprach-basierten Transformationen beleuchtet. Themen der Vorlesung sind:

- Laufzeitstruktur von Programmen auf Maschinenebene
- Angriffe durch Injektion malignen Codes (“code injection attacks”) und deren Abwehr
  - Buffer Overflows und Stack Canaries
  - Control-Flow Hijacking und Control-Flow Integrity
- Angriffe durch Wiederverwendung bereits existierenden Codes (“code re-use attacks”) und deren Abwehr
  - Return-Oriented Programming und Software Diversity
- Angriffe durch Daten
  - Non-Control Data Attacks und Data-Flow Integrity bzw. Data Randomization
- Aktuelle Resultate
  - Theoretische Sicherheit von Control-Flow Integrity
  - Trends in Software Diversity

Leistungsnachweis

Schriftliche Prüfung mit 120 Minuten Dauer oder mündliche Prüfung mit 30 Minuten Dauer oder Notenschein. Die Prüfungsform wird zu Beginn des Moduls festgelegt.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester.

Modulname	Modulnummer
Security- und IT- Management	5508

Konto	Pflichtmodule - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Ulrike Lechner	Pflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	96	144	8

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10106	VÜ	Sicherheitsmanagement	Pflicht	3
10471	VÜ	IT-Governance	Pflicht	5
Summe (Pflicht und Wahlpflicht)				8

Empfohlene Voraussetzungen

Grundlegende Kenntnisse über die Anwendungsbereiche und Methoden der IT-Sicherheit, wie sie z.B. im Modul Grundlagen der Informationssicherheit vermittelt werden.

Qualifikationsziele

Die Studierenden lernen zentrale Fragestellungen und wichtige Instrumente der Organisation, Steuerung und Kontrolle der IT und der IT-Prozesse von Organisationen kennen, in die auch sämtliche operativen Aspekte der Informationssicherheit zu integrieren sind. Sie lernen Fragestellungen und Methoden der Praxis im IT-Management kennen. Sie werden befähigt, Methoden des IT-Managements zu gestalten und zu evaluieren.

Die Vorlesung Sicherheitsmanagement vermittelt die Kompetenz, den Themenkomplex Informationssicherheit in seiner Breite strukturiert und nach technischen und organisatorischen Aspekten differenziert anzugehen und je nach Einsatzszenario systematisch Schwerpunkte im operativen Sicherheitsmanagement zu setzen. Studierende werden in die Lage versetzt, in realistischen Anwendungsbeispielen den Erfüllungsgrad von Anforderungen durch internationale Normen und branchenspezifische Vorgaben zu beurteilen und Maßnahmen zu planen, um identifizierte Defizite zu beseitigen.

Inhalt

Wie kann die IT-Landschaft einer Organisation gestaltet werden? Viele Skandale oder Misserfolge lassen sich auch darauf zurückführen, dass die IT die Unternehmensstrategie nicht richtig umsetzt. Beispielsweise haben fehlende Limits für den Börsenhandel bzw. fehlende Instrumente zur Überwachung der Börsengeschäfte und Durchsetzung dieser Limits Banken und ganze Volkswirtschaften in Bedrängnis bringen können. IT-Sicherheit und Privacy sind weitere zentrale Fragestellungen im IT-Betrieb. Hier müssen

Regeln genauso wie ihre Umsetzung in der Organisation und ihrer IT geklärt sein. Auch moderne Formen des Betriebs der IT, wie IT-Outsourcing oder Cloud Computing können nur dann erfolgreich sein, wenn die Regeln für den Betrieb der IT klar formuliert, in Verträgen geregelt sind und professionell umgesetzt werden können. Gesetzliche Regelungen stellen sich als schwierig dar und häufig genug „überholt" die Technologie die Regelungen. Man denke hier an die Diskussionen um die Panorama Dienste von Google und Microsoft genauso wie über die sozialen Netzwerke. Heute geben z.B. für die Finanzwirtschaft Basel II und Sarbanes-Oxley Regeln für den Betrieb der IT vor.

IT-Governance ist ein vergleichsweise neues Gebiet der Informatik und Wirtschaftsinformatik, das der zentralen Rolle der IT für Organisationen Rechnung trägt. In diesem Themenfeld gibt es einige zentrale Aufgaben. Die IT mit ihren Prozessen ist so zu gestalten, dass Sie den gesetzlichen Vorgaben entspricht und die Geschäftsstrategie umsetzt. Weitere Aufgaben sind Schaffung von Werten durch IT und die Minimierung von IT-Risiken. IT-Governance soll den Rahmen schaffen, IT-Services effektiv, effizient und sicher zu erbringen. IT-Management soll den Betrieb der IT effektiv und effizient sicherstellen. Dazu müssen Strategien mittels IT umgesetzt werden.

Die Vorlesung Sicherheitsmanagement führt in die organisatorischen und technischen Aspekte des Umgangs mit dem Thema Informationssicherheit in komplexen Umgebungen ein, beispielsweise in Konzernen mit mehreren Standorten und bei organisationsübergreifenden Kooperationen wie Zulieferpyramiden oder internationalen Forschungsprojekten. Auf Basis der internationalen Normenreihe ISO/IEC 27000, die u.a. im Rahmen des IT-Sicherheitsgesetzes auch national stark an Bedeutung gewinnt, und weiterer Frameworks wie COBIT werden die Bestandteile so genannter Informationssicherheits-Managementsysteme (ISMS) analysiert und Varianten ihrer Umsetzung mit den damit verbundenen Stärken und Risiken diskutiert. Neben der Integration vorhandener technischer Sicherheitsmaßnahmen in ein ISMS werden auch die Schnittstellen zu branchenspezifischen Vorgaben, beispielsweise dem Data Security Standard der Payment Card Industry, zum professionellen IT Service Management bei IT-Dienstleistern und zu gesetzlichen Auflagen betrachtet.

Leistungsnachweis
Schriftliche Prüfung mit 60 Minuten Dauer oder mündliche Prüfung mit 30 Minuten Dauer oder Notenschein. Die Prüfungsform wird zu Beginn des Moduls festgelegt.
Dauer und Häufigkeit
Das Modul dauert 2 Trimester.

Modulname	Modulnummer
Grundlagen der Informationssicherheit	3459

Konto	Überkonto Wahlpflicht - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. rer. nat. Wolfgang Hommel	Wahlpflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10101	VÜ	Ausgewählte Kapitel der IT-Sicherheit	Pflicht	3
11432	VÜ	Sicherheit in der Informationstechnik	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Für das Modul werden grundlegende Kenntnisse in folgenden Bereichen benötigt:

- Programmieren und Software Engineering, wie z.B. in den Bachelormodulen "Einführung in die Informatik I/II" und "Objektorientierte Programmierung" vermittelt.
- Rechnernetze, wie z.B. in "Einführung in Rechnernetze" vermittelt.

Qualifikationsziele

Das Absolvieren des Moduls wird Studierenden im Bachelor-Studium, die den Master-Studiengang Cyber-Sicherheit (MCYB) studieren möchten, **dringend** empfohlen. MCYB-Studierende, die das Modul nicht bereits im Bachelor-Studium absolviert haben, müssen es zu Beginn des Master-Studiengangs verpflichtend belegen.

Studierende erhalten einen Einblick in die verschiedenen Aspekte der IT-Sicherheit und sind in der Lage, die Bedeutung und Zusammenhänge verschiedener technischer und organisatorischer Einflussfaktoren auf die IT-Sicherheit zu verstehen. Mit den erworbenen Kenntnissen können die Studierenden systematische Bewertungen des Schutzbedarfs und des Sicherheitsniveaus moderner IT-Systeme und IT-Infrastrukturen vornehmen, in die auch in der Praxis häufig noch unterschätzte nicht-technische Faktoren einfließen.

Inhalt

Das Modul führt in die Grundlagen der Informations- und IT-Sicherheit ein und gibt dabei einen breiten Überblick über die Teildisziplinen der Informationssicherheit.

Die Lehrveranstaltung "Sicherheit in der Informationstechnik" umfasst klassische Methoden der technischen und organisatorischen Informationssicherheit, u.a.

- Bedrohungen und Gefährdungen, Risikoanalysen
- Security Engineering
- Grundlagen der angewandten Kryptographie
- Sicherheitsmodelle
- Grundlagen von
  - Netzsicherheit
  - komponentenorientierter Sicherheit
  - Systemsicherheit
  - Anwendungssicherheit
  - Softwaresicherheit

Die Lehrveranstaltung "Ausgewählte Kapitel der IT-Sicherheit" vertieft einige Aspekte der Informationssicherheit mit hoher praktischer Relevanz u.a. anhand von Fallbeispielen und Lösungsansätzen aus der Forschung; die behandelten Themen umfassen u.a.:

- Security Incident Response mit Breach- und Malware-Analyse
- Social Engineering: Faktor Mensch in der Informationssicherheit
- Stolperfallen bei angewandter Kryptographie

Leistungsnachweis

Schriftliche Prüfung (60 Min.) oder mündliche Prüfung (20 Min.) oder Notenschein gemäß Fachprüfungsordnung. Die konkrete Prüfungsform wird zu Beginn in den Lehrveranstaltungen des Moduls bekanntgegeben.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester und wird jeweils im WT für Master-Studierende und im FT für Bachelor-Studierende angeboten.

Sonstige Bemerkungen

Das Modul wird derzeit üblicherweise inhaltsgleich zweimal pro Jahr, im WT und im FT, angeboten. Es ist dabei im WT für Masterstudierende (zum Beginn des Masterstudiums) und im FT für Bachelorstudierende (BINF-/WINF-Wahlpflichtmodul gemäß Musterstudienplan im FT des zweiten Studienjahres) gedacht. Die Teilnahme ist selbstverständlich auch im jeweils anderen Trimester möglich, allerdings kann bei der Termin- und Raumplanung keine Rücksicht auf Überschneidungen mit anderen Mastermodulen (im FT) bzw. Bachelormodulen (im WT) genommen werden.

Modulname	Modulnummer
Einführung in das Industrial Engineering	1008

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Oliver Rose	Wahlpflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10081	VL	Produktionsmanagement in der Fertigung	Pflicht	3
10082	VL	Ressourceneinsatzplanung für die Fertigung	Pflicht	3
10083	P	Praktikum Produktionsplanung und -steuerung	Pflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Vorausgesetzt werden grundlegende Kenntnisse in Modellierung und Simulation sowie grundlegende Programmierkenntnisse.

Qualifikationsziele

Die Studierenden kennen die wichtigsten Fragestellungen und Lösungsansätze bei der Planung und dem Betrieb großer Fertigungsanlagen und können ausgewählte Probleme durch die erlernten Methoden eigenständig lösen. Sie sind mit den grundlegenden Strukturen und Abläufen der Produktion vertraut und sind in der Lage, die Probleme durch Modelle zu beschreiben und anschließend problemspezifische Werkzeuge wie z.B. Fabriksimulatoren einzusetzen oder Lösungsansätze in einer geeigneten Software zu implementieren.

Inhalt

Das Modul führt in die grundlegenden Verfahren des Industrial Engineering ein. Es werden zahlreiche Methoden zur Fabrikplanung und - steuerung behandelt, um die grundlegenden Problemstellungen beim Aufbau und Betrieb von Produktionsanlagen sowie die zugehörigen Lösungsansätze kennenzulernen. Die Fragestellungen orientieren sich an komplexen Massenfertigungsanlagen, wie z.B. in der Halbleiterindustrie, sowie komplexen personalintensiven Montageanlagen, wie z.B. im Flugzeugbau.
In der Vorlesung zum Produktionsmanagement werden die wichtigsten Industrial-Engineering-Verfahren behandelt und zahlreiche Faktoren diskutiert, die bei Fertigungsanlagen zu Leistungsverlusten führen können. In den Übungen werden die Fragestellungen und die Lösungsansätze mit Hilfe von industrietypischen Simulationsmodellen untersucht.

Die Vorlesung zur Ressourceneinsatzplanung behandelt die grundlegenden Verfahren zur Planung von Ressourcen (Mitarbeiter, Maschinen, Transportmittel, ...) bei einem gegebenen Produktionsumfeld und einer zu optimierenden Zielfunktion (z.B. Minimierung der Lieferterminabweichung). Es werden die für die Lösung der Probleme üblicherweise genutzten Algorithmen vorgestellt. Neben den Verfahren für optimale Lösungen werden auch zahlreiche Heuristiken dargestellt. Das Praktikum dient zur Vertiefung der Methodenkenntnisse aus den beiden Vorlesungen an einer aktuellen Forschungsfragestellung.
Leistungsnachweis
Mündliche Prüfung von 30 min.
Verwendbarkeit
Da ein Großteil der Informatiker in der Industrie zum Einsatz kommt, sind grundlegende Kenntnisse über Produktionsanlagen, deren typische Problemstellungen bei Planung und Betrieb sowie die typischen Modellierungsansätze für diese Anlagen von eminenter Bedeutung.
Dauer und Häufigkeit
Das Modul dauert 2-3 Trimester. Das Modul beginnt jedes Studienjahr jeweils im Wintertrimester.

Modulname	Modulnummer
Softwareentwicklungsumgebungen	1034

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Mark Minas	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	60	120	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10122	VÜ	Software-Entwicklungsumgebungen	Wahlpflicht	3
10342	SE	Seminar Ausgewählte Kapitel der Software-Entwicklung	Pflicht	2
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

Vorausgesetzt werden grundlegende Kenntnisse in der Programmierung sowie des Software Engineerings, wie sie in den Bachelormodulen "Objektorientierte Programmierung" und "Einführung in die Praktische Informatik" vermittelt werden.

Qualifikationsziele

Die Studierenden erhalten einen Überblick über Verfahren, Hilfsmittel und Werkzeuge, die sie bei der Realisierung von Software-Projekten unmittelbar einsetzen können. Dadurch verstehen sie die Vorteile der Werkzeugnutzung in der Software-Entwicklung und werden in die Lage versetzt, sich in den Gebrauch weiterer Verfahren, Hilfsmittel und Werkzeuge selbständig einzuarbeiten.

Inhalt

In diesem Modul ergänzen Studierende ihre Kenntnisse, die sie in den einführenden Modulen zur Programmierung und zum Software Engineering erhalten haben. Sie lernen Methoden und Werkzeuge kennen, die in der professionellen Software-Entwicklung eingesetzt werden und die den Software-Entwicklungsprozess vereinfachen sowie verbessern. Dazu gehören Werkzeuge zur Unterstützung der Versions- und Konfigurationsverwaltung sowie die Unterstützung des Build- und Testprozesses.
Zur Beherrschung aufwendiger Software-Entwicklungsaufgaben werden Methoden der komponentenorientierten Softwareentwicklung (OSGi) und die Nutzung von (modellbasierten) Code- und Textgeneratoren behandelt. Als Beispiel einer Integrationsplattform dienen Eclipse und seine Erweiterungsmöglichkeiten.
In der Vorlesung lernen die Studierenden die Methoden und Werkzeuge kennen, in den Übungen werden sie in praktischen Beispielen eingesetzt. Die Studierenden bearbeiten in Gruppen mehrere kleine Projekte, in denen sie Erfahrungen in der Nutzung der Methoden und Werkzeuge sammeln.

Im Seminar erarbeiten die Teilnehmer selbständig Kenntnisse zu vertieften und speziellen Themen im Themenumfeld der Software-Entwicklungsumgebungen. In der Regel arbeitet jeder Teilnehmer einen Vortrag zu vorgegebener Literatur aus, präsentiert ihn in der Gruppe und erstellt eine Seminararbeit.
Leistungsnachweis
Ein Notenschein für Leistungen in der Vorlesung, den Übungen mit den bearbeiteten Projekten und im Seminar.
Verwendbarkeit
Die in diesem Modul vermittelten Kenntnisse und Fertigkeiten werden von jedem Software-Entwickler erwartet. Sie lassen sich unmittelbar in der Bachelor- und der Master-Arbeit anwenden.
Dauer und Häufigkeit
Das Modul dauert 1 Trimester. Das Modul beginnt jedes Studienjahr normalerweise im Herbsttrimester.

Modulname	Modulnummer
Erweiterte Digitale Forensik	1162

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. rer. nat. Harald Baier	Wahlpflicht	4

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
11621	VL	Erweiterte Digitale Forensik (Vorlesung)	Pflicht	3
11622	UE	Erweiterte Digitale Forensik (Übung)	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Das Modul 5505 muss bestanden sein und das Modul 3824 soll bestanden sein. Die Studierenden müssen mit den Grundlagen der IT-Forensik vertraut sein, insbesondere mit IT-forensisch relevanten Spuren und deren Analyse auf Datenträger- und Dateisystemebene.

Qualifikationsziele

Die Studierenden erwerben fortgeschrittene Kenntnisse und Fähigkeiten zur Durchführung einer IT-forensischen Untersuchung. Dazu gehören weitergehende Themen wie Hashfunktionen und Approximate Matching zur Erkennung bzw. Wiedererkennung von Artefakten, fortgeschrittene Dateisystemanalyse am Beispiel ext4, Linux-Analyse und fortgeschrittene Hauptspeicheranalyse.

Inhalt

Die Studierenden lernen fortgeschrittene Betriebssystemforensik am Beispiel von Linux kennen und arbeiten insbesondere mit Linux-Artefakten. Weiterführende Betrachtungen zur Sicherung und Analyse des Hauptspeichers werden mittels des Linux-Betriebssystems und des Frameworks Volatility behandelt. Weiterhin wird der Einsatz von kryptographischen sowie ähnlichkeitserhaltenden Hashfunktionen zur automatisierten (Wieder-)erkennung von Datenstrukturen betrachtet. Im Kontext der Dateisystemforensik wird ein aktuelles Dateisystem analysiert, beispielsweise ext4 wegen seiner Bedeutung für Android. Weiterhin wird ein aktuelles Themengiebt (z.B. Mobilfunkforensik, Netzwerkforensik, Automotive Forensik) bearbeitet.

Leistungsnachweis

Notenschein: Die Übung muss bestanden werden (unbenotete Prüfungsvorleistung). Die Prüfungsleistung ist eine mündliche Prüfung.

Verwendbarkeit
Die im Modul vermittelten Techniken der digitalen Forensik sind in der Beweissicherung und der Zuordnung von Vorfällen im digitalen Zeitalter unerlässlich. Die gelernte Methodik lässt sich auf bisher unbekannte IT-forensische Fragestellungen übertragen.
Dauer und Häufigkeit
Das Modul dauert ein Trimester und beginnt jedes Jahr im WT.

Modulname	Modulnummer
Data Mining und IT- basierte Entscheidungsunterstützung	1231

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Stefan Pickl	Pflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	60	120	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
12311	VÜ	Data Mining und IT-basierte Entscheidungsunterstützung	Pflicht	5
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

Grundkenntnisse zu mathematischen Methoden des Operations Research und der Statistik wie sie z.B. im Bachelor Informatik bzw. Wirtschaftsinformatik vermittelt werden.

Qualifikationsziele

Lernziele sind das kompetente Beherrschen grundlegender Verfahren und Methoden sowie ihrer praktischen Anwendung in den unter Inhalte dargestellten Bereichen.

Inhalt

Die Studierenden sollen in dieser Veranstaltung mit den IT-basierten und entscheidungstheoretischen Grundlagen im Bereich der modernen Datenanalyse vertraut gemacht werden; insbesondere im Hinblick auf die Strukturierung von Entscheidungsproblemen, die Entwicklung von geeigneten Analyseverfahren zur Erforschung von komplexen datenbasierten Zusammenhängen ("Exploratory Analysis"). Data Mining bedeutet dabei das Extrahieren von impliziten, noch unbekannten Informationen aus Rohdaten. Dazu sollten IT-Systeme in die Lage versetzt werden, Datenbanken und Datenansammlungen (z.B. im Bereich der Geoinformatik) automatisch nach Gesetzmäßigkeiten und Mustern zu durchsuchen und einen Abstraktionsprozess durchzuführen, der als Ergebnis aussagekräftige Informationen liefert. Insbesondere das heutige maschinelle Lernen und das Verfahren des "Datafarming" stellen dafür die Werkzeuge und Techniken zur Verfügung, die in den Bereich des modernen Wissensmanagements (bis zur Begriffsanalyse) und "Datamining" hineinführen.

Literatur

- Decision Support Systems Developing Web-Enabled Decision Support Systems, Abhijit A. Pol and Ravindra K. Ahuja. Dynamic Ideas 2007.
- Exploratory Data Analysis Making Sense of Data: A Practical Guide to Exploratory Data Analysis and Data Mining, Glenn J. Myatt. John Wiley, 2006.
- Spatial Data Analysis Spatial Data Analysis - Theory and Practice, Robert Haining, Cambridge University Press 2003.

- Data Mining Data Mining: Practical Machine Learning Tools and Techniques (Second Edition) Ian H. Witten, Eibe Frank. Morgan Kaufmann 2005.
- Data Mining: A Knowledge Discovery, K. Cios, W. Pedrycz, R. Swiniarski Springer, 2007.
- Data Mining Introductery and Advanced Topics, Margaret Dunham, Prentice Hall, 2003.
- Advances in Knowledge Discovery and Data Mining, U. Fayyad, G. Piatetsky-Shapiro, P. Smyth, R. Uthurusamy, editors , MIT Press, 1996.
- Data Mining: Concepts and Techniques, Jiawei Han, Micheline Kamber. Morgan Kaufmann, 2006.
- Principles of Data Mining, David J. Hand, Heikki Mannila and Padhraic Smyth. MIT Press, 2000. Daniel T. Larose,
- Discovering Knowledge in Data: An Introduction to Data Mining, John Wiley 2004. Robert Nisbet, John Elder, IV and Gary Miner.
- Handbook of Statistical Analysis and Data Mining Applications. Elsevier 2009.
- Statistical Learning - Machine Learning Trevor Hastie, Robert Tibshirani, Jerome Friedman,
- The Elements of Statistical Learning: Data Mining, Inference, and Prediction, Springer Verlag, 2001. Mehmed Kantardzic, Data Mining: Concepts, Models, Methods, and Algorithms, Wiley-IEEE Press, 2002.

Weiterführende Literatur:

- Zeitreihenanalyse Time Series Analysis. Hamilton 1994.
- Reinforcement Lernen und Spieltheorie Reinforcement Learning: An Introduction. Sutton and Barto: MIT Press 1998.
- Fun and Games: A Text on Game Theory. Binmore, Linster, Houghton Mifflin 2000.
- Statistik Bayesian Data Analysis. Gelman, Carlin, Stern, Rubin: Chapman 1995. Introduction to Mathematical Statistics. Hogg, Craig: Prentice Hall 2004.
- Principles of Statistics. Bulmer: Dover 1979.
- Probability, Random Variables and Stochastic Proc., Papoulis, McGraw, Hill 2002.

Leistungsnachweis

Mündliche (20min) oder schriftliche (60min) Modulprüfung.

Verwendbarkeit

Die Vorlesung kann durch weiterführende Veranstaltungen im Bereich der Datenanalyse fortgeführt werden, z.B. im Bereich der modernen Begriffsanalyse, des Algorithmic Engineering, im Rahmen von Spezialvorlesungen der Numerik und Statistik sowie der Geoinformatik. Ebenfalls bestehen enge Bezüge zu wissenschaftlichen Forschungsgebieten im Bereich der Künstlichen Intelligenz.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester.
Das Modul beginnt jedes Studienjahr jeweils im Wintertrimeste

Modulname	Modulnummer
Web Technologies	1306

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Michael Koch	Wahlpflicht	6

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	36	144	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
11901	VÜ	Web Technologies	Pflicht	3
Summe (Pflicht und Wahlpflicht)				3

Empfohlene Voraussetzungen
Voraussetzung für das Modul ist die Kenntniss von Grundlagen zu Rechnernetzen, wie sie z.B. in der entsprechenden Veranstaltung im Bachelor-Studium Informatik vermittelt werden.
Qualifikationsziele
Die Veranstaltung vermittelt die Grundlagen und praktische Kenntnisse der verschiedenen Techniken und Werkzeuge des World Wide Web (WWW).
Inhalt
In diesem Modul werden Techniken und Werkzeuge des World Wide Web (WWW) theoretisch und praktisch durch den Einsatz in Fallstudien und Projekten (Teil des Selbststudiums) vermittelt. Dabei werden je nach Ausrichtung sowohl aktuell verbreitete Technologien und Werkzeuge (z.B. HTML, CSS, Ajax, WordPress, ...) als auch neue Technologien und Werkzeuge wie z.B. des Semantik Web (z.B. RDF, Ontologien, ...) oder des Mobile Web (z.B. Mobile-Ajax, ...) betrachtet.
Leistungsnachweis
Notenschein (für vorlesungsbegleitende Leistungen) oder schriftliche Prüfung im Umfang von 60 Minuten.
Dauer und Häufigkeit
Das Modul dauert 1 Trimester.Das Modul startet normalerweise im Frühjahrstrimester, wird aber nicht jedes Studienjahr angeboten.
Sonstige Bemerkungen
Das Modul ist identisch mit dem gleichnamigen Wahlpflichtmodul im Master - kann also entweder im Bachelor oder im Master belegt werden.

Modulname	Modulnummer
Middleware und mobile Cloud Computing	1398

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Andreas Karcher	Pflicht	0

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	60	120	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
13981	VL	Middleware und mobile Cloud Computing	Pflicht	3
13982	UE	Middleware und mobile Cloud Computing	Pflicht	2
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

Vorausgesetzt werden Kenntnisse aus dem Bereich des Software Engineering, insbesondere der Objektorientierung (Modul Objektorientierte Programmierung) sowie der XML-Technologien.

Wünschenswert sind Grundkenntnisse in einer der objektorientierten Programmiersprache, wie z. B. Java, Scala, C++.

Qualifikationsziele

Das Modul Middleware und mobile Cloud Computing zielt darauf ab, den Studierenden vertiefend die Bedeutung der Integration als Kernaufgabe der Angewandten Informatik näher zu bringen. Die Teilnehmer erhalten neben einem grundlegenden Verständnis für die

Anforderungen an eine Middleware-basierte Integration tiefe theoretische Kenntnisse über Architektur, Aufbau und Anwendung aktueller Middlewarekonzepte. Zudem werden querschnittlich Aspekte von verteilten Systemen in diesem Zusammenhang betrachtet.

Im Übungsteil lernen die Teilnehmer parallel zur Vorlesung den praktischen Umgang mit Middleware-Technologien und Cloud-basierten, mobilen Anwendungen. Durch eigenständige Anwendung von unter anderem Remote Method Invocation (RMI), Common Object Request Broker Architecture (CORBA), .NET und Simple Object Access Protocol (SOAP) erhalten die Teilnehmer Methoden- und Fachkompetenz im Umgang mit diesen Technologien.

In der Kombination aus theoretischer Behandlung und praktischer Vertiefung versetzt das Modul die Teilnehmer in die Lage, verteilte Anwendungen auf der Basis von Middleware zu entwerfen und in die Praxis umzusetzen.

Inhalt
Moderne Enterprise Anwendungen basieren auf Standard-Middleware-Architekturen, wo Funktionalität zunehmend über Cloud-basierte Dienste plattformübergreifend den Clients # mehr und mehr auch mobilen Endgeräten # zur Verfügung gestellt wird. Das Modul bietet einen fundierten Einstieg in die aktuellen Basistechnologien. Hierbei wird das Wissen aus dem Modul der objektorientierten Programmierung um die fachwissenschaftliche Denkweise der Entwicklung von verteilten Anwendungen erweitert. Nach einer grundlegenden Einführung in die Integrationsanforderungen zunehmend verteilt strukturierter, internet-basierter betrieblicher Anwendungen vermittelt das Modul zunächst einen Überblick über die Grundarchitektur Middleware-basierter Systeme und geht dann im Folgenden tiefer auf die unterschiedlichen Integrationsparadigmen und -technologien ein. Aktuelle Middlewaredienste und Architekturkonzepte wie Verteilte Objektmodelle, Komponentenmodelle und Service Oriented Middleware (SOA) bilden den Schwerpunkt des zweiten Teils des Moduls. Hier werden jeweils zunächst die allgemeinen Prinzipien erläutert und dann anhand konkreter Beispiele Standard-Middleware-Technologien und deren zugrunde liegenden Konzepte vertieft. Der dritte Teil stellt das Cloud-Konzept in den Mittelpunkt und zeigt Schritt für Schritt an einfachen Beispielen die Entwicklung Cloud-basierter Dienste und deren Zugriff über mobile Clients (Apps). Die begleitende Übung bietet die Gelegenheit, aktuelle Technologien anhand einfacher Beispiele kennen zu lernen und erste praktische Erfahrung im Umgang mit Middleware und mobilen, Cloud-basierten Anwendungen zu sammeln.
Lehrmethoden
Das Modul unterteilt sich in eine Vorlesung und eine Übung pro Woche. Es werden sowohl Lehrmethoden des fremdgesteuerten als auch des selbstgesteuerten Lernens angewendet. Es wird auf die individuellen Voraussetzungen der Studierenden eingegangen, wobei hauptsächlich ein lehrgangsförmiger und kooperativer Unterricht mit Einzelarbeit stattfindet.
Leistungsnachweis
Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer. Die Art der Prüfung wird jeweils zu Beginn des Moduls bekannt gegeben.
Verwendbarkeit
Die im Wahlpflichtmodul erworbenen Kenntnisse sind elementar für die IT-technische Gestaltung von verteilten Informationssystemen und stellen somit eine Grundlage für

Masterstudiengänge im Bereich Informatik/Wirtschaftsinformatik/Ingenieurinformatik/ Cyber Sicherheit dar.
Dauer und Häufigkeit
Das Modul dauert 1 Trimester. Das Modul beginnt jedes Studienjahr jeweils im Wintertrimester.

Modulname	Modulnummer
Identitätsmanagement	1446

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Dr. rer. nat. Daniela Pöhn	Wahlpflicht	4

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
14461	VÜ	Identitätsmanagement	Pflicht	3
14462	SE	Seminar Identitätsmanagement	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Für das Modul werden grundlegende Kenntnisse in den folgenden Bereichen benötigt:

- Funktionsweise von Webanwendungen, wie sie z.B. in der Lehrveranstaltung Sichere vernetzte Anwendungen behandelt werden.
- IT-Sicherheit, wie sie z.B. in Modul 3459 vermittelt werden.

Qualifikationsziele

Die Studierenden erhalten einen Überblick über Protokolle, Anwendungsbeispiele und Sicherheitsaspekte des Identitätsmanagements. Sie verstehen unterschiedliche Methoden und können die Modelle des Identitätsmanagements anwenden sowie die Protokolle vergleichen. Dadurch sind sie in der Lage, Bedeutung und Zusammenhänge verschiedener Einflussfaktoren auf die IT-Sicherheit und damit der Sicherheit der Identitäten zu analysieren. Mit dem erworbenen Wissen werden die Studierenden in die Lage versetzt, sich tiefergehend selbstständig einzuarbeiten und den Einsatz von Protokollen in verschiedenen Anwendungen zu bewerten.

Inhalt

Das Modul führt in die Grundlagen des Identitätsmanagements und deren Zusammenhang mit IT-Sicherheit ein. Darauf aufbauend bietet es einen breiten Überblick über verschiedene Protokolle des Identitätsmanagements im Webbereich, deren Sicherheit und Anwendungsgebiete. Dieser Überblick wird als Basis für die weitere Betrachtung der Sicherheit, des Security Managements und angrenzende Gebiete verwendet.

Die Vorlesung Identitätsmanagement betrachtet unterschiedliche Protokolle für Identitätsmanagement im Web-Bereich und deren Zusammenspiel mit der Sicherheit. Anhand unterschiedlicher Modelle des Identitätsmanagements werden

die darin enthaltenen Protokollen, u.a. SAML, OAuth, OpenID Connect und User Managed Access, mit deren Rollen, Architekturen, Austauschformaten und mit Hilfe von Verwendungsbeispielen erklärt. Darauf aufbauend wird deren Sicherheit und das Vertrauen in die gesendeten Benutzerinformationen analysiert. Dies beinhaltet typische Design-, Implementierungs- und Konfigurationsfehler sowie Fehler im Design der Protokolle selbst. Nach diesem Grundstock werden unter Einbeziehung von IT-Sicherheit und Security Management Normen, Guidelines, wie NIST SP 800-63, und praktischen Anwendungen, u.a. Vectors of Trust, dessen betrachtet. Abschließend wird ein Überblick über angrenzende Themen, wie Identitäten bei IoT, DNS und IEEE 802.1X, gegeben. Das Seminar Identitätsmanagement vertieft einige Aspekte der Vorlesung mit hoher praktischer Relevanz. Die behandelten Themen umfassen u.a. Security Management beim Identitätsmanagement, Angriffe und Abwehrmechanismen und neue Protokoll-Entwicklungen.
Leistungsnachweis
Schriftliche Prüfung im Umfang von 60 Minuten oder mündliche Prüfung mit 30 Minuten Dauer oder Notenschein. Die Prüfungsform wird zu Beginn des Moduls festgelegt.
Dauer und Häufigkeit
Das Modul dauert zwei Trimester und beginnt jedes Jahr im WT.

Modulname	Modulnummer
Enterprise Architecture und IT Service Management	1507

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Andreas Karcher	Wahlpflicht	0

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	60	120	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
15071	VL	Enterprise Architecture und IT Service Management	Pflicht	3
15072	UE	Enterprise Architecture und IT Service Management	Pflicht	2
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

Empfehlenswert aber nicht zwingend erforderlich sind Grundkenntnisse der Service-orientierten Architektur (SOA), wie sie in der Vorlesung "Wirtschaftsinformatik 3" vermittelt werden.

Qualifikationsziele

Die Regierbarkeit komplexer IT-Landschaften (IT Governance)" wird zunehmend zentraler, strategischer Wettbewerbsfaktor für Unternehmen, Organisationen und nicht zuletzt auch Armeen wie die Bundeswehr. Enterprise Architecture & IT Service Management bilden die beiden zentralen Säulen zur Beherrschung dieser komplexen Aufgabenstellung. Die Teilnehmer werden durch das Modul mit breiter Methodenkompetenz und Fachkenntnis in die Lage versetzt, in dem noch relativ jungen Forschungsgebiet auf dem aktuellen Stand und seiner Bedeutung an der Gestaltung komplexer IT-Landschaften mitzuwirken. In der Vertiefung werden heute dominierende Standards und Best Practices, wie TOGAF, ITIL, UAF und ArchiMate, in Aufbau, Struktur und Domänenbezug verankert und die Grundkenntnisse zu ihrer Anwendung vermittelt. Anhand konkreter Fallbeispiele und Diskussionen mit externen Fachleuten erlangen die Teilnehmer zudem die notwendigen Fähigkeiten zur eigenständigen Anwendung und Übertragung der Methoden und Ansätze in Domänenkontexte.

Inhalt

Das Service-basierte Architekturkonzept (Service Oriented Architecture SOA) bildet seit geraumer Zeit einen wichtigen Grundpfeiler für die Gestaltung und Anpassung komplexer IT-Landschaften an die sich fortlaufend verändernden Anforderungen aus dem Geschäftsprozessumfeld einer Unternehmung oder Organisation. Es gilt, Anforderungen aus den Geschäftsprozessen strukturiert, zielgerichtet und möglichst effektiv und effizient auf Basisdienste einer unterliegenden IT Service-Schicht

abzubilden und diese zum Beispiel in Form von Cloud-basierten Diensten orts- und technologieübergreifend der Anwendungsebene zur Verfügung zu stellen. Rahmenwerke zur Beschreibung der für einen Unternehmenstyp bzw. einen Anwendungsbereich typischen Architekturbestandteile und Zusammenhänge zwischen den #Building Blocks" (Enterprise Architecture Frameworks) bilden eine immer wichtiger werdende Grundlage hierfür.

Das Modul führt die Studierenden in die Thematik der architekturbasierten Gestaltung von komplexen IT-Landschaften ein. Im ersten Teil der Veranstaltung werden zunächst die Entwicklungsgeschichte und die zentrale Grundidee von Unternehmens-rahmenwerken vorgestellt und an einführenden Beispielen diskutiert sowie ein Überblick über entsprechende Standards gegeben. Anhand einzelner ausgewählter Standards wie beispielsweise The Open Group Architecture Framework (TOGAF) werden dann einzelne Aspekte der Anwendung von Enterprise Architecture selbstständig an Fallbeispielen vertieft.

Im zweiten Teil des Moduls steht das Management komplexer IT-Landschaften auf Basis der Service-orientierten Architektur im Mittelpunkt. IT Service Management als Überbegriff aller Ansätze und Methoden zur Unterstützung bei der Abbildung von Geschäftsprozessen auf IT-Basisdienste bildet einerseits ein wichtiges Fundament heutiger IT-Governance. Andererseits stellt dieses Paradigma Unternehmen und Anwender vor die Herausforderung einer fortwährenden, systematischen und möglichst optimalen Abbildung der Unternehmensprozesse auf IT-Bausteine und Standard-Anwendungssysteme - auch als Business-IT-Alignement bezeichnet. Hierbei spielen Standards und Rahmenwerke - allen voran die IT Infrastructure Library (ITIL) - eine zentrale Rolle. Neben der Verankerung der grundlegenden Konzepte und Methoden des IT Service Managements wird den Studierenden anhand von Praxisbeispielen gespiegelte Anwendung der Rahmenwerke vermittelt. Die praktische Anwendung dieser zu erlernenden Fähigkeiten steht im Mittelpunkt des Moduls. Anwendungsexperten aus unterschiedlichen Bereichen, z. B. aus Automobilkonzernen, werden zusätzlich tiefere Einblicke in den aktuellen Stand der Handhabung geben.

Lehrmethoden

Das Modul unterteilt sich in eine Vorlesung und eine Übung pro Woche.

Es werden sowohl Lehrmethoden des fremdgesteuerten als auch des selbstgesteuerten Lernens angewendet.

Es wird auf die individuellen Voraussetzungen der Studierenden eingegangen, wobei hauptsächlich ein lehrgangsförmiger und kooperativer Unterricht mit Einzelarbeit stattfindet.

Leistungsnachweis

Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer oder leistungsbezogener Notenschein.

Die Art der Prüfung wird jeweils zu Beginn des Moduls bekannt gegeben.
Verwendbarkeit
Das Wahlpflichtmodul ist die Grundlage für weiterführende und vertiefende Veranstaltungen sowie wissenschaftliche Arbeiten im Kontext der Gestaltung und Anpassung komplexer IT-Landschaften. Es stellt Basiswissen für den Masterstudiengänge Wirtschaftsinformatik, aber auch im Bereich Informatik/ Ingenieurinformatik/Cyber Sicherheit dar und ergänzt sich mit den Wahlpflichtmodulen für "Middleware und mobile Cloud Computing".
Dauer und Häufigkeit
Das Modul dauert 1 Trimester. Das Modul beginnt jedes Studienjahr jeweils im Wintertrimester.

Modulname	Modulnummer
Formale Entwicklung korrekter Software	1518

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
PD Dr. Birgit Elbl Univ.-Prof. Dr.-Ing. Markus Siegle	Wahlpflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	60	120	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
15171	VÜ	Entwurf Verteilter Systeme	Wahlpflicht	5
15172	VÜ	Methoden und Werkzeuge	Wahlpflicht	5
15174	VÜ	Spezifikation	Wahlpflicht	5
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

Vorausgesetzt werden die im Bachelor-Studium erworbenen Grundkenntnisse und Fertigkeiten in diskreter Modellierung (elementare Logik und Mengenlehre), systematischer Programmentwicklung und Theoretischer Informatik. Für den "Entwurf verteilter Systeme" wird darüber hinaus Vertrautheit mit Grundlagen der Architektur und dem Entwurf von Rechen- und Kommunikationssystemen erwartet.

Qualifikationsziele

Die Studierenden erhalten einen Überblick über die wichtigsten Methoden und Werkzeuge für die formale Entwicklung korrekter Software, von der Spezifikation bis hin zum Entwurf verteilter Systeme. Sie erwerben die Kompetenz, diese im Entwurfsprozess gewinnbringend einzusetzen, d.h. einschlägige Verfahren und Werkzeuge auszuwählen und effizient anzuwenden.

Inhalt

Ein Schwerpunkt der Vorlesung "Spezifikation" sind abstrakte Datentypen, bei denen sowohl die initiale Semantik, als auch lose Spezifikationen behandelt werden. Den Studierenden werden Ansätze zur Strukturierung und zum schrittweisen Aufbau von Spezifikationen vorgestellt. Sie sehen Beispiele für die schrittweise Entwicklung von programmnahen aus rein deskriptiven Spezifikationen. Sie lernen die Kernbegriffe Verfeinerung, Erweiterung und abstrakte Implementierung kennen und deren Rolle bei der Entwicklung von Spezifikationen. Beispiele sind u.a. den Bereichen Spezifikation komplexer Datenstrukturen und zustandsorientierte Spezifikation sequentieller Systeme entnommen. Den Abschluss bildet eine kurze Einführung in die temporale Spezifikation nebenläufiger Systeme.

In der Vorlesung "Entwurf verteilter Systeme" werden formale Methoden vorgestellt, mit deren Hilfe die Struktur und das dynamische Verhalten von komplexen verteilten (oder allgemeiner ausgedrückt: nebenläufigen) Systemen spezifiziert werden kann. Wir behandeln insbesondere die beiden Spezifikationsformalismen Petrinetze und Prozessalgebren, und diskutieren ihre mathematischen Eigenschaften und die darauf aufbauenden Analyseverfahren.

Weiterhin behandeln wir die Frage nach der Formalisierung von Anforderungen an ein solches verteiltes System, wobei sich temporale Logiken als wertvolle Hilfsmittel erweisen. Es wird gezeigt, wie man mit der Methode des Model Checking komplexe, temporal spezifizierte Anforderungen automatisch überprüfen kann.

Neben den Verifikationsalgorithmen für die weit verbreitete Logik CTL werden Erweiterungen in Richtung von Realzeiteigenschaften angesprochen. In den Übungen erhalten die Studierenden auch Gelegenheit, entsprechende Software-Werkzeuge kennenzulernen und selbst zu erproben.

Die Vorlesung "Methoden und Werkzeuge" macht die Studierenden mit Systemen zur modellbasierten Spezifikation von Software (wie JCL, OCL und Z) bekannt. Fallstudien werden vorgestellt, von den Studierenden ergänzt und auf Konsistenz untersucht, wobei sie u.a. Methoden und Werkzeuge des Model Checking (z.B. Alloy) einzusetzen lernen.

Die Studierenden befassen sich mit der systematischen Herleitung korrekter Software, entweder durch Programmtransformation oder durch zielgerichtete Programmherleitung (z.B. mit VDM). Sie lernen, mit Hilfe von Werkzeugen (wie Spark) die Korrektheit von Software praktisch nachzuweisen. Dazu bearbeiten sie in Übungen und Hausaufgaben auch über Spielbeispiele hinausgehende Fallstudien.

Leistungsnachweis

Das Modul wird per Notenschein geprüft. Es ist eine der drei Vorlesungen (mit Übung) zu belegen.

Verwendbarkeit

Bei sicherheitskritischer Software ist Korrektheit das wichtigste Qualitätskriterium. Modellbasiertes, formales Vorgehen ist für den Entwurf moderner, komplexer Systeme (sowohl Software als auch Hardware) unerlässlich. Daher ergänzen die hier erworbenen Kenntnisse und Fertigkeiten die Ausbildung im Bereich der Softwaretechnik um einen Aspekt von hoher praktischer Bedeutung.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester.

Sonstige Bemerkungen

Jedes Jahr wird mindestens eine Vorlesung (mit Übung) angeboten, so dass 6 ECTS-Punkte erreichbar sind. Jeweils zu Beginn des Masterstudiums wird den Studierenden das konkrete Angebot erläutert.

Modulname	Modulnummer
Digitale Forensik	1551

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. rer. nat. Harald Baier	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
15511	VL	Digitale Forensik (VL)	Pflicht	3
15512	UE	Digitale Forensik (UE)	Pflicht	3
15513	SE	Seminar Ausgewählte Themen der digitalen Forensik	Pflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Das Modul 5505: Systemsicherheit muss bestanden sein. Die Studierenden müssen mit den Grundlagen der IT-Forensik vertraut sein, insbesondere mit IT-forensisch relevanten Spuren und deren Analyse auf Datenträger- und Dateisystemebene.

Qualifikationsziele

Die Studierenden kennen die allgemeine IT-forensische Vorgehensweise und können diese bei der Durchführung IT-forensischer Analysen anwenden sowie in einem Gutachten dokumentieren. Sie kennen wichtige Spurenquellen im Betriebssystem Windows und können diese auswerten. Die Studierenden kennen Datenformate von verbreiteten Anwendungen und können diese analysieren. Sie wissen Sicherungs- und Analyseverfahren des Hauptspeichers und können diese anwenden. Wesentliche Anti-Forensik-Ansätze sind den Studierenden bekannt, und sie können diese bewerten. Weiterhin können die Studierenden Speichertechnologien erklären und digitale Spuren eingebetteter Systeme IT-forensisch sichern und auswerten.

Inhalt

Die Studierenden lernen die Betriebssystemforensik am Beispiel von Windows kennen und arbeiten insbesondere mit der Windows-Registry sowie Windows-Artefakten. Im Kontext der Anwendungsforensik wird das SQLite Datenbankformat behandelt und für Anwendungen wie Firefox, Thunderbird, Skype analysiert. Die Sicherung und Analyse des Hauptspeichers wird mittels des Windows-Betriebssystems und des Frameworks Volatility behandelt. Auf dem Gebiet der Anti-Forensik lernen die Studierenden die gängigen Kategorien von antiforensischen Maßnahmen kennen und bewerten. Flashbasierte Speichertechnologien sowie der direkte Zugriff auf einen Datenträger und die zugehörige Auswertung sind low-level Fertigkeiten, die die Studierenden einsetzen.

An Hand der Erstellung eines Gutachtens für ein Fallbeispiel werden die gelernten Inhalte praktisch und umfassend geübt. Im Seminar erarbeiten die Teilnehmer selbständig Kenntnisse zu vertieften und speziellen Themen auf dem Gebiet der digitalen Forensik. Jeder Teilnehmer gibt eine Seminararbeit im LNCS-Format ab und präsentiert diese. Es findet auch ein Peer-Review der eingereichten Seminararbeiten statt.
Leistungsnachweis
Notenschein: Die Übung und das Seminar müssen bestanden werden (unbenotete Prüfungsvorleistung). Die Prüfungsleistung ist die Erstellung eines Gutachtens an Hand bereitgestellter Images. Weitere Details zu den Prüfungsleistungen werden zu Beginn des Moduls bekannt gegeben.
Verwendbarkeit
Die im Modul vermittelten Techniken der digitalen Forensik sind in der Beweissicherung und der Zuordnung von Vorfällen im digitalen Zeitalter unerlässlich. Die gelernte Methodik lässt sich auf bisher unbekannte IT-forensische Fragestellungen übertragen.
Dauer und Häufigkeit
Das Modul dauert 2 Trimester.

Modulname	Modulnummer
Language-based Security	3584

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Stefan Brunthaler	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
35841	P	Praktikum Language-based Security	Pflicht	4
35842	SE	Seminar Language-based Security	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Von den Studierenden werden Kenntnisse in der maschinennahen Programmierung und in sprachbasierter Sicherheit vorausgesetzt, wie sie z.B. in den gleichnamigen Bachelor- und Master-Veranstaltungen vermittelt werden.

Qualifikationsziele

Die Studierenden erwerben die Fähigkeit, Probleme der sprachbasierten Sicherheit in der Praxis zu analysieren und sich durch geeignete Implementierungen von Prototypen kritisch mit der Materie auseinanderzusetzen. Dabei sollen die Studenten durch mehrere Varianten verschiedene "Härtegrade" der Verteidigungstechniken illustriert und dadurch Kompetenz bei der Bewertung der relativen Vor- und Nachteile in der Anwendung der Techniken erworben werden.

Inhalt

Im Rahmen des Praktikums werden zu den jeweiligen Themengebieten der Vorlesung "Language-based Security" konkrete Implementierungen von Prototypen in einem kleinen, aber repräsentativen Compiler durchgeführt. Um die Effizienz der Verteidigungstechniken zu messen, werden bei Bedarf vorher Angriffe implementiert und diese dann mit Hilfe der implementierten Verteidigungen abgewehrt. Studenten sollen dabei auch den Effekt der Verteidigung für den Angreifer verstehen und abschätzen lernen.

Beispielsweise werden folgende Verteidigungstechniken implementiert:

1. Stack Canaries in verschiedenen Varianten, plus Code Injection via Buffer Overflows.
2. Bounds Checking in verschiedenen Varianten.

3. Code-Reuse Angriffe und Verteidigungen:
   1. Software Diversity in voller Breite und Tiefe:
      - NOP Insertion
      - Equivalent Instruction Substitution
      - Register Assignment Randomization
      - Basic Block Randomization
      - Function Permutation
      - Data Randomization

   2. Control-Flow Integrity in verschiedenen Varianten.

4. Spectre Angriffe und Verteidigungen.

Das Seminar widmet sich aktuellen Themen der sprachbasierten Sicherheit und je nach Interesse auch dem weiteren Gebiet der Software- und Systemsicherheit.

Leistungsnachweis
Notenschein.
Dauer und Häufigkeit
Das Modul dauert ein Trimester.

Modulname	Modulnummer
Compilerbau	3647

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Stefan Brunthaler	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
36471	VL	Compilerbau	Pflicht	2
36472	UE	Compilerbau	Pflicht	4
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Von den Studierenden werden Kenntnisse in der maschinennahen Programmierung vorausgesetzt, wie sie z.B. in der gleichnamigen Bachelorveranstaltung vermittelt werden.

Qualifikationsziele

Studierende erwerben fundierte Kenntnisse sowohl über theoretische Grundlagen des Compilerbaus, als auch deren praktische Anwendung zur systematischen, Werkzeug-unterstützten Erstellung von Compilern.

Inhalt

Die Vorlesung Compilerbau orientiert sich am Buch "Essentials of Compilation" von Prof. Siek an der Indiana University, Bloomington. Es wird ein Compiler erstellt, der schrittweise eine Untermenge von Scheme bzw. Racket nach Intel x86-64 übersetzt. Dabei wird die Untermenge von Scheme didaktisch optimal ebenfalls schrittweise um zusätzliche Fähigkeiten erweitert, die dann wiederum eine Änderung der einzelnen Übersetzungsschritte nach sich zieht.

Der Fokus der Vorlesung liegt daher mehr auf dem Thema Codegenerierung, im Speziellen, Register Allokation, Instruction Selection und Peephole Optimization. Das Thema Typ-Überprüfung wird ebenfalls ausführlich behandelt.

Leistungsnachweis

Schriftliche Prüfung 120 Minuten oder Notenschein.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester.

Modulname	Modulnummer
Compilerbau (erweitert)	3648

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Stefan Brunthaler	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
36471	VL	Compilerbau	Pflicht	2
36472	UE	Compilerbau	Pflicht	4
36481	P	Praktikum Compilerbau	Pflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Von den Studierenden werden Kenntnisse in der maschinennahen Programmierung vorausgesetzt, wie sie z.B. in der gleichnamigen Bachelorveranstaltung vermittelt werden.

Qualifikationsziele

Studierende erwerben fundierte Kenntnisse sowohl über theoretische Grundlagen des Compilerbaus, als auch deren praktische Anwendung zur systematischen, Werkzeug-unterstützten Erstellung von Compilern.

Inhalt

Die Vorlesung Compilerbau orientiert sich am Buch "Essentials of Compilation" von Prof. Siek an der Indiana University, Bloomington. Es wird ein Compiler erstellt, der schrittweise eine Untermenge von Scheme bzw. Racket nach Intel x86-64 übersetzt. Dabei wird die Untermenge von Scheme didaktisch optimal ebenfalls schrittweise um zusätzliche Fähigkeiten erweitert, die dann wiederum eine Änderung der einzelnen Übersetzungsschritte nach sich zieht.

Der Fokus der Vorlesung liegt daher mehr auf dem Thema Codegenerierung, im Speziellen, Register Allokation, Instruction Selection und Peephole Optimization. Das Thema Typ-Überprüfung wird ebenfalls ausführlich behandelt.

Das Praktikum Compilerbau vertieft die Kenntnisse des Compilerbaus und bietet folgende Erweiterungen des in der VL & UE erstellten Compilers:

1. Fokus Syntax: Erstellen eines einfachen Frontends anhand des Buchs "Beautiful Racket" fuer eine einfache Untermenge von Pascal. Diese Untermenge von Pascal soll auf die vom Compiler unterstützte Untermenge von Racket abgebildet werden.

2. Fokus Optimierung: Erstellen eines einfachen, automatischen Instruction Selection Mechanismus basierend auf KURS Baumgrammatiken und Baumautomaten.
3. Fokus Sicherheit: Implementierung aufwändigerer und vollständigerer Verteidigungen aus dem Bereich sprachbasierter Sicherheit.

Die Richtungen können in Zweier-Gruppen bearbeitet werden und abschließend nach einer Präsentation vor allen Teilnehmern besprochen.

Leistungsnachweis
Notenschein.
Dauer und Häufigkeit
Das Modul dauert 2 Trimester.

Modulname	Modulnummer
Benutzbare Sicherheit	3665

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Florian Alt	Wahlpflicht	4

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
36651	VÜ	Benutzbare Sicherheit	Pflicht	3
36653	P	Praktikum Design sicherer und benutzbarer Systeme	Pflicht	3
3665-V1	VÜ	Sichere Mensch-Maschine Schnittstellen	Pflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Für die Teilnahme an diesem Modul werden Grundkenntnisse in der Informatik und in der Programmierung vorausgesetzt. Insbesondere Erfahrung mit Android und Web-Programmierung sind von Vorteil. Hilfreich sind außerdem Grundkenntnisse in der Mensch-Maschine Interaktion. Folgende Literatur kann zur Vorbereitung dienen:

- Butz, Andreas, and Antonio Krüger. Mensch-Maschine-Interaktion. Walter de Gruyter GmbH & Co KG, 2017.
- Cranor, Lorrie Faith, and Simson Garfinkel. Security and usability: designing secure systems that people can use. O'Reilly Media, Inc., 2005.
- Lazar, Jonathan, Jinjuan Heidi Feng, and Harry Hochheiser. Research methods in human-computer interaction. Morgan Kaufmann, 2017.
- Oates, Briony J. Researching information systems and computing. Sage, 2005.

Qualifikationsziele

In diesem Modul erlernen die Teilnehmer die Fähigkeit, sich beim Design sicherer Systeme kritisch mit dem Faktor „Mensch“ auseinanderzusetzen. Insbesondere wird ein Verständnis für Anforderungen solcher Systeme hinsichtlich ihrer Sicherheit aber auch ihrer Benutzbarkeit geschaffen.

Den Studierenden werden Grundlagen der Mensch-Maschine Interaktion und der benutzbaren Sicherheit (Grundbegriffe, Sicherheitsmechanismen, Bedrohungsmodelle) vermittelt. Sie erarbeiten sich tiefgehende, methodische Kenntnisse, welche es ihnen ermöglichen, Konzepte und Systeme zu entwickeln und hinsichtlich ihrer Sicherheit und Benutzbarkeit zu evaluieren. Basierend auf dem theoretischen Grundlagen- und

Methodenwissen wird im praktischen Teil des Moduls die Fähigkeit zur Konzeption und praktischen Umsetzung sicherer und benutzbarer Systeme vertieft.

Inhalt

Technologie kann nicht die alleinige Lösung für Herausforderungen im Bereich IT-Sicherheit sein. Wir sind heute in der Lage, Mechanismen zu schaffen, die aktuell nicht brechbar sind. Trotzdem ist Sicherheit in vielen Bereichen immer noch ein ungelöstes Problem, da viele der von uns entwickelten Systeme und Mechanismen nicht nutzbar sind. Das hat zur Folge, dass Menschen freiwillig oder unfreiwillig Wege finden, solche Mechanismen auszuhebeln. Menschliche Faktoren spielen eine zentrale Rolle in der IT-Sicherheit. Daher ist es wichtig, dass Experten für Benutzbare Sicherheit ein Verständnis dafür entwickeln, wie Menschen mit den von uns entwickelten Systemen interagieren. Dieses Modul führt die Teilnehmer in eine Vielzahl von Herausforderungen in Bezug auf die Benutzerfreundlichkeit und die Sicherheit in ubiquitären Systemen ein. Es vermittelt die theoretischen, methodischen und praktischen Grundlagen für das Design sicherer und benutzbarer Systeme.

Hierfür dienen drei Lehrveranstaltungen:

Sichere Mensch-Maschine-Schnittstellen – Die Veranstaltung vermittelt Grundlagenwissen für die Konzeption, das Design und die Evaluierung benutzbarer und gleichzeitig sicherer Mensch-Maschine-Schnittstellen. Hierfür werden im ersten Teil die Informationsverarbeitung des Menschen (physiologische und psychologische Grundlagen, Modelle, Handlungsprozesse) sowie die technische Realisierung von Benutzungsschnittstellen (Ein- und Ausgabegeräte, Interaktionsstile) behandelt sowie benutzerorientierte Entwurfsprozesse, Richtlinien und Standards für Benutzbarkeit und Sicherheit vorgestellt. Der zweite Teil widmet sich der Evaluation und der Bewertung von Mensch-Maschine Schnittstellen hinsichtlich verschiedener Kriterien. Dies erfordert ein breites Wissen in der Forschungsmethodik. Daher werden verschiedene Studientypen (z.B. deskriptive Studien, relationale Studien, experimentelle Studien), Studienparadigmen (u.a. Ethnographie, Laborstudien, Feldstudien, Deployments) sowie Datenerhebungsmethoden (z.B. Fragebögen, Interviews, Beobachtungen, Experience Sampling und Crowdsourcing) behandelt.

Benutzbare Sicherheit – Diese Vorlesung gibt einen Überblick über Herausforderungen hinsichtlich der Benutzbarkeit sicherer und benutzbarer Systeme. Die Studierenden lernen verschiedene Sicherheits-Mechanismen und mentale Modelle der Benutzer kennen. Zudem erhalten sie eine Einführung in die Modellierung von Bedrohungen. Insbesondere behandelt die Veranstaltung aktuelle Themen der Benutzbaren Sicherheit, unter anderem, Authentifizierung, Passwörter und Social Engineering. Die Lehrveranstaltung richtet sich sowohl an Studierende, die an Sicherheit und Datenschutz interessiert sind und mehrüber Benutzbarkeit erfahren möchten, als auch an Studierende, die an Benutzbarkeit interessiert sind, aber mehr über Sicherheit und Datenschutz erfahren möchten.

Design sicherer und benutzbarer Systeme – Ziel dieses Praktikums ist das Erlernen benutzer-zentrierter Techniken für die Konzeption, das Design und die Umsetzung sicherer und benutzbarer Systeme. Die Teilnehmer dieser Lehrveranstaltung wenden

hierzu einen benutzer-zentrierten Designprozess an. In Gruppen werden neuartige Konzepte erarbeitet. Ausgewählte Konzept werden anschließend prototypisch umgesetzt und mithilfe von Benutzerstudien hinsichtlich Sicherheit und Benutzbarkeit getestet.
Leistungsnachweis
Das Modul wird mit einem Notenschein abgeschlossen.
Dauer und Häufigkeit
Das Modul dauert 2 Trimester und beginnt jedes Jahr im WT.

Modulname	Modulnummer
Quantenkommunikation	3695

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. rer. nat. Wolfgang Hommel	Wahlpflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3695-V1	VÜ	Quantenkommunikation	Pflicht	3
3695-V2	P	Praktikum Quantenschlüsselaustausch	Wahlpflicht	3
3695-V3	SE	Seminar Quantentechnologien	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Grundlegende Kenntnisse in linearer Algebra, komplexen Zahlen sowie Interesse an Quantenphysik und -technologie. Grundwissen über Kryptographie ist hilfreich, aber nicht zwingend erforderlich.

Qualifikationsziele

Verständnis des Quantenschlüsselaustauschs (Quantum Key Distribution, QKD) und seiner mathematischen Modellierung über Zweizustandssysteme. Kenntnisse der wichtigsten Protokolle zum Schlüsselaustausch sowie von Postprocessing-Methoden des Schlüsselmaterials (Privacy Amplification, Quantum Error Correction). Überblick über mögliche Angriffe auf den Quantenschlüsselaustausch sowie Maßnahmen zu deren Abwehr. Verständnis der Herausforderungen bei der technologischen Umsetzung des Quantenschlüsselaustauschs.

Praktisches Verständnis davon, wie der Quantenschlüsselaustausch experimentell umgesetzt werden kann. Überblick über die aktuellen Entwicklungen in im Bereich Quantentechnologien.

Inhalt

Der Quantenschlüsselaustausch ist eine der wichtigsten Quantentechnologien.
Seine Bedeutung entsteht daraus, dass die Sicherheit auf physikalischen Prinzipien beruht, nicht wie bei konventioneller Kryptographie auf Annahmen über den Rechnenaufwand beim Lösen bestimmter mathematischer Probleme. Daher ist der Quantenschlüsselaustausch auch sicher gegenüber Angriffen von Quantencomputern. Dieses Modul bietet eine Einführung in die Theorie und Praxis dieser neuen und spannenden Technologie.

Vorlesung:

- Grundlegender Formalismus der Quantenmechanik für Zweizustandssysteme
- Wichtigste Protokolle zum Quantenschlüsselaustausch (BB84, Ekert91, COW-Protokoll)
- Technologische Umsetzung von Qubits für den Quantenschlüsselaustausch
- Postprocessing-Methoden des Schlüsselmaterials: Error Correction, Privacy Amplification
- Sicherheitsanalysen, Seitenkanäle und Quantum Hacking
- Quantenkommunikationsnetzwerke und Quantenrepeater

Praktikum:

- Durchführung eines QKD-Modellversuchs, der das BB84-Protokoll mit polarisiertem Licht in der Praxis umsetzt
- Detailliertes Wissen über die Schritte, die für ein QKD-Protokoll erforderlich sind
- Experimentelle Durchführung des Protokolls in Teams bestehend aus zwei Personen, die die Rolle von Sender und Empfänger übernehmen
- Versenden einer mit Quantenschlüsseln verschlüsselten Nachricht
- Verfassen eines Versuchsprotokolls

Seminar: Aktuelle Themen in den folgenden Bereichen:

- Verschiedene technologische Realisierungen des Quantenschlüsselaustausches
- Quantum Hacking
- Überblick über bestehende und geplante Quantenkommunikationsnetzwerke
- Ansätze zur Realisierung von Quantenrepeatern
- Standardisierung von Protokollen und Geräten zum QKD-Schlüsselmanagement
- Aktuelle technologische Fortschritte in den Bereichen Quantenmeteorologie, Quantensensoren und Quantencomputern

Leistungsnachweis

Schriftliche Prüfung (60 min) oder mündliche Prüfung (30 min) oder Notenschein. Die Prüfungsform wird zu Beginn des Moduls festgelegt.

Dauer und Häufigkeit

Das Modul wird jedes Jahr ab dem WT angeboten und dauert zwei Trimester. Die Vorlesung wird im WT angeboten, das Praktikum oder das Seminar im FT.

Modulname	Modulnummer
Reverse Engineering	3819

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Johannes Kinder	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
38191	VL	Reverse Engineering	Pflicht	2
38192	P	Reverse Engineering	Pflicht	4
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Von den Studierenden werden Kenntnisse in der maschinennahen Programmierung vorausgesetzt, wie sie z.B. in der gleichnamigen Bachelor-Veranstaltung vermittelt werden.

Grundlagen von Betriebssystemen, wie sie z.B. in der Bachelorvorlesung Einführung in Betriebssysteme vermittelt werden.

Qualifikationsziele

Die Studierenden erwerben die Fähigkeit, passende Werkzeuge und Methoden zur Analyse von geschützten Programmen zu bewerten und auszuwählen, sowie die praktische Fähigkeit, Programme manuell zu analysieren bzw. für eine automatisierte Analyse vorzubereiten. Sie können dabei wiederkehrende Aufgaben identifizieren und geeigneten Mechanismen (z.B. Skripte/Plugins) zur Unterstützung entwickeln. Dies ermöglicht ihnen, in kompilierten Programmen ohne Zugriff auf Quelltext effektiv nach Informationen oder Schwachstellen zu suchen.

Inhalt

Die Vorlesung behandelt aktuelle Themengebiete des Reverse Engineerings, insbesondere relevante Grundlagen, wie Maschinensprache, Disassemblierung, Debugging, und die Semantik von Instruktionen. Ein Schwerpunkt wird auf die Analyse des Kontrollflusses gesetzt, und wie das Verhalten von Code zur Laufzeit vorhergesagt werden kann. Dabei sind sowohl interaktive statische und/oder dynamische Methoden, als auch automatische Methoden von Interesse.

Darüber hinaus beschäftigt sich die Vorlesung mit verschiedenen Schutzmechanismen (Obfuscations), die ein Reverse Engineering verhindern sollen, und effektiven Gegenmaßnahmen. Dies beinhaltet z.B. sog. „Packer“, die verschlüsselte Programme

zur Laufzeit in den Arbeitsspeicher entpacken, sowie „Virtualizer“, die einen zufälligen Interpreter für jedes Programm erzeugen.

Im Praktikum Reverse Engineering lernen die Studierenden, die in der Vorlesung vermittelten Techniken umzusetzen. Hierbei werden verschiedene aktuelle Tools eingesetzt, um komplexe Probleme aus der Praxis eigenständig bzw. in kleinen Teams zu lösen.

Leistungsnachweis
Notenschein oder schriftliche Prüfung mit 60 Minuten Dauer oder mündliche Prüfung mit 20 Minuten Dauer. Die Prüfungsform wird zu Beginn des Moduls festgelegt.
Verwendbarkeit
Die manuelle oder automatisierte Analyse von Programmen mittels Reverse Engineering ist in der praktischen Sicherheitsanalyse von Software in vielen Bereichen unumgänglich.
Dauer und Häufigkeit
Das Modul dauert 1 Trimester.

Modulname	Modulnummer
Quantencomputer in Theorie und Praxis	3820

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
PD Dr. Rupert Hölzl	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
12113	VÜ	Quantencomputer	Pflicht	3
38202	P	Praktikum Quantencomputer-Programmierung	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Generelles Interesse an Mathematik und Theorie. Grundlegende Kenntnisse in Linearer Algebra erforderlich. Grundlegende Python-Kenntnisse sind nützlich, aber nicht zwingend erforderlich.

Qualifikationsziele

Verständnis des theoretischen Modells des Quantencomputers und seiner besonderen Möglichkeiten und Herausforderungen. Verständnis für das Design von Quantenalgorithmen. Praktische Erfahrung im Implementieren dieser Algorithmen.

Inhalt

In der Vorlesung wird das Modell des Quantencomputers vorgestellt. Seit Jahrzehnten gibt es nämlich die Hoffnung, dass man durch Ausnutzen von quantenmechanischen Vorgängen Computer bauen kann, die bestimmte Berechnungsprobleme schneller lösen können als herkömmliche Computer. Zuerst werden einige mathematische Grundlagen gelegt, und es wird eine kurze Einführung in die notwendigen Begriffe der Quantenmechanik gegeben. Dann wird das Modell des Quantencomputers eingeführt, und es werden verschiedene Algorithmen für Quantencomputer behandelt, unter anderem der Algorithmus von Grover und der berühmte Faktorisierungalgorithmus von Shor. Auch komplexitätstheoretische Aspekte werden besprochen.

Das Praktikum bietet Gelegenheit zum Experimentieren mit ausgewählten Quantenalgorithmen, die in der Vorlesung präsentiert wurden. Für einfache Experimente wird der webbasierte Circuit Composer aus der IBM Q Experience demonstriert. Für komplexere Experimente kommt die Softwarebibliothek Qiskit für Python3 zum Einsatz. Dabei wird sowohl die Verwendung von Scripts auf der Kommandozeile als auch die

komfortablere Nutzung von Jupyter Notebooks gezeigt. Tests laufen auf dem lokalen Rechner, in der IBM-Cloud zur Simulation, oder auf einem echten Quantencomputer. Darüberhinaus wird die Beschreibungssprache OpenQASM für Quantenschaltkreise vorgestellt.
Leistungsnachweis
Notenschein: Das Praktikum muss erfolgreich absolviert werden. Zur Vorlesung findet eine mündliche (30 Min.) oder schriftliche (60 Min.) Prüfung statt. Die genauen Prüfungsmodalitäten werden zu Beginn des Moduls festgelegt.
Dauer und Häufigkeit
Das Modul wird alle zwei Jahre angeboten und dauert zwei Trimester.

Modulname	Modulnummer
Statische Programmanalyse	3838

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Johannes Kinder	Wahlpflicht	4

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	84	96	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
38381	VÜ	Statische Programmanalyse	Pflicht	4
38382	P	Praktikum Statische Programmanalyse	Pflicht	3
Summe (Pflicht und Wahlpflicht)				7

Empfohlene Voraussetzungen

Vorausgesetzt werden Grundkenntnisse der mathematischen Logik wie sie im Bachelor vermittelt werden. Darüber hinaus sind für das Praktikum Kenntnisse in funktionalen Programmiersprachen (z.B. Scala) hilfreich, aber nicht notwendig.

Qualifikationsziele

Die Studierenden kennen die wichtigsten Konzepte und Techniken aus dem Bereich der statischen Programmanalyse. Sie erwerben ein Verständnis der mathematischen Grundlagen sowie der Chancen und Grenzen dieser Verfahren. Sie sind ebenso in der Lage, einfache statische Analysen selbst umzusetzen.

Inhalt

Statische Programmanalysen sind in modernen Entwicklungsprozessen ein häufig eingesetztes Werkzeug zur automatischen Fehlersuche. Ursprünglich hauptsächlich im Bereich der sicherheitskritischen Software verwendet, findet man kommerzielle Tools zunehmend als Teil von Continuous-Integration Plattformen. Viele führende Softwarefirmen beschäftigen mittlerweile Teams, die angepasste Software für die statische Analyse der eigenen Code-Basis entwickelt und pflegt.

Statische Programmanalyse bezeichnet Verfahren, die automatisch Software untersuchen, um bestimmte Eigenschaften zu überprüfen oder automatisch Fehler zu finden. Dabei wird die Software nicht ausgeführt, sondern ausschließlich der Programmcode (Quelltext oder Maschinensprache) betrachtet. Die zu Grunde liegende Idee ist, mit Hilfe von mathematischen Verfahren die Semantik des Programms zu approximieren, und so Fehler und Schwachstellen auszuschließen oder zu finden.

Die Vorlesung Statische Programmanalyse gibt einen Überblick über die relevanten Grundlagen und stellt dann ausgewählte Anwendungen vor. Abgedeckte Themen sind unter anderem:

- Automatische Fehlersuche
- Datenflussanalyse
- Kontrollflussanalyse
- Pointeranalyse
- Abstrakte Interpretation

Im begleitenden Praktikum Statische Programmanalyse lernen die Studierenden, Techniken der statischen Analyse selbst für eine einfache Programmiersprache zu implementieren.

Leistungsnachweis
Notenschein

Verwendbarkeit
Statische Programmanalysen sind weit verbreitet, Einsatzgebiete sind unter anderem die automatische Fehlersuche zur Entwicklungszeit, Security Audits von binärer Third-Party Software, Compileroptimierungen und Unterstützung und Automatisierung innerhalb von Entwicklungsumgebungen.

Dauer und Häufigkeit
Das Modul dauert ein Trimester.

Modulname	Modulnummer
Dynamische Programmanalyse	3849

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Johannes Kinder	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	84	96	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
38491	VÜ	Dynamische Programmanalyse	Pflicht	4
38492	P	Praktikum Fuzzing	Pflicht	3
Summe (Pflicht und Wahlpflicht)				7

Empfohlene Voraussetzungen

Von den Studierenden werden Kenntnisse in der maschinennahen Programmierung vorausgesetzt, wie sie in der gleichnamigen Bachelor-Veranstaltung vermittelt werden. Kenntnisse in der Programmiersprache Python sind hilfreich, aber nicht notwendig.

Qualifikationsziele

Die Studierenden kennen verschiedene Konzepte und Werkzeuge der dynamischen Programmanalyse. Dies beinhaltet das Verständnis verschiedener Verfahren zur automatischen Suche nach Fehlern, insbesondere des automatischen Fuzz Testings. Sie können verschiedene Techniken aus diesen Bereichen umsetzen und ihre Vor- und Nachteile abwägen.

Inhalt

Dynamische Programmanalysen bezeichnen zusammenfassend Verfahren, die automatisch Software zur Laufzeit untersuchen um Informationen über das Programmverhalten zu bekommen, wie z.B. welche Eingaben zu Programmabstürzen führen, oder ob die Software vertrauliche Informationen ausgeben kann. Dynamische Programmanalysen basieren teils auf Zufallsverfahren, teils auf logischer Charakterisierung der Eingaben. Sie werden in der Praxis eingesetzt um Fehler und Schwachstellen in Software zu verhindern oder zu erkennen.

Die Vorlesung behandelt unter anderem die folgenden Themen und Techniken:

- Fuzzing (Mutation-based, Grammar-based)
- Coverage Feedback
- Taint Tracking
- Binary Instrumentation
- Symbolic Execution

Im Praktikum Fuzzing lernen die Studierenden den Stand der Technik und praktische Herausforderungen im Fuzztesting kennen. Als Teil des Praktikums wenden die Studenten bestehende Systeme an und entwickeln auch einen eigenen Fuzzer und eigene Teststrategien. In vielen Fällen wird Eigenrecherche und Autodidaktik zur Lösung der Aufgaben notwendig sein.
Leistungsnachweis
Notenschein
Verwendbarkeit
Dynamische Programmanalyse und Fuzzing sind in der Praxis weit verbreitet und werden ergänzend zur manuellen Analyse von Programmen eingesetzt.
Dauer und Häufigkeit
Das Modul dauert ein Trimester.

Modulname	Modulnummer
Cryptography Engineering	5519

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Cornelius Greither	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
12111	VÜ	Algorithmische Zahlentheorie	Pflicht	5
12112	VÜ	Ausgewählte mathematische Methoden in Kryptographie und Codierungstheorie	Wahlpflicht	3
55191	VÜ	Post-Quantum Kryptographie	Wahlpflicht	3
55192	P	Implementierung und Anwendung kryptographischer Verfahren	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Grundlagen zur Kryptographie und Kryptoanalyse, wie sie z.B. im Modul Kryptologie vermittelt werden.

Qualifikationsziele

Die Studierenden erlernen fortgeschrittene Konzepte und Algorithmen der Kryptographie und können ihr Wissen im Bereich der Kryptographie in Gebieten ihrer Wahl vertiefen. Dies können algebraische Methoden für den Entwurf von kryptographischen Verfahren oder kryptoanalytischen Verfahren sein oder Algorithmen im Bereich der Quantencomputer sowie Verfahren, die auch bei Verwendung von Quantencomputern noch sicher sind. Auch praktische Erfahrungen bei der Implementierung von kryptographischen Verfahren und von Analyse-Verfahren werden vermittelt.

Inhalt

Die Veranstaltung "Algorithmische Zahlentheorie" befasst sich mit grundlegenden Begriffen und Algorithmen der algebraischen Zahlentheorie. (Stichworte: Primelemente, Primalitätstests, Faktorisierung, elliptische Kurven, u.a.). Ein Großteil dieser abstrakten Konzepte ist fundamental für die moderne Kryptographie (Public Key) und die Codierungstheorie. Der Schwerpunkt dieser Vorlesung ist zwar die systematische Erarbeitung der theoretischen Grundlagen und grundlegenden Algorithmen, es wird aber auch immer wieder auf Anwendungen eingegangen. Ergänzt werden diese durch zahlentheoretische Konzepte, die eventuell in einer Post-Quantencomputer-Epoche relevant sein könnten.

Die Veranstaltung "Ausgewählte mathematische Methoden der Kryptographie und Codierungstheorie" befasst sich mit ausgewählten und fortgeschrittenen Themen aus der Kryptographie und/oder der Codierungstheorie. Hierhin gehören kryptographische Verfahren, die auf zahlentheoretischen Ergebnissen aufsetzen, und "gute" Codes, die man mit Hilfe von algebraischen Kurven gefunden hat. Sowohl kryptographische als auch codierungstheoretische Inhalte sind vorgesehen; die Gewichtung zwischen diesen beiden Gebieten kann aber variieren.

Ein sehr wichtiges theoretisches Resultat von Peter Shor besagt, dass man mit Hilfe von Quantencomputern schnell große Zahlen faktorisieren kann und damit viele der heutzutage häufig verwendeten kryptographischen Verfahren brechen kann.
In der Vorlesung mit Übungen "Post-Quantum Kryptographie" soll zuerst dieses Resultat mit den notwendigen Grundlagen vorgestellt werden. Dann sollen einerseits quantenkryptographische Verfahren präsentiert werden und andererseits Verfahren, die sogar gegen Angriffe mit Hilfe von Quantencomputern resistent sind. Genannt seien: gitterbasierte Verfahren, codebasierte Verfahren, Hash-Verfahren und Verfahren, die auf multivariaten Polynomen basieren.

In dem Praktikum "Implementierung und Anwendung kryptographischer Verfahren" werden verschiedene kryptographische und kryptoanalytische Verfahren implementiert. Dabei werden auch verschiedene Anwendungsbereiche abgedeckt, z.B. Verschlüsselung von Nachrichten, Signatur-Verfahren, Authentizität von Nachrichten, Authentifikation von Kommunikationsteilnehmern sowie für diese Probleme geeignete Protokolle. Es werden auch Analyse-Verfahren und mögliche Angriffe auf kryptographische Protokolle implementiert und durchgespielt.

Leistungsnachweis

Schriftliche Prüfung mit 60 Minuten Dauer oder mündliche Prüfung mit 30 Minuten Dauer oder Notenschein. Die Prüfungsform wird zu Beginn des Moduls festgelegt.

Dauer und Häufigkeit

Das Modul dauert 1-2 Trimester.

Sonstige Bemerkungen

Es ist entweder die Vorlesung "Algorithmische Zahlentheorie" und eine der anderen Veranstaltungen zu belegen; oder die beiden anderen Vorlesungen und das Praktikum. Je nach Kombination der Veranstaltungen, ergibt sich die TWS-Summe 8 bzw. 9.

Modulname	Modulnummer
Offensive Sicherheitsüberprüfungen	5523

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Arno Wacker	Wahlpflicht	4

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55091	VÜ	Penetration Testing	Pflicht	6
55093	P	Penetration Testing	Pflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Gute Kenntnisse in den Bereichen Netzsicherheit und Systemsicherheit, wie in den gleichnamigen beiden Modulen vermittelt.

Qualifikationsziele

Die Studierenden können organisationsinterne Überprüfungen der IT-Sicherheitseigenschaften von Systemen, Diensten und Netzen planen und durchführen. Sie beherrschen Testmethoden auf Netz-, Anwendungs- und Systemebene und haben ausgewählte aktuelle Werkzeuge für diesen Zweck kennengelernt. Sie kennen die Aufgabenbereiche und Randbedingungen von Red Teams und Pentesting-Dienstleistern.

Inhalt

Die Vorlesung Penetration Testing führt in die Aufgabengebiete von Pentesting- bzw. Red-Teams ein. Für verschiedene Anwendungsgebiete wie das Sicherheitstesten einzelner Systeme, komplexerer IT-Dienste und ganzer Rechnernetze und IT-Infrastrukturen werden die Vor- und Nachteile verschiedener Testvarianten wie Whitebox- und Blackbox-Tests analysiert. Unter Orientierung an bewährten Good-Practice-Dokumentationen wie OWASP und OSSTMM werden praxisrelevante Angriffsvarianten von der Reconnaissance-Phase bis zum Einbringen von Exploit-Payloads behandelt. Ebenso werden die strukturierte Erstellung von Pentesting-Berichten und deren Auswertung durch die auftraggebende Organisation betrachtet.

Das Praktikum Penetration Testing stellt auf Basis einer Praktikumsinfrastruktur (abgeschottete Laborumgebung) Aufgaben, in denen die Studierenden als fiktiver Auftragnehmer eines technischen Penetrationstests fungieren. Mithilfe ausgewählter bereitgestellter Softwarewerkzeuge müssen die für Pentests ausgewählten Systeme, Dienste und Subnetze erkundet und auf verschiedenste Verwundbarkeiten untersucht

werden, ohne den Betrieb der übrigen Infrastruktur zu beeinträchtigen. Für einige Überprüfungen müssen eigene Werkzeuge bzw. Skripte/Payloads konzipiert und implementiert werden. Über die gewählte Vorgehensweise, die einzelnen Schritte der Durchführung und die zu priorisierenden Ergebnisse ist eine Ausarbeitung zu erstellen, die vom Stil her an Pentest-Berichte angelehnt ist.
Leistungsnachweis
Notenschein
Dauer und Häufigkeit
Das Modul dauert 1-2 Trimester.

Modulname	Modulnummer
Einführung in das Industrial Engineering	1008

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Oliver Rose	Wahlpflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10081	VL	Produktionsmanagement in der Fertigung	Pflicht	3
10082	VL	Ressourceneinsatzplanung für die Fertigung	Pflicht	3
10083	P	Praktikum Produktionsplanung und -steuerung	Pflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Vorausgesetzt werden grundlegende Kenntnisse in Modellierung und Simulation sowie grundlegende Programmierkenntnisse.

Qualifikationsziele

Die Studierenden kennen die wichtigsten Fragestellungen und Lösungsansätze bei der Planung und dem Betrieb großer Fertigungsanlagen und können ausgewählte Probleme durch die erlernten Methoden eigenständig lösen. Sie sind mit den grundlegenden Strukturen und Abläufen der Produktion vertraut und sind in der Lage, die Probleme durch Modelle zu beschreiben und anschließend problemspezifische Werkzeuge wie z.B. Fabriksimulatoren einzusetzen oder Lösungsansätze in einer geeigneten Software zu implementieren.

Inhalt

Das Modul führt in die grundlegenden Verfahren des Industrial Engineering ein. Es werden zahlreiche Methoden zur Fabrikplanung und - steuerung behandelt, um die grundlegenden Problemstellungen beim Aufbau und Betrieb von Produktionsanlagen sowie die zugehörigen Lösungsansätze kennenzulernen. Die Fragestellungen orientieren sich an komplexen Massenfertigungsanlagen, wie z.B. in der Halbleiterindustrie, sowie komplexen personalintensiven Montageanlagen, wie z.B. im Flugzeugbau.
In der Vorlesung zum Produktionsmanagement werden die wichtigsten Industrial-Engineering-Verfahren behandelt und zahlreiche Faktoren diskutiert, die bei Fertigungsanlagen zu Leistungsverlusten führen können. In den Übungen werden die Fragestellungen und die Lösungsansätze mit Hilfe von industrietypischen Simulationsmodellen untersucht.

Die Vorlesung zur Ressourceneinsatzplanung behandelt die grundlegenden Verfahren zur Planung von Ressourcen (Mitarbeiter, Maschinen, Transportmittel, ...) bei einem gegebenen Produktionsumfeld und einer zu optimierenden Zielfunktion (z.B. Minimierung der Lieferterminabweichung). Es werden die für die Lösung der Probleme üblicherweise genutzten Algorithmen vorgestellt. Neben den Verfahren für optimale Lösungen werden auch zahlreiche Heuristiken dargestellt. Das Praktikum dient zur Vertiefung der Methodenkenntnisse aus den beiden Vorlesungen an einer aktuellen Forschungsfragestellung.
Leistungsnachweis
Mündliche Prüfung von 30 min.
Verwendbarkeit
Da ein Großteil der Informatiker in der Industrie zum Einsatz kommt, sind grundlegende Kenntnisse über Produktionsanlagen, deren typische Problemstellungen bei Planung und Betrieb sowie die typischen Modellierungsansätze für diese Anlagen von eminenter Bedeutung.
Dauer und Häufigkeit
Das Modul dauert 2-3 Trimester. Das Modul beginnt jedes Studienjahr jeweils im Wintertrimester.

Modulname	Modulnummer
Simulationstechnik	1033

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Oliver Rose	Wahlpflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	96	174	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10244	P	Praktikum Modellbildung und Simulation	Wahlpflicht	4
10331	VÜ	Parallele und verteilte Simulation	Pflicht	3
10332	VÜ	Entscheidungsunterstützende Modellbildung und Simulation	Wahlpflicht	3
10333	VÜ	Moderne Heuristiken	Wahlpflicht	3
10334	VÜ	Verifikation und Validierung von Modellen	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				7

Empfohlene Voraussetzungen

Grundlegende Kenntnisse zu Wahrscheinlichkeitstheorie und Statistik sowie zu Simulation, wie sie beispielsweise in den entsprechenden Modulen im Bachelor Informatik oder Master Informatik vermittelt werden.

Qualifikationsziele

Ziel der Lehrveranstaltungen dieses Moduls ist es, den Studierenden - auf der Basis profunder Kenntnisse der Simulation im Allgemeinen - spezielle Techniken aus den Gebieten parallele und verteilte Simulation, heuristische Optimierungsverfahren, Verifikation und Validierung sowie Entscheidungsunterstützungsverfahren zu vermitteln. Insbesondere sollen die Studierenden dabei lernen, wie sie komplexe Simulationsmodelle durch diese besonderen Techniken verbessern können, um Probleme zu lösen, die rein analytisch oder mit Standardmethoden nicht mehr beherrschbar sind.

Inhalt

In den Lehrveranstaltungen dieses Moduls werden Kenntnisse der Computersimulation unter besonderer Berücksichtigung spezieller Modellierungsziele und Verwendungszwecke in der Praxis methodisch vertieft. Dabei handelt es sich um:

- die verteilte oder parallele Ausführung von Simulationsmodellen auf mehreren Prozessoren oder Rechnern aus Gründen der Erhöhung der Leistungsfähigkeit oder auch der Zuverlässigkeit (Parallele und verteilte Simulation),

- Maßnahmen zur Sicherstellung der Glaubwürdigkeit, Gültigkeit und Qualität von Modellen und deren Ergebnissen hinsichtlich eines bestimmten Verwendungszwecks (Verifikation und Validierung von Modellen),
- Vorgehensweisen, Paradigmen und Methoden zum Einsatz von Simulation als Hilfsmittel zur Entscheidungsfindung, welche meist unter Annahmen über die Realsysteme zu erfolgen hat und zu Ergebnissen führen muss, die dem Anwender plausibel erscheinen (Entscheidungsunterstützende Modellbildung und Simulation),
- heuristische Verfahren, die zur Optimierung von Simulationsergebnissen und Eingabeparameter insbesondere bei komplexen Modellen unverzichtbar geworden sind (Moderne Heuristiken).

Im Praktikum sollen gegebenenfalls einzelne dieser Methoden im Rahmen eines Beispiels umgesetzt werden.

Leistungsnachweis

Schriftliche Prüfung von 60 Minuten oder mündliche Prüfung von 30 Minuten.

Verwendbarkeit

Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit auf den durch die Module adressierten speziellen Feldern der Modellbildung und Simulation. Zudem sind die Inhalte des Moduls erfahrungsgemäß von besonderer Bedeutung, wenn in der beruflichen Praxis komplexe Simulationsmodelle zum Einsatz kommen.

Dauer und Häufigkeit

Das Modul dauert 3 Trimester.
Das Modul beginnt jedes Studienjahr jeweils im Wintertrimester.
Als Startzeitpunkt ist das Wintertrimester im 1. Studienjahr vorgesehen.

Sonstige Bemerkungen

Neben der Pflichtveranstaltung sind entweder zwei Wahlpflichtveranstaltungen oder das Praktikum zu wählen. Je nach Kombination der Veranstaltungen, ergibt sich die TWS-Summe 7 bzw. 9.

Modulname	Modulnummer
Knowledge Discovery in Big Data	1144

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. phil. Michaela Geierhos	Wahlpflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
11441	VÜ	Knowledge Discovery	Wahlpflicht	3
11442	VÜ	Methoden der Data Science	Wahlpflicht	3
11443	SE	Research Topics in Data Science	Wahlpflicht	3
11444	VÜ	Big Data Management	Wahlpflicht	3
11445	SE	Datenethik und -sicherheit	Wahlpflicht	3
11446	P	Data Science Praktikum	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Die Studierenden sollen grundlegende Kenntnisse in Programmierung und Software-Entwurf sowie ein Grundverständnis von Algorithmen und Datenstrukturen haben.

Qualifikationsziele

Lernziele sind das kompetente Beherrschen grundlegender Verfahren und Methoden sowie ihrer praktischen Anwendung in den unter Inhalte dargestellten Bereichen.

Inhalt

- In der Vorlesung „Big-Data-Management“ lernen die Studierenden Architekturen kennen, die für die Erfassung, Verarbeitung und Analyse von Big Data konzipiert sind, wofür sich herkömmliche Datenbanksysteme nicht mehr eignen. In diesem Zusammenhang wird nicht nur die verteilte Big-Data-Infrastruktur behandelt, sondern auch Themen wie Datenstrukturierung, Datensynchronisation/Parallelität und Speicherverwaltung in den Fokus gerückt. In der Übung werden erste Erfahrungen mit Big-Data-Architekturen gemacht.
- In der Vorlesung „Knowledge Discovery“ geht es um den Umgang mit heterogenen Datenquellen, deren Kategorisierung sowie deren Analyse. Hierfür werden Methoden wie u.a. Visual Analytics/Knowledge sowie Techniken des Discovery & Data Mining und die explorative Datenanalyse unter Zuhilfenahme von KI-Methoden wie z. B. Machine Learning oder Computational Intelligence vorgestellt und in den Übungen praktisch vertieft.
- In der Vorlesung „Methoden der Data Science” werden grundlegende Konzepte und Methoden entlang eines Data Science Projektzyklus, von der Formulierung der

Problemstellung über die Sammlung, Vorbereitung und Visualisierung der Daten bis hin zur Erkennung von Mustern und Trends in diesen mittels Verfahren des maschinellen Lernens (z. B. Regression, Klassifikation, Clustering) vermittelt. Das erlernte Methodenwissen wird kontinuierlich durch praxisnahe Übungen mit der Programmiersprache Python angewandt und vertieft.

- Im Seminar „Research Topics in Data Science“ werden ausgewählte, aktuelle Methoden aus dem Bereich Data Science, Machine Learning und Deep Learning vorgestellt. Das Seminar soll den Studierenden einen Einblick in State-of-the-Art Forschungsthemen geben. Die behandelten Themen orientieren sich am aktuellen Gartner Hyper Cycle for Artificial Intelligence (wie bspw. Decision Intelligence, Responsible AI, Knowledge Graphs) und dem Gartner Hype Cycle for Emerging Technologies (wie bspw. Self-Supervised Learning, Explainable AI, Social Data).
- Im Seminar „Datenethik und -sicherheit“ werden u.a. Fragen der Datenethik diskutiert, um einen kritischen und verantwortungsvollen Umgang mit Daten und dem daraus gewonnenen Wissen zu erlernen. Behandelt werden ethische und legale Fragen in Bezug auf AI- und Data Science-Anwendungen, welche einen großen Einfluss auf die Gesellschaft haben (z. B. autonomes Fahren, Social Media Plattformen, Tools zur medizinischen und juristischen Entscheidungsfindung). Ferner lernen die Studierenden, wie man AI- und Data Science-Applikationen kontrolliert anwendet, um der Gesellschaft und individuellen Personen zu nutzen, und möglichen Schaden in Bezug auf Datensicherheit und Datenschutz zu vermeiden. In der Übung soll das Wissen zu ethischen Implikationen genutzt werden, um Strategien und Konzepte für ethische Anwendungen zu entwickeln.
- Im „Data Science Praktikum” wir das in der Theorie gelernte Wissen in einem Projekt praktisch implementiert. Die Studierenden werden in Kleingruppen an einem größeren Projekt im Bereich Data Science arbeiten und dies am Ende des Trimesters präsentieren. Das Projekt umfasst dabei einen gesamten Projektzyklus – von der Idee und Konzeption, über die Datensammlung und deren Aufbereitung bis hin zum Tainieren eines Machine Learning-Modells und Auswertung der Ergebnisse. Das Plenum bietet dabei einen regelmäßigen Austausch und Feedback zwischen den Gruppen. Themen der Projekte beziehen sich auf die kennengelernten Forschungsbereiche aus „Research Topics in Data Science“ und „Methoden der Data Science“. Es wird dringend empfohlen einen der o.g. Kurse besucht zu haben.

Leistungsnachweis

Das gesamte Modul wird per Notenschein geprüft, mit Anteilen von je 3 ECTS-LP zu jeder der Vorlesungen (mit Übung), zu jedem Seminar und im Praktikum. Die Studierenden können (je nach Angebot) entweder zwei Vorlesungen mit Übungen oder zwei Seminare oder eine Vorlesung mit Übung und ein Praktikum oder eine Vorlesung mit Übung und ein Seminar einbringen – was insgesamt die 6 ECTS-LP des Moduls ergibt.

Verwendbarkeit

Die hier erworbenen Kenntnisse und Fertigkeiten ergänzen die Ausbildung im Bereich der Softwaretechnik um einen Aspekt von hoher praktischer Bedeutung. Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit im Bereich Data Science.

Dauer und Häufigkeit

Das Modul dauert 2 bis 3 Trimester und beginnt jedes Jahr im FT.

Sonstige Bemerkungen
Die Vorlesungen, Seminare und das Praktikum werden nicht alle jedes Jahr angeboten, aber in jedem Jahr mindestens so viele Lehrveranstaltungen, dass 6 ECTS-Leistungspunkte erreichbar sind. Jeweils zu Beginn des Moduls wird den Studierenden das konkrete Angebot erläutert.

Modulname	Modulnummer
Web Technologies	1306

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Michael Koch	Wahlpflicht	6

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	36	144	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
11901	VÜ	Web Technologies	Pflicht	3
Summe (Pflicht und Wahlpflicht)				3

Empfohlene Voraussetzungen
Voraussetzung für das Modul ist die Kenntniss von Grundlagen zu Rechnernetzen, wie sie z.B. in der entsprechenden Veranstaltung im Bachelor-Studium Informatik vermittelt werden.
Qualifikationsziele
Die Veranstaltung vermittelt die Grundlagen und praktische Kenntnisse der verschiedenen Techniken und Werkzeuge des World Wide Web (WWW).
Inhalt
In diesem Modul werden Techniken und Werkzeuge des World Wide Web (WWW) theoretisch und praktisch durch den Einsatz in Fallstudien und Projekten (Teil des Selbststudiums) vermittelt. Dabei werden je nach Ausrichtung sowohl aktuell verbreitete Technologien und Werkzeuge (z.B. HTML, CSS, Ajax, WordPress, ...) als auch neue Technologien und Werkzeuge wie z.B. des Semantik Web (z.B. RDF, Ontologien, ...) oder des Mobile Web (z.B. Mobile-Ajax, ...) betrachtet.
Leistungsnachweis
Notenschein (für vorlesungsbegleitende Leistungen) oder schriftliche Prüfung im Umfang von 60 Minuten.
Dauer und Häufigkeit
Das Modul dauert 1 Trimester.Das Modul startet normalerweise im Frühjahrstrimester, wird aber nicht jedes Studienjahr angeboten.
Sonstige Bemerkungen
Das Modul ist identisch mit dem gleichnamigen Wahlpflichtmodul im Master - kann also entweder im Bachelor oder im Master belegt werden.

Modulname	Modulnummer
Aviation Management, Computational Networks and System Dynamics	1394

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Stefan Pickl	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
12322	VÜ	Aviation Management: Safety und Security	Wahlpflicht	3
12324	VÜ	System Dynamics	Wahlpflicht	3
12325	P	Praktikum Operations Research - Entscheidungsunterstützung II	Wahlpflicht	3
12326	SE	Seminar Ausgewählte Kapitel des Operations Research II	Wahlpflicht	3
13943	VÜ	Computational Networks	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen
Grundkenntnisse zu Statistik

Qualifikationsziele
Lernziele sind das kompetente Beherrschen grundlegender Verfahren und Methoden sowie ihrer praktischen Anwendung in den oben dargestellten Bereichen.

Inhalt
Die Studierenden sollen in diesem Modul mit den system- und entscheidungstheoretischen Grundlagen der Planung und Steuerung komplexer Systeme im Bereich des Aviation Managements vertraut gemacht werden; insbesondere im Hinblick auf die Strukturierung von Entscheidungsproblemen, die Entwicklung von Prozessmodellen zur Erforschung des Systemverhaltens (im Bereich Aviation Operations) sowie die Erarbeitung von Entscheidungsgrundlagen auf der Grundlage von Systembewertungen und speziellen OR-Techniken. Ein weiterer ergänzender Schwerpunkt dieses Moduls liegt im Bereich der Anwendung und Weiterentwicklung von System Dynamics Modellen im Bereich der strategischen Planung und Szenarentwicklung. Eine exemplarische Auswahl der Inhalte besteht aus: • Einführung ins Aviation Management • Theoretische Einführung in die System- und Entscheidungstheorie (Systemklassifikation, Eigenschaften von Systemen)

- Der systemanalytische Planungsprozess

  (Beispiel: Nutzer-Modell Interaktionen im Bereich Airport Operations)
- Modellbildung, Dynamische Systeme und Simulationen
- Szenartechniken, Zukunftsanalysen (RAHS), System Dynamics
- Soft OR/ Hard OR Analysen - Netzwerkplanungen
- Ausblick: System Dynamiks im Bereich MST (Modelling, Simulation, Training), Bestimmungsgrößen internationaler Sicherheit durch OR, Safety & Security

Leistungsnachweis

Schriftliche Prüfung über 60 min oder mündliche Prüfung von 30 min oder Notenschein.

Verwendbarkeit

Weiterführende Veranstaltungen im Bereich der Entscheidungstheorie und des Operations Research

Dauer und Häufigkeit

Das Modul dauert ein Trimester. Es beginnt jedes Studienjahr jeweils im Herbsttrimester.

Sonstige Bemerkungen

Es sind zwei Wahlpflichtveranstaltungen im Umfang von je 3 TWS zu wählen. Mindestens eine davon muss eine Vorlesung mit Übung sein, also "Aviation Management: Safety and Security" oder "Computational Networks" oder "System Dynamics".

Modulname	Modulnummer
Middleware und mobile Cloud Computing	1398

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Andreas Karcher	Pflicht	0

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	60	120	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
13981	VL	Middleware und mobile Cloud Computing	Pflicht	3
13982	UE	Middleware und mobile Cloud Computing	Pflicht	2
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

Vorausgesetzt werden Kenntnisse aus dem Bereich des Software Engineering, insbesondere der Objektorientierung (Modul Objektorientierte Programmierung) sowie der XML-Technologien.

Wünschenswert sind Grundkenntnisse in einer der objektorientierten Programmiersprache, wie z. B. Java, Scala, C++.

Qualifikationsziele

Das Modul Middleware und mobile Cloud Computing zielt darauf ab, den Studierenden vertiefend die Bedeutung der Integration als Kernaufgabe der Angewandten Informatik näher zu bringen. Die Teilnehmer erhalten neben einem grundlegenden Verständnis für die

Anforderungen an eine Middleware-basierte Integration tiefe theoretische Kenntnisse über Architektur, Aufbau und Anwendung aktueller Middlewarekonzepte. Zudem werden querschnittlich Aspekte von verteilten Systemen in diesem Zusammenhang betrachtet.

Im Übungsteil lernen die Teilnehmer parallel zur Vorlesung den praktischen Umgang mit Middleware-Technologien und Cloud-basierten, mobilen Anwendungen. Durch eigenständige Anwendung von unter anderem Remote Method Invocation (RMI), Common Object Request Broker Architecture (CORBA), .NET und Simple Object Access Protocol (SOAP) erhalten die Teilnehmer Methoden- und Fachkompetenz im Umgang mit diesen Technologien.

In der Kombination aus theoretischer Behandlung und praktischer Vertiefung versetzt das Modul die Teilnehmer in die Lage, verteilte Anwendungen auf der Basis von Middleware zu entwerfen und in die Praxis umzusetzen.

Inhalt
Moderne Enterprise Anwendungen basieren auf Standard-Middleware-Architekturen, wo Funktionalität zunehmend über Cloud-basierte Dienste plattformübergreifend den Clients # mehr und mehr auch mobilen Endgeräten # zur Verfügung gestellt wird. Das Modul bietet einen fundierten Einstieg in die aktuellen Basistechnologien. Hierbei wird das Wissen aus dem Modul der objektorientierten Programmierung um die fachwissenschaftliche Denkweise der Entwicklung von verteilten Anwendungen erweitert. Nach einer grundlegenden Einführung in die Integrationsanforderungen zunehmend verteilt strukturierter, internet-basierter betrieblicher Anwendungen vermittelt das Modul zunächst einen Überblick über die Grundarchitektur Middleware-basierter Systeme und geht dann im Folgenden tiefer auf die unterschiedlichen Integrationsparadigmen und -technologien ein. Aktuelle Middlewaredienste und Architekturkonzepte wie Verteilte Objektmodelle, Komponentenmodelle und Service Oriented Middleware (SOA) bilden den Schwerpunkt des zweiten Teils des Moduls. Hier werden jeweils zunächst die allgemeinen Prinzipien erläutert und dann anhand konkreter Beispiele Standard-Middleware-Technologien und deren zugrunde liegenden Konzepte vertieft. Der dritte Teil stellt das Cloud-Konzept in den Mittelpunkt und zeigt Schritt für Schritt an einfachen Beispielen die Entwicklung Cloud-basierter Dienste und deren Zugriff über mobile Clients (Apps). Die begleitende Übung bietet die Gelegenheit, aktuelle Technologien anhand einfacher Beispiele kennen zu lernen und erste praktische Erfahrung im Umgang mit Middleware und mobilen, Cloud-basierten Anwendungen zu sammeln.
Lehrmethoden
Das Modul unterteilt sich in eine Vorlesung und eine Übung pro Woche. Es werden sowohl Lehrmethoden des fremdgesteuerten als auch des selbstgesteuerten Lernens angewendet. Es wird auf die individuellen Voraussetzungen der Studierenden eingegangen, wobei hauptsächlich ein lehrgangsförmiger und kooperativer Unterricht mit Einzelarbeit stattfindet.
Leistungsnachweis
Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer. Die Art der Prüfung wird jeweils zu Beginn des Moduls bekannt gegeben.
Verwendbarkeit
Die im Wahlpflichtmodul erworbenen Kenntnisse sind elementar für die IT-technische Gestaltung von verteilten Informationssystemen und stellen somit eine Grundlage für

Masterstudiengänge im Bereich Informatik/Wirtschaftsinformatik/Ingenieurinformatik/ Cyber Sicherheit dar.
Dauer und Häufigkeit
Das Modul dauert 1 Trimester. Das Modul beginnt jedes Studienjahr jeweils im Wintertrimester.

Modulname	Modulnummer
Operations Research, Complex Analytics and Decision Support Systems (ORMS I)	1490

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Stefan Pickl	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10333	VÜ	Moderne Heuristiken	Wahlpflicht	3
12325	P	Praktikum Operations Research - Entscheidungsunterstützung II	Wahlpflicht	3
12326	SE	Seminar Ausgewählte Kapitel des Operations Research II	Wahlpflicht	3
14901	VÜ	Ausgewählte Kapitel des Operations Research und der Entscheidungstheorie	Pflicht	3
149010	VÜ	Spieltheorie: Einführung in die mathematische Theorie strategischer Spiele	Wahlpflicht	3
149014	B	Geschichte des Operations Research	Wahlpflicht	3
14902	VÜ	Diskrete Optimierung	Wahlpflicht	3
14904	VÜ	Scheduling	Wahlpflicht	3
14905	VÜ	Schwarmbasierte Verfahren	Wahlpflicht	3
14906	VÜ	Soft Computing A: Management Science and Complex System Analysis - System Dynamics and Strategic Planning	Wahlpflicht	3
14907	VÜ	Soft Computing B: Fuzzy Systems - Network Operations	Wahlpflicht	3
14908	VÜ	Soft Computing C: Natural Computing - Evolutionary Algorithms	Wahlpflicht	3
14909	VÜ	Soft Computing D: Neural Networks and Network Analysis	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				9

Qualifikationsziele
Studierende sollen in die Lage versetzt werden, Probleme im Bereich der industriellen Anwendung, der öffentlichen Verwaltung, der internationalen Konflikte und des

strategischen Managements als Operations Research zugehörige Probleme zu identifizieren und mit geeigneten Modellen und Lösungsverfahren zu behandeln.

Es ist das Ziel dieses Moduls, dass die Studierenden sicher mit den Standard Verfahren des Operations Research und der Computational Intelligence umgehen können. Im Rahmen des heutigen unterstützenden Rechnereinsatzes sollen Sie in der Lage sein, zukünftige Potentiale zu erkennen und damit verbundene Komplexitätsaspekte im Ramen eines modernen Komplexitätsmanagements mit Methoden des Soft Computing kompetent zu behandeln.

Inhalt

Die Veranstaltung führt in das weite fachliche Gebiet des Operations Research ein. Der quantitativen Beschreibung und Lösung von komplexen Entscheidungs-problemen kommt hierbei eine besondere Bedeutung zu (Operations Research im engeren Sinne). Ferner wird auf die Entwicklung von algorithmischen Verfahren und Lösungsstrategien großen Wert gelegt (im Rahmen einer anwendungsbetonten Mathematischen Programmierung/ Computational Intelligence). Die behandelten Modelle und Verfahren werden exemplarisch aus dem Bereich der industriellen Anwendung, der öffentlichen Verwaltung, der internationalen Konflikte und des strategischen Managements gewählt werden.

Das Gebiet "Computational Intelligence" umfasst Methoden der sogenannten subsymbolischen Informationsverarbeitung. Auch wenn derzeit noch keine allgemeingültige genaue wissenschaftliche Definition dieses Begriffes existiert, so dient er dazu, die Gebiete "Evolutionary Computation", "Fuzzy Computation" und "Neural Computation" zusammenzufassen. "Computational Intelligence" betont zum einen den algorithmischen Aspekt und zum anderen die Fundierung im Bereich der künstlichen Intelligenz, der Entscheidungstheorie und der multikriteriellen Optimierung.

Im Zentrum dieses Moduls steht die Vermittlung von grundlegenden Kenntnissen über die in diesen Bereichen angewendeten relevanten Algorithmen, Heuristiken und Methoden. Die praktischen Bezüge reichen von den Bereichen "Business Intelligence/Optimization" und "Experimental Design" (z.B. im Bereich einer vernetzten Operationsführung) bis hin zum "Algorithmic Engineering".

Eine inhaltliche Auswahl besteht aus folgenden Elementen: Einführung in die Problemstellung und Lösungsmethoden der allgemeinen Unternehmensforschung (inklusive Operations Management), Klassische Optimierungsverfahren (lineare, nichtlineare, dynamische und diskrete Optimierung, Spieltheoretische Modelle und Verfahren, Mathematische Programmierung, Theorie dynamischer und stochastischer Prozesse, Ausblick auf aktuelle Probleme der Logistik, Steuerung und Netzwerktheorie und Soft Computing).

Leistungsnachweis

Mündliche Prüfung von 30 min oder Notenschein. Die Art der Prüfung wird am Anfang des Moduls festgelegt und bekannt gegeben.

Dauer und Häufigkeit

Das Modul dauert 2 bis 3 Trimester. Es wird nicht regelmäßig angeboten.

Sonstige Bemerkungen
Neben der Pflichtveranstaltung "Ausgewählte Kapitel des Operations Research und der Entscheidungstheorie" müssen zwei Lehrveranstaltungen mit Übungen im Umfang von je 3 TWS besucht werden.

Modulname	Modulnummer
Formale Entwicklung korrekter Software	1518

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
PD Dr. Birgit Elbl Univ.-Prof. Dr.-Ing. Markus Siegle	Wahlpflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	60	120	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
15171	VÜ	Entwurf Verteilter Systeme	Wahlpflicht	5
15172	VÜ	Methoden und Werkzeuge	Wahlpflicht	5
15174	VÜ	Spezifikation	Wahlpflicht	5
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

Vorausgesetzt werden die im Bachelor-Studium erworbenen Grundkenntnisse und Fertigkeiten in diskreter Modellierung (elementare Logik und Mengenlehre), systematischer Programmentwicklung und Theoretischer Informatik. Für den "Entwurf verteilter Systeme" wird darüber hinaus Vertrautheit mit Grundlagen der Architektur und dem Entwurf von Rechen- und Kommunikationssystemen erwartet.

Qualifikationsziele

Die Studierenden erhalten einen Überblick über die wichtigsten Methoden und Werkzeuge für die formale Entwicklung korrekter Software, von der Spezifikation bis hin zum Entwurf verteilter Systeme. Sie erwerben die Kompetenz, diese im Entwurfsprozess gewinnbringend einzusetzen, d.h. einschlägige Verfahren und Werkzeuge auszuwählen und effizient anzuwenden.

Inhalt

Ein Schwerpunkt der Vorlesung "Spezifikation" sind abstrakte Datentypen, bei denen sowohl die initiale Semantik, als auch lose Spezifikationen behandelt werden. Den Studierenden werden Ansätze zur Strukturierung und zum schrittweisen Aufbau von Spezifikationen vorgestellt. Sie sehen Beispiele für die schrittweise Entwicklung von programmnahen aus rein deskriptiven Spezifikationen. Sie lernen die Kernbegriffe Verfeinerung, Erweiterung und abstrakte Implementierung kennen und deren Rolle bei der Entwicklung von Spezifikationen. Beispiele sind u.a. den Bereichen Spezifikation komplexer Datenstrukturen und zustandsorientierte Spezifikation sequentieller Systeme entnommen. Den Abschluss bildet eine kurze Einführung in die temporale Spezifikation nebenläufiger Systeme.

In der Vorlesung "Entwurf verteilter Systeme" werden formale Methoden vorgestellt, mit deren Hilfe die Struktur und das dynamische Verhalten von komplexen verteilten (oder allgemeiner ausgedrückt: nebenläufigen) Systemen spezifiziert werden kann. Wir behandeln insbesondere die beiden Spezifikationsformalismen Petrinetze und Prozessalgebren, und diskutieren ihre mathematischen Eigenschaften und die darauf aufbauenden Analyseverfahren.

Weiterhin behandeln wir die Frage nach der Formalisierung von Anforderungen an ein solches verteiltes System, wobei sich temporale Logiken als wertvolle Hilfsmittel erweisen. Es wird gezeigt, wie man mit der Methode des Model Checking komplexe, temporal spezifizierte Anforderungen automatisch überprüfen kann.

Neben den Verifikationsalgorithmen für die weit verbreitete Logik CTL werden Erweiterungen in Richtung von Realzeiteigenschaften angesprochen. In den Übungen erhalten die Studierenden auch Gelegenheit, entsprechende Software-Werkzeuge kennenzulernen und selbst zu erproben.

Die Vorlesung "Methoden und Werkzeuge" macht die Studierenden mit Systemen zur modellbasierten Spezifikation von Software (wie JCL, OCL und Z) bekannt. Fallstudien werden vorgestellt, von den Studierenden ergänzt und auf Konsistenz untersucht, wobei sie u.a. Methoden und Werkzeuge des Model Checking (z.B. Alloy) einzusetzen lernen.

Die Studierenden befassen sich mit der systematischen Herleitung korrekter Software, entweder durch Programmtransformation oder durch zielgerichtete Programmherleitung (z.B. mit VDM). Sie lernen, mit Hilfe von Werkzeugen (wie Spark) die Korrektheit von Software praktisch nachzuweisen. Dazu bearbeiten sie in Übungen und Hausaufgaben auch über Spielbeispiele hinausgehende Fallstudien.

Leistungsnachweis

Das Modul wird per Notenschein geprüft. Es ist eine der drei Vorlesungen (mit Übung) zu belegen.

Verwendbarkeit

Bei sicherheitskritischer Software ist Korrektheit das wichtigste Qualitätskriterium. Modellbasiertes, formales Vorgehen ist für den Entwurf moderner, komplexer Systeme (sowohl Software als auch Hardware) unerlässlich. Daher ergänzen die hier erworbenen Kenntnisse und Fertigkeiten die Ausbildung im Bereich der Softwaretechnik um einen Aspekt von hoher praktischer Bedeutung.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester.

Sonstige Bemerkungen

Jedes Jahr wird mindestens eine Vorlesung (mit Übung) angeboten, so dass 6 ECTS-Punkte erreichbar sind. Jeweils zu Beginn des Masterstudiums wird den Studierenden das konkrete Angebot erläutert.

Modulname	Modulnummer
Ökonomie und Recht der Informationsgesellschaft	2461

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. jur. Stefan Koos Univ.-Prof. Dr. rer. pol. Karl Morasch	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
150	24	126	5

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
24611	VS	Ökonomie und Recht der Informationsgesellschaft	Wahlpflicht	2
Summe (Pflicht und Wahlpflicht)				2

Empfohlene Voraussetzungen

Es werden rechtliche und wirtschaftswissenschaftlichen Kenntnissen vorausgesetzt, wie sie üblicherweise in einem wirtschaftswissenschaftlichen Bachelor-Studiengang erworben werden. Englischkenntnisse werden vorausgesetzt; das Modul kann auch in englischer Sprache abgehalten werden (hierüber entscheidet der/die Modulverantwortliche jeweils zu Beginn des Moduls).

Qualifikationsziele

Die Studierenden erwerben in juristischer Hinsicht Kenntnisse über nationale und internationale Rechtsnormen zum Recht des elektronischen Handels und in ökonomischer Hinsicht zur Ökonomie von Informationsgütern und elektronischen Märkten. Die unmittelbare Verknüpfung rechtlicher und ökonomischer Aspekte verdeutlicht dabei die komplexe Interaktion institutioneller Rahmenbedingungen und ökonomischer Anreize. Bei Belegung im Rahmen der Vertiefung „Management marktorientierter Wertschöpfungsketten“ dient das Modul dazu, sich auf einen Aspekt des Managements marktorientierter Wertschöpfungsketten zu spezialisieren. Es hat zum Ziel, die Möglichkeit einer verstärkten Profilierung zu eröffnen und vertiefte inhaltliche Kompetenzen bei einzelnen Aspekten des Managements marktorientierter Wertschöpfungsketten zu erwerben. Bei Belegung im Rahmen der Vertiefung „Ökonomie und Recht der globalen Wirtschaft“ ermöglicht dieses Modul in Verbindung mit den Pflichtmodulen und den zwei anderen Wahlpflichtmodulen ein integriertes Gesamtverständnis der globalen Wirtschaft zu erlangen.

Inhalt

Die Veranstaltung beschäftigt sich mit den ökonomischen und rechtlichen Fragestellungen, die sich aus der zunehmenden Bedeutung elektronischer Marktpätze und von Märkten für Informationsgüter (Musik, Filme, News etc.) ergeben. Es werden die Besonderheiten solcher Informationsgüter und von Märkten mit Netzwerkeffekten, sowie geeignete Unternehmensstrategien für den Wettbewerb auf solchen Märkten

diskutiert. Anschließend werden im Kontext der Intermediations- und der Auktionstheorie elektronische Marktplätze für Konsumenten (z.B. Ebay) und der Einsatz des E-Commerce beim Handel zwischen Unternehmen thematisiert. Aus rechtlicher Perspektive werden neben den für Informationsgüter relevanten immaterialgüterrechtlichen Regelungen (Copyright, Software-Patente) insbesondere die vertragsrechtlichen und wettbewerbsrechtlichen Fragen des elektronischen Handels sowie die besonderen rechtlichen Probleme des grenzüberschreitenden elektronischen Handels und das Domainrecht behandelt.

Das Modul kann auch in englischer Sprache gehalten werden.

Literatur

Shapiro, C., Varian H. R. (1999), Information Rules. A Strategic Guide to the Network Economy, Boston (MA): Harvard Business School Press.

Shy, O., (2001), The Economics of Network Industries, Cambridge (UK): Cambridge University Press.

Leistungsnachweis

Schriftliche Prüfung im Umfang von 60 Minuten oder Notenschein. Falls der Leistungsnachweis durch Notenschein erfolgt, wird dies zusammen mit den konkreten Modalitäten für den Erwerb des Notenscheins spätestens zu Beginn der Veranstaltung bekanntgegeben.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester. Das Modul beginnt in jedem Studienjahr im Herbsttrimester. Als Startzeit ist das Herbsttrimester im 1. Studienjahr vorgesehen.

Modulname	Modulnummer
Ausgewählte Kapitel des OR: Data-driven Optimization	2994

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. rer. nat. Maximilian Moll	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
29941	VÜ	Ausgewählte Kapitel des Data-driven Optimization	Pflicht	3
29942	VÜ	Quantum Machine Learning & Optimization	Wahlpflicht	3
29943	SE	Seminar: Ausgewählte Kapitel des OR	Wahlpflicht	3
29944	P	Praktikum: Ausgewählte Kapitel des OR	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Grundlegende Kenntnisse in Methoden des Operations Research und des Data Minings oder der Statistik werden vorausgesetzt.

Qualifikationsziele

Studierende sollen in die Lage versetzt werden, sich selbstständig mit neuartigen Methoden der data-driven Optimization in Theorie und Praxis auseinander zu setzen. Hierzu sollen sie im Rahmen der Vorlesung, sowie vertiefend in Seminar und Praktikum, verschiedene Methoden analysieren und anwenden.

Hierbei soll nicht nur die Fähigkeit entwickelt werden Ansätze auf ihre theoretische Richtigkeit und praktische Anwendbarkeit zu beurteilen, sondern diese auf ein Problem hin anpassen zu können.

Schließlich soll das Identifizieren geeigneter Probleme und passender Lösungsansätze geschult werden.

Inhalt

Data-driven Optimization beschäftigt sich zukunftsweisend mit der Kombination von klassischen Optimierungsmethoden und daten-basierten Ansätzen. Im Gegensatz zu der klassischen Optimierung der letzten Jahrhunderte, die ausgehend von einem zu optimierenden Modell eine Lösung sucht, bietet das Data-driven Optimization die Möglichkeit, ohne eine exakte mathematische Abstrahierung des zugrunde liegenden Modells Optimierungsmethoden anzuwenden.

Das Modul bietet aufbauend auf dem vorhandenen Grundwissen einen vertiefenden Einblick in ausgewählte Themengebiete des data-driven Optimization. Neben der grundlegenden Problematik werden Themen aus dem Reinforcement Learning, Prescriptive Analytics und der konvexen Optimierung unter Unsicherheit behandelt.

Das Reinforcement Learning ist neben Supervised und Unsupervised Learning das dritte Teilgebiet des Machine Learnings und beschäftigt sich mit daten-basierten Ansätzen zu Problemen der klassischen Kontrolltheorie. Hierbei soll im Modul auch die Anwendung auf praxis-relevante Probleme herausgestellt werden, die über die bekannten Lösungen von Spielen, wie z.B. Go, hinausgehen.

Prescriptive Analytics stellt aufbauend auf Descriptive und Predictive Analytics die nützlichste und schwerste Stufe des Data Science dar. Hier müssen nicht nur datan-basierte Vorhersagen getroffen werden, sondern das zukünftige System auf eine gegebene Zielvorstellung hin optimiert werden. In der Vorlesung werden verschiedene grundsätzliche Herangehensweisen mit ihren Vor- und Nachteilen diskutiert, sowie die Abgrenzung zu Predictive Analytics konkretisiert.

Die konvexe Optimierung stellt ein zentrales Element des Operations Research und der modernen Entscheidungsunterstützung dar. In vielen Fällen sind jedoch die Parameter der Optimierungsmodelle nicht explizit bekannt, sondern müssen zunächst aus Daten abgeleitet werden. Die Vorlesung thematisiert, wie sich dies auf die zu wählenden Optimierungsverfahren auswirken muss.

Das Seminar greift aktuelle Publikationen zu den Themen der Vorlesung auf.

Im Praktikum setzen sich die Studierenden mit einer konkreten, praxis-nahen Problemstellung des data-driven Optimization auseinander.

In der Vorlesung Quantum Machine Learning and Optimization wird spezifisch auf die Verwendung von Quantum Computern für effizientere Algorithmen im Kontext der NISQ-Maschinen eingegangen.

Leistungsnachweis

Mündliche Prüfung von 30 min.

Zum Absolvieren des Moduls sind drei der vier Wahlpflichtveranstaltungen zu belegen.

Dauer und Häufigkeit

Das Modul dauert 2 Trimester. Es beginnt immer im Frühjahrstrimester.

Modulname	Modulnummer
Benutzbare Sicherheit	3665

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Florian Alt	Wahlpflicht	4

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
36651	VÜ	Benutzbare Sicherheit	Pflicht	3
36653	P	Praktikum Design sicherer und benutzbarer Systeme	Pflicht	3
3665-V1	VÜ	Sichere Mensch-Maschine Schnittstellen	Pflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Für die Teilnahme an diesem Modul werden Grundkenntnisse in der Informatik und in der Programmierung vorausgesetzt. Insbesondere Erfahrung mit Android und Web-Programmierung sind von Vorteil. Hilfreich sind außerdem Grundkenntnisse in der Mensch-Maschine Interaktion. Folgende Literatur kann zur Vorbereitung dienen:

- Butz, Andreas, and Antonio Krüger. Mensch-Maschine-Interaktion. Walter de Gruyter GmbH & Co KG, 2017.
- Cranor, Lorrie Faith, and Simson Garfinkel. Security and usability: designing secure systems that people can use. O'Reilly Media, Inc., 2005.
- Lazar, Jonathan, Jinjuan Heidi Feng, and Harry Hochheiser. Research methods in human-computer interaction. Morgan Kaufmann, 2017.
- Oates, Briony J. Researching information systems and computing. Sage, 2005.

Qualifikationsziele

In diesem Modul erlernen die Teilnehmer die Fähigkeit, sich beim Design sicherer Systeme kritisch mit dem Faktor „Mensch“ auseinanderzusetzen. Insbesondere wird ein Verständnis für Anforderungen solcher Systeme hinsichtlich ihrer Sicherheit aber auch ihrer Benutzbarkeit geschaffen.

Den Studierenden werden Grundlagen der Mensch-Maschine Interaktion und der benutzbaren Sicherheit (Grundbegriffe, Sicherheitsmechanismen, Bedrohungsmodelle) vermittelt. Sie erarbeiten sich tiefgehende, methodische Kenntnisse, welche es ihnen ermöglichen, Konzepte und Systeme zu entwickeln und hinsichtlich ihrer Sicherheit und Benutzbarkeit zu evaluieren. Basierend auf dem theoretischen Grundlagen- und

Methodenwissen wird im praktischen Teil des Moduls die Fähigkeit zur Konzeption und praktischen Umsetzung sicherer und benutzbarer Systeme vertieft.

Inhalt

Technologie kann nicht die alleinige Lösung für Herausforderungen im Bereich IT-Sicherheit sein. Wir sind heute in der Lage, Mechanismen zu schaffen, die aktuell nicht brechbar sind. Trotzdem ist Sicherheit in vielen Bereichen immer noch ein ungelöstes Problem, da viele der von uns entwickelten Systeme und Mechanismen nicht nutzbar sind. Das hat zur Folge, dass Menschen freiwillig oder unfreiwillig Wege finden, solche Mechanismen auszuhebeln. Menschliche Faktoren spielen eine zentrale Rolle in der IT-Sicherheit. Daher ist es wichtig, dass Experten für Benutzbare Sicherheit ein Verständnis dafür entwickeln, wie Menschen mit den von uns entwickelten Systemen interagieren. Dieses Modul führt die Teilnehmer in eine Vielzahl von Herausforderungen in Bezug auf die Benutzerfreundlichkeit und die Sicherheit in ubiquitären Systemen ein. Es vermittelt die theoretischen, methodischen und praktischen Grundlagen für das Design sicherer und benutzbarer Systeme.

Hierfür dienen drei Lehrveranstaltungen:

Sichere Mensch-Maschine-Schnittstellen – Die Veranstaltung vermittelt Grundlagenwissen für die Konzeption, das Design und die Evaluierung benutzbarer und gleichzeitig sicherer Mensch-Maschine-Schnittstellen. Hierfür werden im ersten Teil die Informationsverarbeitung des Menschen (physiologische und psychologische Grundlagen, Modelle, Handlungsprozesse) sowie die technische Realisierung von Benutzungsschnittstellen (Ein- und Ausgabegeräte, Interaktionsstile) behandelt sowie benutzerorientierte Entwurfsprozesse, Richtlinien und Standards für Benutzbarkeit und Sicherheit vorgestellt. Der zweite Teil widmet sich der Evaluation und der Bewertung von Mensch-Maschine Schnittstellen hinsichtlich verschiedener Kriterien. Dies erfordert ein breites Wissen in der Forschungsmethodik. Daher werden verschiedene Studientypen (z.B. deskriptive Studien, relationale Studien, experimentelle Studien), Studienparadigmen (u.a. Ethnographie, Laborstudien, Feldstudien, Deployments) sowie Datenerhebungsmethoden (z.B. Fragebögen, Interviews, Beobachtungen, Experience Sampling und Crowdsourcing) behandelt.

Benutzbare Sicherheit – Diese Vorlesung gibt einen Überblick über Herausforderungen hinsichtlich der Benutzbarkeit sicherer und benutzbarer Systeme. Die Studierenden lernen verschiedene Sicherheits-Mechanismen und mentale Modelle der Benutzer kennen. Zudem erhalten sie eine Einführung in die Modellierung von Bedrohungen. Insbesondere behandelt die Veranstaltung aktuelle Themen der Benutzbaren Sicherheit, unter anderem, Authentifizierung, Passwörter und Social Engineering. Die Lehrveranstaltung richtet sich sowohl an Studierende, die an Sicherheit und Datenschutz interessiert sind und mehrüber Benutzbarkeit erfahren möchten, als auch an Studierende, die an Benutzbarkeit interessiert sind, aber mehr über Sicherheit und Datenschutz erfahren möchten.

Design sicherer und benutzbarer Systeme – Ziel dieses Praktikums ist das Erlernen benutzer-zentrierter Techniken für die Konzeption, das Design und die Umsetzung sicherer und benutzbarer Systeme. Die Teilnehmer dieser Lehrveranstaltung wenden

hierzu einen benutzer-zentrierten Designprozess an. In Gruppen werden neuartige Konzepte erarbeitet. Ausgewählte Konzept werden anschließend prototypisch umgesetzt und mithilfe von Benutzerstudien hinsichtlich Sicherheit und Benutzbarkeit getestet.
Leistungsnachweis
Das Modul wird mit einem Notenschein abgeschlossen.
Dauer und Häufigkeit
Das Modul dauert 2 Trimester und beginnt jedes Jahr im WT.

Modulname	Modulnummer
Natural Language Processing	3850

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. phil. Michaela Geierhos	Wahlpflicht	4

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
38501	VÜ	Natural Language Processing	Pflicht	3
38502	P	Praktikum Natural Language Processing	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen
Die Studierenden sollten Grundkenntnisse in Informatik besitzen, insbesondere Erfahrung mit Algorithmen sowie Programmierkenntnisse in Python haben.

Qualifikationsziele
Ziel der Lehrveranstaltungen dieses Moduls ist es, die Studierenden mit speziellen Techniken des Natural Language Processing vertraut zu machen. Insbesondere sollen die Studierenden dabei lernen, wie Qualität, Zuverlässigkeit und Leistungsfähigkeit komplexer Sprachmodelle durch Auswahl entsprechender Entwicklungs- und Evaluationsmethoden gewährleistet werden können.

Inhalt
Die Studierenden lernen die wichtigsten Phänomene in natürlichen Sprachen auf verschiedenen Granularitätsebenen kennen, angefangen bei der Kombination von Lauten bis hin zur Bedeutung von Wörtern, Sätzen und Texten. Sie erhalten eine Einführung in die wichtigsten symbolischen und statistischen Ansätze des Natural Language Processing (NLP) zur Modellierung dieser Phänomene. Alle theoretischen Themen werden von Übungen begleitet, die sich mit diesen Phänomenen befassen und die ihre Anwendung in praktischen Szenarien demonstrieren, wie z. B. Rechtschreibkorrektur, automatische Vervollständigung, Schlüsselwortextraktion, Themenerkennung, Erkennung von benannten Entitäten (Eigennamen), Relationsextraktion, Synonymerkennung, etc. Im Praktikum werden die Inhalte der Vorlesung im Rahmen eines exemplarischen NLP-Projekts zur Anwendung gebracht.

Leistungsnachweis
Leistungsnachweis für das Gesamtmodul ist ein Notenschein, der sich aus den Einzelleistungen in den beiden Teilveranstaltungen zusammensetzt. Die geforderten Einzelleistungen werden in den einzelnen Veranstaltungen separat bekannt gegeben.
Verwendbarkeit
Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit im Bereich Data Science mit Fokus auf Natural Language Processing.
Dauer und Häufigkeit
Das Modul dauert 2 Trimester und beginnt jedes Jahr im WT.

Modulname	Modulnummer
Information Retrieval	3851

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. phil. Michaela Geierhos	Wahlpflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
38511	VÜ	Information Retrieval	Pflicht	6
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen
Die Studierenden sollen grundlegende Programmierkenntnisse sowie ein Grundverständnis von Algorithmen und Datenstrukturen haben.

Qualifikationsziele
Studierende lernen Aufgabenstellung, Modelle und Methoden des Information Retrieval kennen. Dabei soll die Fähigkeit zur Nutzung und zur Mitwirkung bei der Konzeption und Konfiguration von Suchmaschinenlösungen für Web und Enterprise Search vermittelt werden. Darüber hinaus sollen die Vor- und Nachteile der zugrundeliegenden Konzepte und Modelle sowie der verschiedenen Implementierungstechniken verstanden werden.

Inhalt
Dieses Modul gibt einen Einblick in die wichtigsten Themen des Information Retrieval. Hierfür werden die Grundlagen der wichtigsten Modelle aus dem Bereich des Information Retrieval vermittelt. Außerdem werden Techniken und Verfahren wie z. B. Term-Gewichtungen, Ähnlichkeitsmaße und Rankingmechanismen, Evaluierungsprinzipien, Benutzerinteraktion und Feedbackmechanismen sowie Indexierung und computerlinguistische Hilfsmittel für dem Bereich des Information Retrieval detailliert behandelt. In der Übung werden theoretische und praktische Fragestellungen gleichermaßen behandelt. Der theoretische Teil dient zur Wiederholung der Vorlesungsinhalte. Im praktischen Teil sind die Studierenden aufgefordert, ausgewählte Verfahren aus dem Information Retrieval eigenständig zu implementieren. Für die Übungen sind Programmierkenntnisse erforderlich.

Leistungsnachweis
Schriftliche Prüfung von 60 Minuten oder mündliche Prüfung von 30 Minuten.

Verwendbarkeit
Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit im Bereich Data Science mit Fokus auf Information Retrieval.
Dauer und Häufigkeit
Das Modul dauert ein Trimester und beginnt jedes Jahr im WT.

Modulname	Modulnummer
Anwendungsgebiete der Data Science	3852

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. phil. Michaela Geierhos	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
38521	VÜ	Sentiment Analysis	Wahlpflicht	3
38522	VÜ	Social Media Mining	Wahlpflicht	3
38523	VÜ	Semantische Technologien	Wahlpflicht	3
38524	PRO	Modulprojekt Anwendungsgebiete der Data Science	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Die Studierenden sollen grundlegende Kenntnisse in Programmierung und Software-Entwurf sowie ein Grundverständnis von Algorithmen und Datenstrukturen haben.

Qualifikationsziele

Die Studierenden lernen Herausforderungen und Methoden beim Text Mining kennen und lernen die besprochenen Techniken anzuwenden. Zudem lernen sie theoretische Ansätze auf konkrete, praxisrelevante Fragestellungen zu übertragen. Für exemplarische Aufgabenstellungen können die Studierenden bestehende methodische Ansätze beurteilen und Weiterentwicklungen anregen resp. eigenständig umsetzen. Sie können begründet argumentieren und eine von ihnen selbständig gefundene Lösung vertreten und reflexiv bewerten.

Inhalt

- In der Vorlesung „Sentiment Analysis“ soll die schon umfangreiche Forschungsliteratur zum Opinion Mining aufgearbeitet werden. Dabei reichen die Ansätze von der Text- bis zur Wortebene, die Aufgaben sind das Erkennen von Subjektivität vs. Objektivität, das Bestimmen der Perspektive von Autoren, das Extrahieren ihrer Meinung. Datenquellen können Review-Seiten aus dem Internet sein, Blog-Posts und -kommentare, Nachrichten auf Twitter, gesprochene Sprache, usw.
- In der Vorlesung „Social Media Mining“ wird exemplarisch die Entwicklung eines Systems besprochen, welches über soziale Netzwerke direkt oder indirekt an Unternehmen adressierte Meldungen, Nachrichten oder Kommentare erfasst, klassifiziert und auswertet. Hierbei werden Textmining- und Klassifikationsverfahren mit Fokus auf Kurztexten diskutiert und der begleitenden Übung praktisch vertieft.

- Die Vorlesung „Semantische Technologien“ gibt einen Einblick in Grundlagen und praktische Anwendungen wissensbasierter Softewarelösung. Sie gibt einen breiten Überblick über den Nutzen und die Möglichkeiten dieser Technologien. Semantische Technologien versetzen uns nicht nur in die Lage, Informationen zu speichern und wiederzufinden, sondern sie gemäß ihrer Bedeutung und Funktion entsprechend auszuwerten, zu verbinden, zu Neuem zu verknüpfen und so flexibel und zielgerichtet anzuwenden.
- Im Modulprojekt setzen sich Studierende unter Anleitung selbständig mit Texten und Aufgaben zum Modulthema auseinander und präsentieren ihre Ergebnisse geeignet in mündlicher und/oder schriftlicher Form. Zu Beginn des Modulprojekts werden die geplanten Einzelthemen angekündigt und festgelegt, in welcher Form die Ergebnisse zu präsentieren sind.

Leistungsnachweis
Das gesamte Modul wird per Notenschein geprüft, mit Anteilen von je 3 ECTS-LP zu jeder der Vorlesungen (mit Übung) und im Modulprojekt. Die Studierenden können (je nach Angebot) entweder zwei Vorlesungen mit Übungen oder eine Vorlesung mit Übungen und ein Modulprojekt einbringen – was insgesamt die 6 ECTS-LP des Moduls ergibt.
Verwendbarkeit
Die hier erworbenen Kenntnisse und Fertigkeiten ergänzen die Ausbildung im Bereich der Softwaretechnik um einen Aspekt von hoher praktischer Bedeutung. Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit im Bereich Data Science.
Dauer und Häufigkeit
Das Modul dauert 1-2 Trimester und beginnt jedes Jahr im HT.
Sonstige Bemerkungen
Die Vorlesungen und das Praktikum werden nicht alle jedes Jahr angeboten, aber in jedem Jahr mindestens so viele Lehrveranstaltungen, dass 6 ECTS-Leistungspunkte erreichbar sind. Jeweils zu Beginn des Moduls wird den Studierenden das konkrete Angebot erläutert.

Modulname	Modulnummer
Analyse unstrukturierter Daten	3853

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. phil. Michaela Geierhos	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
38531	VÜ	Analyse unstrukturierter Daten	Pflicht	6
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Die Studierenden sollen grundlegende Programmierkenntnisse sowie ein Grundverständnis von Algorithmen und Datenstrukturen haben.

Qualifikationsziele

Die Studierenden lernen Herausforderungen und Methoden bei der Informationsbeschaffung und -extraktion kennen und lernen die besprochenen Analyse-Methoden anzuwenden. Sie lernen Verfahren der Analyse unstrukturierter Daten auf konkrete, praxisrelevante Fragestellungen (insb. im Bereich Wissensgewinnung) anzuwenden und können für exemplarische Aufgabenstellungen existierende Ansätze beurteilen und Weiterentwicklungen anregen resp. eigenständig umsetzen.

Inhalt

Dieses Modul gibt einen Einblick in die Herausforderungen und Verfahren, die bei der Analyse unstrukturierter Daten zum Einsatz kommen. Unstrukturierte Informationen sind in der Regel sehr textlastig, weshalb viele vorhersagende Analyse-Verfahren den Informationswert dieser Daten nicht nutzen können. Allerdings können textbasierte Medien (E-Mails, Webseiten-Inhalte, Fachartikel, Social Media Beiträge, etc.) u. a. dabei helfen, Trends zu erkennen, Wissen zu gewinnen und Fake News aufzudecken. Hierfür müssen Informationen identifiziert, extrahiert, aufbereitet und interpretiert werden. Die Herausforderung besteht darin, relevante Informationen zu erkennen, aus unstrukturierten Texten zu extrahieren und fehlende Informationen ggf. hinzufügen.

In der Veranstaltung werden auch Themen wie die Informationsgewinnung aus unterschiedlichen Quellen sowie Fragen der Qualitätssicherung bei der Datenspeicherung und des Datenmanagements in wissensbasierten Strukturen behandelt.

In der Übung werden theoretische und praktische Fragestellungen gleichermaßen adressiert. Der theoretische Teil dient zur Wiederholung der Vorlesungsinhalte. Im

praktischen Teil sind die Studierenden aufgefordert, ausgewählte Verfahren zur Analyse unstrukturierter Daten eigenständig zu implementieren. Für die Übungen sind Programmierkenntnisse erforderlich.
Leistungsnachweis
Schriftliche Prüfung von 60 Minuten oder mündliche Prüfung von 30 Minuten.
Verwendbarkeit
Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit im Bereich Data Science mit Fokus auf die Analyse unstrukturierter Daten.
Dauer und Häufigkeit
Das Modul dauert ein Trimester und beginnt jedes Jahr im HT.

Modulname	Modulnummer
Mobile Security	5513

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Gabi Dreo Rodosek	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
11972	VÜ	Mobile Kommunikationssysteme	Pflicht	3
55131	VÜ	Sichere mobile Systeme	Wahlpflicht	3
55132	VÜ	Sensorik und Manipulationsdetektion	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Für die Veranstaltungen im Modul werden grundlegende Kenntnisse in Rechnernetzen vorausgesetzt, wie sie z.B. im Bachelor-Modul Einführung in die Technische Informatik vermittelt werden.

Qualifikationsziele

Die Studierenden erhalten ein umfassendes Wissen der Funktionsweise mobiler Kommunikationsnetze. Sie können die wichtigsten Grundlagen drahtloser Kommunikationstechniken erläutern und die verschiedenen Verfahren und Systeme kategorisieren. Je nach erfolgter Auswahl innerhalb des Moduls haben sie vertiefte Kenntnisse in Bezug auf die Sicherheitsaspekte der Übertragungswege oder der Hardware-Komponenten. Sie sind in der Lage, die Wirksamkeit von Sicherheitsmaßnahmen einzuordnen und Sicherheitseigenschaften von mobilen Kommunikationssystemen zu bewerten. Sie erhalten eine erste Orientierung zum Vorgehen bei der Absicherung von mobilen Systemen durch Auswahl der Technologie und Konfiguration des Systems und den Einsatz spezieller Sicherheitsmechanismen.

Inhalt

Die Pflichtveranstaltung behandelt die wesentlichen Techniken zur Realisierung von mobiler (drahtloser) Kommunikation mit dem Schwerpunkt auf IT-Systemen. Dazu gehören die Funkübertragungstechniken, insbesondere die zellenbasierten Funksysteme, die Medienzugriffsverfahren, die die gemeinsame Nutzung des Funkraums koordinieren (Multiplexverfahren, Kollisionserkennung und -vermeidung), und die mobilen Varianten der Vermittlungsschicht (mobile IP, ad-hoc networking, Routingverfahren) und der Transportschicht (flow control, quality of service). Daneben werden die verschiedenen Arten der verwendeten mobilen Kommunikationssysteme vorgestellt: Drahtlose Telekommunikationssysteme (u.a. GSM, UMTS, LTE), Satellitensysteme, Rundfunksysteme (DAB, DVB) und drahtlose lokale Netze (u.a. WLAN, Bluetooth).

In der Wahlpflichtveranstaltung „Sichere Mobile Systeme“ werden zum einen verschiedene Kommunikationsstandards (u.a. WLAN, Bluetooth, und IEEE 802.15.4) vorgestellt, die im Bereich IoT ihren Einsatz finden, welche Einschränkungen sie haben und welche Sicherheitsaspekte sie erfüllen. Zum anderen werden konkrete Anwendungen wie elektronische Ausweise, Gesundheitskarte und mobiles Bezahlen näher betrachtet.

Ergänzend zu den Grundlagen werden in der Vorlesung Sensorik und Manipulationsdetektion Algorithmen, Protokolle und Paradigmen für den Einsatz von Sensornetzen sowie deren Absicherung vorgestellt. Dabei werden Konzepte wie etwa Lokalisierung, Zeitsynchronisation und datenzentrische Ansätze betrachtet sowie Lösungen für System-Software, Aggregation, Routing und Datenverteilung aus der Perspektive von Sensornetzen betrachtet. Ferner behandelt die Vorlesung Grundlagen, Systeme und Verfahren zur Detektion von Manipulationen. Dies beinhaltet die gesicherte Informationsübertragung in verteilten Systemen sowie die Bestätigung und Überprüfung von detektierten Ereignissen durch verschiedene Methoden.

Leistungsnachweis
Notenschein
Dauer und Häufigkeit
Das Modul dauert 2 Trimester.

Modulname	Modulnummer
Staatliche IT-Sicherheit	5514

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Ulrike Lechner	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55141	VÜ	Schutz von kritischen Infrastrukturen	Pflicht	3
55144	SE	Internationale Sicherheitsarchitekturen und Krisenmanagement im Cyberraum	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Allgemeinwissen in Themen der IT-Sicherheit und zu IT-Sicherheitsmaßnahmen, so wie es in einem Bachelor Informatik oder Wirtschaftsinformatik vermittelt wird.

Qualifikationsziele

- Studierende kennen Sicherheitsarchitekturen national und international mit wesentlichen Akteuren
- Studierende kennen gesetzliche Grundlagen, Normen und Standards der IT-Sicherheit Kritischer Infrastrukturen
- Studierende kennen IT-Sicherheitsmaßnahmen für Kritische Infrastrukturen, die Technik, Mensch und Organisation adressieren
- Studierende kennen Verfahren, IT-Sicherheitsmaßnahmen zu konzipieren und umzusetzen.

Inhalt

Die Veranstaltung „IT-Sicherheit Kritischer Infrastrukturen“ thematisiert gesetzliche Grundlagen der IT-Sicherheit Kritischer Infrastrukturen und die Umsetzung der gesetzlichen Forderungen in den verschiedenen Sektoren der Kritischen Infrastrukturen.
Eine Fallstudienserie zu IT-Sicherheit Kritischer Infrastrukturen sowie konkrete Anwendungsbeispiele aus den Sektoren Kritischer Infrastrukturen stellen den Kern der Veranstaltung dar. Studierende lernen sowohl anhand von Fallbeispielen als auch anhand von Rahmenwerken wie den BSI IT-Grundschutz-Katalogen IT-Sicherheitsmaßnahmen kennen. Sie lernen Verfahren kennen, IT-Sicherheitsmaßnahmen für Kritische Infrastrukturen zu konzipieren, umzusetzen sowie zu evaluieren.

In der Veranstaltung „IT-Sicherheit in der zivilen Sicherheit“ ist die Sicherheitsarchitektur Deutschlands im Kontext nationaler und internationaler Sicherheitsarchitekturen mit Gesetzgebung und wesentlichen Organen Thema. Weitere Themen der Veranstaltung

sind Netzpolitik und Digitale Souveränität sowie Privatheit und Schutz der Privatsphäre. Studierende lernen abstrakte Konzepte sowie Fallbeispiele zu unterschiedlichen Themen der zivilen Sicherheit und IT-Sicherheit kennen.

Staatliche IT-Sicherheit mit dem Fokus auf Security- und Krisenmanagement thematisiert die Resilienz der Gesellschaft sowie das Management von Krisen und das Management von Sicherheit. Thema der Veranstaltung sind Geschäftsmodelle und Innovationsansätze genau wie gesetzliche Grundlagen. Studierende lernen wichtige Konzepte und Methoden sowie ausgewählte Fallbeispiele kennen.

In der Veranstaltung „Internationale Sicherheitsarchitekturen und Krisenmanagement im Cyberraum“ sind die Sicherheitsarchitektur Deutschlands im Kontext nationaler und internationaler Sicherheitsarchitekturen Thema. Es werden die zugrunde liegenden Gesetzgebungen und zuständigen Behörden auf deutscher und europäischer Ebene behandelt. Dies wird im Kontext der Netzpolitik und Digitale Souveränität thematisiert. IT-Standardisierung und Privatheit sowie Schutz der Privatsphäre werden dabei vertieft. Weitere Themen sind das Management von IT-Security in Unternehmen und Behörden sowie das Management von Cyber-Krisen sowohl in privaten Unternehmen als auch im Fall staatenübergreifender Konflikte. Die Studierenden lernen politische Konzepte und deren Umsetzung zu unterschiedlichen Themen der zivilen IT Sicherheit kennen.

Leistungsnachweis
Der Leistungsnachweis erfolgt als Notenschein mit Präsentationen, schriftlichen Ausarbeitungen und Fallstudien. Die Prüfungsform wird zu Beginn des Moduls festgelegt.
Dauer und Häufigkeit
Das Modul dauert 1-2 Trimester.
Sonstige Bemerkungen
Neben der Pflichtveranstaltung ist eine der Wahlpflicht-Veranstaltungen zu belegen.

Modulname	Modulnummer
Industrial Security	5521

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
N.N.	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55211	VÜ	Internet of Things and Industrial Internet Security	Wahlpflicht	3
55212	P	Praktikum Sicherheit eingebetteter Systeme	Wahlpflicht	3
55213	VÜ	Trusted Computing	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Gute Kenntnisse der Hardwaresicherheit, wie im gleichnamigen Modul vermittelt. Gute Kenntnisse in imperativer und systemnaher Programmierung.

Qualifikationsziele

Studierende entwickeln ein vertieftes Verständnis für die aktuellen Sicherheitsdefizite bei den bislang in Consumer-Geräten und z.B. in Industrieproduktionsanlagen verbauten eingebetteten Systemen. Sie kennen Algorithmen und Protokolle aus dem Bereich Lightweight Cryptography, deren Einsatzgebiete und die mit ihnen verbundenen Kompromisse. Die Studierenden können das in IoT- und Industrie-4.0-Szenarien erreichte Sicherheitsniveau bewerten und geeignete Schutzmaßnahmen auswählen. Sie können eigene Seitenkanalanalysen durchführen und auf eingebetteten Systemen ablaufende Algorithmen gegen entsprechende Angriffe schützen.

Inhalt

Die Vorlesung Internet of Things and Industrial Internet Security vertieft die IT-Sicherheit eingebetteter Systeme im Kontext von Cyber-Physical Systems. Dabei werden zum einen Endanwender-Anwendungsgebiete wie Smart Homes und Bestandteile kritischer Infrastrukturen wie Smart Meters mit den dort eingesetzten Schutzmaßnahmen für Kommunikationsprotokolle, Manipulationssicherheit und Datenschutz betrachtet. Zum anderen werden industrielle Anwendungsgebiete wie vernetzte Produktionsanlagen und organisationsübergreifender Datenaustausch im Rahmen von Supply Chains und die mit ihnen verbundenen Risiken analysiert. Durch die beschränkte Leistungsfähigkeit der eingesetzten Embedded Systems müssen insbesondere bei der Anwendung kryptographischer Verfahren Kompromisse eingegangen werden; ausgewählte Algorithmen und ihre Anwendung in Form von

Kommunikationsprotokollen der Lightweight Cryptography werden eingeführt und bezüglich ihrer Sicherheitseigenschaften mit herkömmlichen Chiffren und Message Authentication Codes gegenübergestellt.

Das Praktikum Embedded Systems Security bietet die Möglichkeit, ausgewählte Angriffe und Gegenmaßnahmen, die im Modul Hardwaresicherheit behandelt werden, im Labor in kleinen Gruppen selbst durchzuführen und zu vertiefen. Der Quelltext der auf Kleinstrechnern laufenden Programme muss dabei z.B. gegen Timing-Angriffe und Messungen des Stromverbrauchs gehärtet werden. Weitere Aufgaben umfassen z.B. das Reverse-Engineering und Nachbilden von Protokollen, wie sie z.B. für Smart-Home-Geräte eingesetzt werden könnten.

Leistungsnachweis
Notenschein, der sich aus Teilleistungen zu den beiden Lehrveranstaltungen zusammensetzt. Die jeweilige Prüfungsform für die Teilleistungen wird zu Beginn des Moduls bzw. der Lehrveranstaltungen festgelegt.
Dauer und Häufigkeit
Das Modul dauert 1-2 Trimester.

Modulname	Modulnummer
Privacy-Enhancing Cryptography	5548

Konto	Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Mark Manulis	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55481	VÜ	Advanced Cryptography	Pflicht	4
55482	SE	Seminar Research Trends in Privacy Tech	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Von den Studierenden werden grundlegende Kenntnisse von kryptographischen Verfahren und mathematischen Grundlagen aus dem Pflichtmodul "Kryptologie" sowie ein generelles Interesse an Privacy Tech und an der Verwendung von kryptographischen Verfahren zum Schutz der Privatheit vorausgesetzt.

Qualifikationsziele

Die Studierenden kennen verschiedene Konzepte und Verfahren zum Schutz der Privatheit mittels kryptographischer Methoden und beherrschen den Umgang mit entsprechender Sicherheitsmodellierung und -beweisführung. Sie sind in der Lage die technischen Lösungen zum Schutz der Privatheit kritisch zu analysieren und kennen den aktuellen Stand in Forschung und Entwicklung rund um die Technologien zum Schutz der Privatheit und deren Anwendungen.

Inhalt

Advanced Cryptography: In dieser Vorlesung werden moderne kryptographischen Methoden sowie weiterführende kryptographischen Verfahren und Protokolle vorgestellt. Neben der Funktionsweise wird auch auf die beweisbare Sicherheit der Verfahren eingegangen. Dazu werden moderne Methoden zur Sicherheitsmodellierung und -beweisführung (z.B. kryptographische Reduktionen) eingeführt. Aus der Sicht der beweisbaren Sicherheit werden sowohl die bereits bekannten Verfahrensklassen wie Einwegfunktionen, Hashfunktionen, digitale Signaturen und Verschlüsselungsverfahren wiederholt sowie neue Verfahren, wie etwa authenticated encryption, signcryption, zero-knowledge Protokolle, Identifikationsverfahren und Schlüsselvereinbarungsprotokolle vorgestellt. Zudem werden neue mathematischen Grundlagen und Verfahren basierend auf elliptischen Kurven und bilinearen Abbildungen eingeführt. In Übungen werden die Methoden der beweisbaren Sicherheit sowie die Funktionsweise von eingeführten Verfahren anhand von Rechen- und Beweisbeispielen anschaulich dargestellt.

Seminar Research Trends in Privacy Tech: In diesem Seminar wird den Studierenden ein Einblick in aktuelle Forschungsfelder rund um die technologischen Aspekte der Privacy gewährt. Die Schwerpunkte liegen bei Verfahren, Technologien und Anwendungen zum Schutz der Privatheit von Nutzern, deren Daten und digitalen Transaktionen. Zu Beginn der Veranstaltung wird eine Auswahlliste von aktuellen Themen vorgestellt, die von Studierenden über die Dauer der Veranstaltung ausgearbeitet und am Ende vorgetragen werden. Die Arbeiten sollen sich auf eine Auswahl relevanter Forschungsartikeln (aus bekannten Tagungen) und Open-Source Quellen (z.B. Softwarebibliotheken) stützen. Mögliche Themen rund um Privacy Tech sind etwa private messaging, anonymous communications, computing on encrypted data, secure multi-party computation, privacy in distributed ledgers und blockchain, electronic payments and cryptocurrencies, e-voting, privacy in IoT-Anwendungen, usw.

In allen Lehrveranstaltungen werden die Lehrmaterialien in englischer Sprache zur Verfügung gestellt. Die Veranstaltungen werden zum Teil auch in englischer Sprache gehalten.

Literatur

Katz, J. and Lindell, Y. Introduction to Modern Cryptography (2nd Edition), Chapman & Hall/CRC Cryptography and Network Security Series, 2014.

Leistungsnachweis

Notenschein, der zwei Teilleistungen umfasst. Die Prüfungsform wird zu Beginn des Moduls festgelegt.

Verwendbarkeit

Die hier erworbenen Kenntnisse und Fertigkeiten ergänzen die Ausbildung in IT-Sicherheit um die wichtigen technologischen Aspekte der Privatheit und entsprechenden kryptographischen Verfahren. Die Veranstaltungen fördern analytisches Denken nach Security & Privacy by Design und vermitteln die Fähigkeiten technische Verfahren zum Schutz der Privatheit zu entwerfen und ihr Einsatz in digitalen Anwendungen zu planen. Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit im Überschneidungsbereich des technologischen Privacy-Schutzes und angewandter Kryptographie.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester und wird im HT angeboten. Als Startzeitpunkt ist das 1. Studienjahr vorgesehen.

Modulname	Modulnummer
Analytische Modelle	1032

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Markus Siegle	Wahlpflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	96	174	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10321	VÜ	Quantitative Modelle	Pflicht	5
10322	VÜ	Verlässliche Systeme	Wahlpflicht	3
10323	VÜ	Zuverlässigkeitstheorie	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				8

Empfohlene Voraussetzungen

Wahrscheinlichkeitsrechnung auf Bachelor-Niveau wird vorausgesetzt. Voraussetzung ist ferner eine Vertrautheit mit Grundlagen der Architektur und des Entwurfs von Rechen- und Kommunikationssystemen.

Qualifikationsziele

Die Studierenden lernen, ein existierendes oder geplantes reales System auf ein Modell abzubilden und anhand des Modells Aussagen über die zu erwartende Leistungsfähigkeit und/oder Zuverlässigkeit zu machen. Sie werden in die Lage versetzt, die Zusammenhänge zwischen den diversen Parametern eines Systems und den zu erwartenden Leistungs- und Zuverlässigkeitskenngrößen zu verstehen. Die Studierenden sollten nach erfolgreicher Teilnahme an diesem Modul in der Lage sein, (Rechner-)Systeme performanter und verlässlicher zu entwerfen, bzw. existierende Systeme bezüglich Performance und Verlässlichkeit bewerten zu können.

Inhalt

Neben der Frage, ob ein Rechen- oder Kommunikationssystem seine funktionalen Anforderungen korrekt und vollständig erfüllt, spielt die Frage nach der Leistungsfähigkeit und Zuverlässigkeit des Systems eine zentrale Rolle. Modelle mit stochastischem Charakter sind ein wichtiges Hilfsmittel für die Leistungs- und Zuverlässigkeitsbewertung von Systemen.

In diesem Modul werden die Grundlagen solcher Modelle und ihrer quantitativen Analyse behandelt. Im Pflichtteil "Quantitative Modelle" werden einfache stochastische Prozesse, insbesondere Markov-Prozesse mit diskretem oder stetigem Zeitparameter eingeführt. Es werden wichtige Leistungs- und Zuverlässigkeitskenngrößen definiert und bestimmt. Wichtige Gesetzmäßigkeiten, wie das Gesetz von Little, werden erläutert. Es werden unterschiedliche Typen von Bediensystemen betrachtet, und schließlich verschiedene

Verfahren für die Analyse von Warteschlangennetzen und die numerische Analyse von Markovketten vorgestellt.

Die Wahlpflicht-Lehrveranstaltung "Verlässliche Systeme" fokussiert insbesondere auf Fehlertoleranz-Methoden und deren Bewertung zur Erhöhung der Systemzuverlässigkeit solcher Systeme. Neben zentralen Begrifflichkeiten werden Modellierungsmethoden wie Fehlerbäume, Zuverlässigkeitsblockdiagramme und Markov-Modelle für Systeme mit und ohne Reparaturen thematisiert.

In der alternativen Wahlpflicht-Lehrveranstaltung "Zuverlässigkeitstheorie" werden strukturelle Eigenschaften kohärenter Systeme betrachtet, d.h. die Funktionstüchtigkeit des Systems wird in Beziehung zur Funktionstüchtigkeit seiner Komponenten gesetzt. Die Studierenden lernen Methoden und Ansätze kennen, mit denen z.B. das Ausfall- und Überlebensverhalten von einzelnen Bauteilen oder Geräten (die als ein vernetztes System von Bauteilen aufgefasst werden können) modelliert und analysiert werden können.

Leistungsnachweis

Schriftliche Prüfung über 60 min oder mündliche Prüfung über 30 min. Voraussetzung für die Teilnahme an der Prüfung ist die erfolgreiche Bearbeitung von Aufgaben während der Übungen und zu Hause. Der Prüfungsmodus und die Details zur Aufgabenbearbeitung werden zu Beginn des Moduls bekannt gegeben.

Verwendbarkeit

Angesichts der hohen Leistungs- und Zuverlässigkeitsanforderungen an informationsverarbeitende Systeme in den unterschiedlichsten Anwendungsbereichen (z.B. verteilte eingebettete Systeme, Prozesssteuerungen, sicherheitskritische Systeme, Workflow-Systeme oder paralleles wissenschaftliches Rechnen) bilden die erworbenen Kenntnisse einen wichtigen Bestandteil der Ausbildung von Informatikern.

Dauer und Häufigkeit

Das Modul dauert 2 Trimester.
Das Modul beginnt jedes Studienjahr jeweils im Frühjahrstrimester.
Als Startzeitpunkt ist das Frühjahrstrimester im 1. Studienjahr vorgesehen.

Sonstige Bemerkungen

In diesem Modul ist neben der Pflichtveranstaltung (mit Übung) eine der beiden Wahlpflichtveranstaltungen (mit Übung) zu wählen.

Modulname	Modulnummer
Informations- und Codierungstheorie	1037

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. rer. nat. Peter Hertling	Wahlpflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	60	120	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
1037	VÜ	Informations- und Codierungstheorie	Wahlpflicht	5
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen
Es werden Grundkenntnisse in Analysis, linearer Algebra und Wahrscheinlichkeitstheorie vorausgesetzt.

Qualifikationsziele
Die Studierenden lernen einerseits grundlegende theoretische Begriffe zur Übertragung von Information durch einen Bitstrom kennen, sowie prinzipielle Grenzen der Informationsübertragung. Andererseits lernen sie wichtige Codierungsmethoden kennen, die in der digitalen elektronischen Datenübertragung verwendet werden. Sie lernen zu beurteilen, welche Codierungsmethoden in welcher Situation vorzuziehen sind. Außerdem sollen sie selbst Algorithmen zur Codierung und Decodierung (auch Fehlerkorrektur) implementieren können.

Inhalt
Grundlegende Fragen der Informationsverarbeitung sind, wieviel Information man in einen Bitstrom hineincodieren kann und wieviel Information man durch das Senden eines Bitstroms in einer bestimmten Zeit von einem Ort zu einem anderen Ort übertragen kann, wenn der Bitstrom nur mit einer bestimmten Geschwindigkeit gesendet werden kann und die Sendung womöglich noch gestört wird. Diese Fragen werden in der Shannonschen Informationstheorie behandelt, die Inhalt dieser Veranstaltung ist. Dazu werden Grundbegriffe zu Codes eingeführt, der Begriff der Entropie, Nachrichtenquellen und Kanäle. Ziele sind der Quellencodierungssatz und der Kanalcodierungssatz von Shannon. Anschließend werden in der Praxis wichtige Codierungsmethoden behandelt z.B. lineare Codes und Faltungscodes. Es werden Algorithmen und Ergebnisse zu derartigen Codierungsmethoden und zur Decodierung und Fehlerkorrektur einer übertragenen, codierten, aber möglicherweise gestörten Nachricht behandelt werden. Am Ende soll noch eine kurze Einführung in die algorithmische Informationstheorie gegeben werden.

Leistungsnachweis
Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer. Die Art der Prüfung wird zu Beginn des Moduls bekannt gegeben.
Verwendbarkeit
Die Kenntnis der Inhalte dieses Moduls ist sehr nützlich für eine spätere Beschäftigung mit Datenübertragung und elektronischen Kommunikationssystemen
Dauer und Häufigkeit
Das Modul dauert 1 Trimester. Es beginnt immer im Wintertrimester, wird aber nicht in jedem Studienjahr angeboten. Die konkreten Angebotstermine können der Lehrveranstaltungsplanung der Fakultät für Informatik entnommen werden.

Modulname	Modulnummer
Knowledge Discovery in Big Data	1144

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. phil. Michaela Geierhos	Wahlpflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
11441	VÜ	Knowledge Discovery	Wahlpflicht	3
11442	VÜ	Methoden der Data Science	Wahlpflicht	3
11443	SE	Research Topics in Data Science	Wahlpflicht	3
11444	VÜ	Big Data Management	Wahlpflicht	3
11445	SE	Datenethik und -sicherheit	Wahlpflicht	3
11446	P	Data Science Praktikum	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Die Studierenden sollen grundlegende Kenntnisse in Programmierung und Software-Entwurf sowie ein Grundverständnis von Algorithmen und Datenstrukturen haben.

Qualifikationsziele

Lernziele sind das kompetente Beherrschen grundlegender Verfahren und Methoden sowie ihrer praktischen Anwendung in den unter Inhalte dargestellten Bereichen.

Inhalt

- In der Vorlesung „Big-Data-Management“ lernen die Studierenden Architekturen kennen, die für die Erfassung, Verarbeitung und Analyse von Big Data konzipiert sind, wofür sich herkömmliche Datenbanksysteme nicht mehr eignen. In diesem Zusammenhang wird nicht nur die verteilte Big-Data-Infrastruktur behandelt, sondern auch Themen wie Datenstrukturierung, Datensynchronisation/Parallelität und Speicherverwaltung in den Fokus gerückt. In der Übung werden erste Erfahrungen mit Big-Data-Architekturen gemacht.
- In der Vorlesung „Knowledge Discovery“ geht es um den Umgang mit heterogenen Datenquellen, deren Kategorisierung sowie deren Analyse. Hierfür werden Methoden wie u.a. Visual Analytics/Knowledge sowie Techniken des Discovery & Data Mining und die explorative Datenanalyse unter Zuhilfenahme von KI-Methoden wie z. B. Machine Learning oder Computational Intelligence vorgestellt und in den Übungen praktisch vertieft.
- In der Vorlesung „Methoden der Data Science” werden grundlegende Konzepte und Methoden entlang eines Data Science Projektzyklus, von der Formulierung der

Problemstellung über die Sammlung, Vorbereitung und Visualisierung der Daten bis hin zur Erkennung von Mustern und Trends in diesen mittels Verfahren des maschinellen Lernens (z. B. Regression, Klassifikation, Clustering) vermittelt. Das erlernte Methodenwissen wird kontinuierlich durch praxisnahe Übungen mit der Programmiersprache Python angewandt und vertieft.

- Im Seminar „Research Topics in Data Science“ werden ausgewählte, aktuelle Methoden aus dem Bereich Data Science, Machine Learning und Deep Learning vorgestellt. Das Seminar soll den Studierenden einen Einblick in State-of-the-Art Forschungsthemen geben. Die behandelten Themen orientieren sich am aktuellen Gartner Hyper Cycle for Artificial Intelligence (wie bspw. Decision Intelligence, Responsible AI, Knowledge Graphs) und dem Gartner Hype Cycle for Emerging Technologies (wie bspw. Self-Supervised Learning, Explainable AI, Social Data).
- Im Seminar „Datenethik und -sicherheit“ werden u.a. Fragen der Datenethik diskutiert, um einen kritischen und verantwortungsvollen Umgang mit Daten und dem daraus gewonnenen Wissen zu erlernen. Behandelt werden ethische und legale Fragen in Bezug auf AI- und Data Science-Anwendungen, welche einen großen Einfluss auf die Gesellschaft haben (z. B. autonomes Fahren, Social Media Plattformen, Tools zur medizinischen und juristischen Entscheidungsfindung). Ferner lernen die Studierenden, wie man AI- und Data Science-Applikationen kontrolliert anwendet, um der Gesellschaft und individuellen Personen zu nutzen, und möglichen Schaden in Bezug auf Datensicherheit und Datenschutz zu vermeiden. In der Übung soll das Wissen zu ethischen Implikationen genutzt werden, um Strategien und Konzepte für ethische Anwendungen zu entwickeln.
- Im „Data Science Praktikum” wir das in der Theorie gelernte Wissen in einem Projekt praktisch implementiert. Die Studierenden werden in Kleingruppen an einem größeren Projekt im Bereich Data Science arbeiten und dies am Ende des Trimesters präsentieren. Das Projekt umfasst dabei einen gesamten Projektzyklus – von der Idee und Konzeption, über die Datensammlung und deren Aufbereitung bis hin zum Tainieren eines Machine Learning-Modells und Auswertung der Ergebnisse. Das Plenum bietet dabei einen regelmäßigen Austausch und Feedback zwischen den Gruppen. Themen der Projekte beziehen sich auf die kennengelernten Forschungsbereiche aus „Research Topics in Data Science“ und „Methoden der Data Science“. Es wird dringend empfohlen einen der o.g. Kurse besucht zu haben.

Leistungsnachweis

Das gesamte Modul wird per Notenschein geprüft, mit Anteilen von je 3 ECTS-LP zu jeder der Vorlesungen (mit Übung), zu jedem Seminar und im Praktikum. Die Studierenden können (je nach Angebot) entweder zwei Vorlesungen mit Übungen oder zwei Seminare oder eine Vorlesung mit Übung und ein Praktikum oder eine Vorlesung mit Übung und ein Seminar einbringen – was insgesamt die 6 ECTS-LP des Moduls ergibt.

Verwendbarkeit

Die hier erworbenen Kenntnisse und Fertigkeiten ergänzen die Ausbildung im Bereich der Softwaretechnik um einen Aspekt von hoher praktischer Bedeutung. Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit im Bereich Data Science.

Dauer und Häufigkeit

Das Modul dauert 2 bis 3 Trimester und beginnt jedes Jahr im FT.

Sonstige Bemerkungen
Die Vorlesungen, Seminare und das Praktikum werden nicht alle jedes Jahr angeboten, aber in jedem Jahr mindestens so viele Lehrveranstaltungen, dass 6 ECTS-Leistungspunkte erreichbar sind. Jeweils zu Beginn des Moduls wird den Studierenden das konkrete Angebot erläutert.

Modulname	Modulnummer
Visual Computing (erweitert)	1152

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Helmut Mayer	Wahlpflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
11521	VÜ	Computer Vision	Pflicht	3
11522	VÜ	Computer Vision und Graphik	Wahlpflicht	3
11523	VÜ	Bildverarbeitung für Computer Vision	Pflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

- Kenntnisse der Mathematik und Physik.
- Grundkenntnisse der digitalen Signalverarbeitung sind hilfreich.

Qualifikationsziele

In der Vorlesung und den Übungen zu Bildverarbeitung für Computer Vision erwerben Studierende vertiefte Kenntnisse über Techniken der Bildverarbeitung, die in Computer Vision verwendet werden, auch in Form der praktischen Auswertung von Bildern.
Sie kennen grundlegende Methoden wie Bildtransformationen, Segmentierung, Binärbildverarbeitung sowie Merkmalsextraktion und können diese sinnvoll kombinieren. Damit können sie abschätzen, welche Methoden sich in Abhängigkeit von Faktoren wie Genauigkeit, Robustheit und Geschwindigkeit besonders gut für welches Einsatzgebiet eignet.

Mittels der Vorlesung und Übungen zu Computer Vision erwerben Studierende vertieftes Wissen über die Rekonstruktion von 3D Geometrie aus perspektiven Bildern. Sie kennen verschiedene Techniken, die eine Poseschätzung mit und ohne Wissen über den Aufbau der Kamera (Kalibrierung) ermöglichen. Sie können diese zusammen mit Wissen über Bildzuordnung und robusten statistischen Verfahren anwenden, um die relative Pose für Bildpaare auch bei groben Fehlern in der Zuordnung zu schätzen. Damit sind die Studierenden grundsätzlich in der Lage, die Posen für weit auseinander liegende Aufnahmen (wide-baseline) zu bestimmen.

Das Ziel der Vorlesung und Seminarübung zu Computer Vision und Graphik besteht darin, den Studierenden vertieftes Wissen zu Techniken der automatischen Extraktion von Objekten aus Bildern zu vermitteln. Weiterhin bekommen die Studierenden die Fähigkeit, dichte Tiefendaten durch Bildzuordnung zu generieren, mittels derer realistische 3D Visualisierungen erzeugt werden können. Die Studierenden erhalten

neben breitem Wissen zur aussehensbasierten Extraktion auf Grundlage von ähnlichem Aussehen und ähnlicher Anordnung von kleinen Bildausschnitten insbesondere ein Verständnis der Möglichkeiten, die sich durch eine Kopplung von Computer Vision und Graphik in Form von generativen Modellen ergeben. Mittels eines Vortrags lernen die Studierenden die Einordnung eines spezifischen Themas in den Rahmen der Techniken von Computer Vision und Graphik.

Inhalt

Die Vorlesung Bildverarbeitung für Computer Vision geht von der Bildgewinnung aus. Es wird gezeigt, wie Bilder und Bildausschnitte mittels statistischer Maße, wie z.B. Varianz und Korrelationskoeffizient, charakterisiert werden können. Bildtransformationen verändern entweder die Radiometrie oder die Geometrie der Bilder. Mittels lokaler Transformationen werden Kanten hervorgehoben oder Störungen beseitigt. Die Bildsegmentierung, die z.B. auf Grundlage einzelner Pixel oder Regionen-orientiert erfolgen kann, führt zu homogenen Bildbereichen. Für die Verarbeitung binärer Bilder, d.h. Bilder mit nur zwei Grauwerten, werden Verfahren vorgestellt, die spezielle Formen herausarbeiten (mathematische Morphologie). Auf Grundlage aller bis dahin vorgestellter Techniken wird es mögliche, Merkmale, d.h. nulldimensionale (0D)-Punkte, 1D-Kanten / Linien und 2D Flächen zu extrahieren. Für Flächen wird deren Umsetzung in Vektoren inkl. Graphbildung und Polygonapproximation aufgezeigt.

Die Vorlesung Computer Vision legt zuerst Grundlagen der projektiven Geometrie. Für das Einzelbild wird die Modellierung mittels Projektionsmatrix und Kollinearitätsgleichung dargestellt und daraus die Rekonstruktion der Orientierung auf Grundlage der Direkten Linearen Transformation und die hoch genaue Bündellösung abgeleitet. Die relative Orientierung des Bildpaars kann mittels Fundamentalmatrix, essentieller Matrix und Homographie direkt bestimmt werden, daneben wird aber auch die hoch genaue Bündellösung dargestellt. Für drei und mehr Bilder wird der Trifokaltensor vorgestellt. Da reale Kameras nicht der idealen Zentralperspektive entsprechen, wird auf Objektivfehler eingegangen. Um Bilder orientieren zu können, sind korrespondierende Punkte oder Linien in den Bildern notwendig. Hierfür werden Grundlagen der Bildzuordnung dargestellt. Darauf aufbauend wird dargestellt, wie Bildpaare, -tripel und -sequenzen automatisch orientiert werden können und welche Probleme hierbei auftreten. Die bei der Orientierung der Bilder entstehenden 3D Punkte füllen den Raum nur unzureichend. Um eine realistische 3D Darstellung zu ermöglichen, werden Verfahren zur dichten Tiefenschätzung vorgestellt. Zuletzt werden an Hand der 3D Rekonstruktion aus Bildern von Unmanned Aircraft Systems (UAS) und der (Echtzeit) Navigation Möglichkeiten aber auch Probleme dargestellt.

Die Vorlesung Computer Vision und Graphik führt zuerst in die Modellbildung für die Objektextraktion mit Objekten (Geometrie und Radiometrie), Relationen, Kontext und Ebenen der Extraktion ein. Für die aussehensbasierte Objektextraktion werden Verfahren zur Detektion und Beschreibung von kleinen Bildausschnitten, z.B. SIFT, und zum Vergleich der Anordnung, wie z.B. Schätzung der Homographie mit RANSAC oder Hough-Transformation vorgestellt. Generative Modelle beruhen auf einer möglichst realistischen Visualisierung. Hierfür werden verschiedene Techniken der (Computer) Graphik vorgestellt und es wird aufgezeigt, wie diese in Graphik-Hardware realisiert werden. Die Extraktion der Objekte beruht auf a priori Annahmen (Priors) über die Geometrie und Radiometrie der Objekte. Der Vergleich von Visualisierung und realem Bild führt zu Likelihoods. Die Modelle werden auf Grundlage der Priors statistisch

modifiziert und die Lösung als MAP (Maximum a posteriori) Schätzung bestimmt. Hierfür werden Techniken wie (Reversible Jump) Markov Chain Monte Carlo (MCMC) verwendet. Es wird die Extraktion topographischer Objekte, vor allem Gebäudefassaden und Vegetation aus terrestrischen Daten, aber auch von Straßen aus Luft- und Satellitenbildern dargestellt. Weitere Anwendungen werden in Seminarvorträgen vorgestellt und diskutiert.

Leistungsnachweis
Schriftliche Prüfung von 90 min oder mündliche Prüfung von 30 min (normalerweise am Ende des HT). Voraussetzung für die Teilnahme an der Prüfung ist die erfolgreiche Bearbeitung von Übungen und Seminarübungen.
Verwendbarkeit
Das Modul gibt Grundlagen für praktische Anwendungen im Bereich von Visual Computing.
Dauer und Häufigkeit
Das Modul dauert 2 Trimester. Das Modul beginnt jedes Studienjahr jeweils im Frühjahrstrimester. Als Startzeitpunkt ist das Frühjahrstrimester im 1. Studienjahr vorgesehen.
Sonstige Bemerkungen
Die Vorlesungen und Übungen Bildverarbeitung für Computer Vision und Computer Vision liegen im Frühjahrstrimester im 1. und die Seminarübung Computer Vision und Graphik im Herbsttrimester des 2. Studienjahres.

Modulname	Modulnummer
Quellencodierung und Kanalcodierung	1220

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Andreas Knopp	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
150	60	90	5

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
12201	VÜ	Quellencodierung und Kanalcodierung	Wahlpflicht	5
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

- Mathematik A, B,C
- Wünschenswert sind Kenntnisse der Signalverarbeitung (z.B. Module „Signalverarbeitung und Informationsverarbeitung digitale Regelung und Sensornetze" oder „Signalverarbeitung und Übertragungssysteme der Hochfrequenztechnik" oder „Digitale Signalverarbeitung")
- Wünschenswert sind Kenntnisse der Mobilkommunikation
- Wünschenswert sind Kenntnisse der Kommunikationstechnik, wie sie in den Vorlesungen „Signale und Kommunikationssysteme" und „Kommunikationstechnik I" (BA-Modul „Kommunikationstechnik") und „Kommunikationstechnik II" (MA-Modul „Informationsverarbeitung und Kommunikationstechnik" oder „Kommunikationstechnik B") vermittelt werden

Qualifikationsziele

- Grundkenntnisse der Quellencodierung und beispielhafte Quellencodierverfahren
- Grundkenntnisse der informationstheoretischen Grundlagen der Kanalcodierung
- Kenntnisse grundlegender Codierverfahren und ihrer Decodierung
- Kenntnisse zur analytischen Untersuchung von Codierverfahren
- Verständnis des Turbo-Prinzips zur iterativen Decodierung und Verständnis der Anwendung dieses Prinzips bei anderen Detektionsproblemen
- Kenntnis von Codierungsverfahren in kommerziellen Systemen
- Verständnis der praktischen Probleme bei der Implementierung von Codierungsverfahren in kommerziellen Systemen
- Fähigkeit zur Abgrenzung von Quellen- und Kanalcodierung nach Zweck, Wirkungsweise und Einsatzgebieten

Inhalt

- Kurzeinführung in die Informationstheorie
- Quellencodierungstheorem

- Grundlegende Quellencodierverfahren: Huffman code, Shannon-Fano Algorithmus, Lempel-Ziv Algorithmus
- Kanalcodierungstheorem
- Kanalkapazität verschiedener Übertragungskanäle
- Prinzip der Kanalcodierung
- Prinzip der Maximum-Likelihood und Maximum-A-Posteriori Decodierung
- Soft-in soft-out Decodierung
- Lineare Blockcodes
- Analytische und simulative Bestimmung der Fehlerwahrscheinlichkeit von Blockcodes
- Low Density Parity Check (LDPC) Codes:

  # Tanner Graphen

  # Message Passing Decodierung
- Faltungscodes und Viterbi-Decodierung
- Verkettete Codes und iterative Decodierung:

  # Parallel und seriell verkettete Codes, Turbo-Codes

  # Turbo-Decodierung

  # Beurteilung und Konstruktion von Codes mithilfe von EXIT Charts (Grundlagen)

  # MAP Decodierung mit dem BCJR Algorithmus (Grundlagen)
- Anwendungen von Quellencodierung und Kanalcodierung in kommerziellen Systemen (u.a. CD, DVD, Funkkommunikation)

Leistungsnachweis

Mündliche Modulprüfung von 30min Dauer (mP-30) oder schriftliche Prüfung von 60min Dauer (sP-60)

Verwendbarkeit

- Pflichtmodul für die Vertiefungsrichtung ME-VSK im Studiengang Mathematical Engineering (M. Sc.)
- Wahlpflichtmodul für die Vertiefungsrichtungen ME-EET, ME-Mechatronic und ME-PTM im Studiengang Mathematical Engineering (M. Sc.)
- Wahlpflichtmodul für den Masterstudiengang EIT in den Vertiefungsrichtungen EIT-KT und EIT-ES

Dauer und Häufigkeit

Das Modul dauert 1 Trimester, beginnt jedes Studienjahr, Startzeitpunkt ist das HT im 1. Studienjahr (10tes Trimester)

Modulname	Modulnummer
Data Mining und IT- basierte Entscheidungsunterstützung	1231

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Stefan Pickl	Pflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	60	120	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
12311	VÜ	Data Mining und IT-basierte Entscheidungsunterstützung	Pflicht	5
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

Grundkenntnisse zu mathematischen Methoden des Operations Research und der Statistik wie sie z.B. im Bachelor Informatik bzw. Wirtschaftsinformatik vermittelt werden.

Qualifikationsziele

Lernziele sind das kompetente Beherrschen grundlegender Verfahren und Methoden sowie ihrer praktischen Anwendung in den unter Inhalte dargestellten Bereichen.

Inhalt

Die Studierenden sollen in dieser Veranstaltung mit den IT-basierten und entscheidungstheoretischen Grundlagen im Bereich der modernen Datenanalyse vertraut gemacht werden; insbesondere im Hinblick auf die Strukturierung von Entscheidungsproblemen, die Entwicklung von geeigneten Analyseverfahren zur Erforschung von komplexen datenbasierten Zusammenhängen ("Exploratory Analysis"). Data Mining bedeutet dabei das Extrahieren von impliziten, noch unbekannten Informationen aus Rohdaten. Dazu sollten IT-Systeme in die Lage versetzt werden, Datenbanken und Datenansammlungen (z.B. im Bereich der Geoinformatik) automatisch nach Gesetzmäßigkeiten und Mustern zu durchsuchen und einen Abstraktionsprozess durchzuführen, der als Ergebnis aussagekräftige Informationen liefert. Insbesondere das heutige maschinelle Lernen und das Verfahren des "Datafarming" stellen dafür die Werkzeuge und Techniken zur Verfügung, die in den Bereich des modernen Wissensmanagements (bis zur Begriffsanalyse) und "Datamining" hineinführen.

Literatur

- Decision Support Systems Developing Web-Enabled Decision Support Systems, Abhijit A. Pol and Ravindra K. Ahuja. Dynamic Ideas 2007.
- Exploratory Data Analysis Making Sense of Data: A Practical Guide to Exploratory Data Analysis and Data Mining, Glenn J. Myatt. John Wiley, 2006.
- Spatial Data Analysis Spatial Data Analysis - Theory and Practice, Robert Haining, Cambridge University Press 2003.

- Data Mining Data Mining: Practical Machine Learning Tools and Techniques (Second Edition) Ian H. Witten, Eibe Frank. Morgan Kaufmann 2005.
- Data Mining: A Knowledge Discovery, K. Cios, W. Pedrycz, R. Swiniarski Springer, 2007.
- Data Mining Introductery and Advanced Topics, Margaret Dunham, Prentice Hall, 2003.
- Advances in Knowledge Discovery and Data Mining, U. Fayyad, G. Piatetsky-Shapiro, P. Smyth, R. Uthurusamy, editors , MIT Press, 1996.
- Data Mining: Concepts and Techniques, Jiawei Han, Micheline Kamber. Morgan Kaufmann, 2006.
- Principles of Data Mining, David J. Hand, Heikki Mannila and Padhraic Smyth. MIT Press, 2000. Daniel T. Larose,
- Discovering Knowledge in Data: An Introduction to Data Mining, John Wiley 2004. Robert Nisbet, John Elder, IV and Gary Miner.
- Handbook of Statistical Analysis and Data Mining Applications. Elsevier 2009.
- Statistical Learning - Machine Learning Trevor Hastie, Robert Tibshirani, Jerome Friedman,
- The Elements of Statistical Learning: Data Mining, Inference, and Prediction, Springer Verlag, 2001. Mehmed Kantardzic, Data Mining: Concepts, Models, Methods, and Algorithms, Wiley-IEEE Press, 2002.

Weiterführende Literatur:

- Zeitreihenanalyse Time Series Analysis. Hamilton 1994.
- Reinforcement Lernen und Spieltheorie Reinforcement Learning: An Introduction. Sutton and Barto: MIT Press 1998.
- Fun and Games: A Text on Game Theory. Binmore, Linster, Houghton Mifflin 2000.
- Statistik Bayesian Data Analysis. Gelman, Carlin, Stern, Rubin: Chapman 1995. Introduction to Mathematical Statistics. Hogg, Craig: Prentice Hall 2004.
- Principles of Statistics. Bulmer: Dover 1979.
- Probability, Random Variables and Stochastic Proc., Papoulis, McGraw, Hill 2002.

Leistungsnachweis

Mündliche (20min) oder schriftliche (60min) Modulprüfung.

Verwendbarkeit

Die Vorlesung kann durch weiterführende Veranstaltungen im Bereich der Datenanalyse fortgeführt werden, z.B. im Bereich der modernen Begriffsanalyse, des Algorithmic Engineering, im Rahmen von Spezialvorlesungen der Numerik und Statistik sowie der Geoinformatik. Ebenfalls bestehen enge Bezüge zu wissenschaftlichen Forschungsgebieten im Bereich der Künstlichen Intelligenz.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester.
Das Modul beginnt jedes Studienjahr jeweils im Wintertrimeste

Modulname	Modulnummer
Signal- und Informationsverarbeitung	1243

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Andreas Knopp	Pflicht	8

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
240	96	144	8

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
12431	VÜ	Signalverarbeitung	Pflicht	4
12432	VÜ	Informationsverarbeitung	Pflicht	4
Summe (Pflicht und Wahlpflicht)				8

Empfohlene Voraussetzungen

- Kenntnisse der Signal- und Systemtheorie
- Kenntnisse der Wahrscheinlichkeitsrechnung und stochastischer Prozesse
- Höhere Mathematik.

Qualifikationsziele

- Verständnis der mit dem Übergang vom kontinuierlichen Signal zum zeit- und wertdiskreten Signal einhergehenden Veränderungen von Signaleigenschaften
- Sicherer Umgang mit Schlüsseltechniken der digitalen Signalverarbeitung im Zeit- und Frequenzbereich
- Beherrschung von Entwurfs- und Analyseverfahren digitaler Filter
- Verständnis für die Anwendungsbreite von Schätzverfahren über die Zeit- und Frequenzbereichsschätzung hinaus
- Verständnis für die Prinzipien der statistischen Signalklassifikation
- Sicherer Umgang mit wesentlichen Algorithmen der räumlichen Signalanalyse

Inhalt

Modulteil Signalverarbeitung:

- Charakterisierung von Signalen:
  # Analoge und digitale Signale
  # Deterministische Signale und Zufallssignale
- Darstellung zeitkontinuierlicher und zeitdiskreter Signale in Zeit- und Frequenzbereich:
  # Fourier-Reihe
  # Fourier-Transformation
  # Laplace-Transformation
  # Z-Transformation
  # Zeitdiskrete Fourier-Transformation (DTFT)
- Zeitdiskrete lineare zeitinvariante Systeme (LTI-Systeme)

- Abtastung
- Zufallssignale
  # Zufallsvariablen
  # Stochastische Prozesse
- Grundlagen digitaler Filter
- Adaptive Filter
  # Minimum Mean Squared Error (MMSE) Filter, Wiener Filter
  # Least Mean Squares (LMS) Algorithmus
  # Recursive Least Squares (RLS) Algorithmus
- Diskrete Fourier-Transformation (DFT), Fast Fourier Transform (FFT)

Modulteil Informationsverarbeitung:
- Schnelle Faltung
- Spektralanalyse von deterministischen Signalen und Zufallssignalen
- Traditionelle und parametrische Spektralschätzung
- Parametrische und nicht parametrische Schätzung von weiteren Signalkenngrößen am Beispiel der Einfallswinkelschätzung mit Antennen-Arrays
- Higher-Order-Statistics (HOS) Schätzung von Modulationsart uns Signal-Rausch-Abstand
- Beurteilung der Schätzgüte mithilfe der Cramer-Rao-Bound
- Grundlagen der Sprach- und Bildverarbeitung

Literatur

• K.-D. Kammeyer, K. Kroschel: Digitale Signalverarbeitung. B.G. Teubner.
• A. Oppenheim, R. Schafer: Discrete-Time Signal Processing. Prentice Hall

Leistungsnachweis

Schriftliche Prüfung von 90min Dauer (sP-90) oder mündliche Prüfung von 30min Dauer (mP-30) am Ende des Frühjahrstrimesters. Wiederholungsmöglichkeit am Ende des Herbsttrimesters. Die genaue Art der Prüfung wird zu Beginn des Moduls bekannt gegeben.

Verwendbarkeit

- Pflichtmodul für die Vertiefungsrichtung "Kommunikationstechnik" im Studiengang EIT (M.Sc.)
- Wahlpflichtmodul für die Vertiefungsrichtung "Energietechnische Systeme" im Studiengang EIT (M.Sc.)
- Pflichtmodul für die Vertiefungsrichtung ME-VSK im Studiengang Mathematical Engineering (M.Sc.)
- Wahlpflichtmodul für die Vertiefungsrichtungen ME-EET, ME-Mechatronik und ME-PTM im Studiengang Mathematical Engineering (M.Sc.)
- Wahlpflichtmodul für das Anwendungsfach Elektrotechnik im Masterstudiengang INF (M.Sc.)
- Dieses Modul kann nicht gleichzeitig mit dem Modul 1249 eingebracht werden

Dauer und Häufigkeit

Das Modul dauert 2 Trimester.
Das Modul findet jedes Studienjahr im Wintertrimester und Frühjahrstrimester statt.
Als Startzeitpunkt ist das Wintertrimester im ersten Studienjahr vorgesehen.

Modulname	Modulnummer
Sicherheit in der Kommunikationstechnik	1253

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Berthold Lankl	Pflicht	0

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
12531	VÜ	Moderne Verfahren der Kanalcodierung und Decodierung	Pflicht	3
12532	VÜ	Übertragungssicherheit	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

• Höhere Mathematik
• Kenntnisse der Signal- und Systemtheorie wie sie in der Vorlesung „Signale und Kommunikationssysteme" (BA Modul „Kommunikationstechnik") erlernt werden sowie Kenntnisse von Kommunikationssystemgrundlagen, wie sie in der Vorlesung „Kommunikationssysteme I" (BA Modul „Kommunikationstechnik") erlernt werden sind wünschenswert.
• Hochfrequenztechnik 1 und 2, Übertragungssysteme der Hochfrequenztechnik
• Empfohlen: EMV in der Kommunikationstechnik

Qualifikationsziele

Lehrveranstaltung a):
• Grundkenntnisse der informationstheoretischen Grundlagen der Kanalcodierung
• Kenntnisse grundlegender Codierverfahren und ihrer Decodierung
• Kenntnisse zur analytischen Untersuchung von Codierverfahren
• Verständnis des Turbo-Prinzips zur iterativen Decodierung und Verständnis der Anwendung dieses Prinzips bei anderen Detektionsproblemen
• Kenntnis von Kanalcodierungsverfahren in kommerziellen Systemen
• Verständnis der praktischen Probleme bei der Implementierung von Kanalcodierungsverfahren in kommerziellen Systemen
Lehrveranstaltung b):
• Der Student/die Studentin kennt Verfahren und Methoden auf System- und Komponentenebene um die Übertragungssicherheit von Kommunikationssystemen zu bewerten und erlernt Fähigkeiten um Systeme mit erhöhter Übertragungssicherheit zu entwerfen.
• Die Studierenden gewinnen einen Einblick in die Problemstellungen der Sicherheit moderner Informations-Übertragungssysteme mit dem besonderen Hinblick auf drahtlose Systeme, welche in den letzten Jahren eine stetig zunehmende Bedeutung erlangt

haben. Hierbei werden zuerst Einschränkungen der Informationsübertragungen durch Störungen sowie der Abhörsicherheit durch elektromagnetische Kopplungseffekte und Übersprechen betrachtet, woraufhin die technischen Lösungen zur Reduzierung dieser Einschränkungen dargestellt werden. Den Studierenden wird die Fähigkeit vermittelt, die Übertragungssicherheit gegebener Systeme einschätzen zu können und als Ingenieure die Strategien zur Verbesserung der Übertragungssicherheit zu beherrschen.

Inhalt

Lehrveranstaltung a): Moderne Verfahren der Kanalcodierung und Decodierung (Knopp)
• Kurzeinführung in die Informationstheorie
• Kanalcodierungstheorem
• Kanalkapazität verschiedener Übertragungskanäle
• Prinzip der Kanalcodierung
• Prinzip der Maximum-Likelihood und Maximum-A-Posteriori Decodierung
• Soft-in soft-out Decodierung
• Lineare Blockcodes
• Analytische und simulative Bestimmung der Fehlerwahrscheinlichkeit von Blockcodes
• Low Density Parity Check (LDPC) Codes
o Tanner Graphen
o Message Passing Decodierung
• Faltungscodes und Viterbi-Decodierung
• Verkettete Codes und iterative Decodierung:
o Parallel und seriell verkettete Codes, Turbo-Codes
o Turbo-Decodierung
• Beurteilung und Konstruktion von Codes mithilfe von EXIT Charts (Grundlagen)
• MAP Decodierung mit dem BCJR Algorithmus (Grundlagen)
• Anwendungen von Kanalcodierung in kommerziellen Systemen (u.a. CD, DVD, Funkkommunikation)
Lehrveranstaltung b): Übertragungssicherheit (Lindenmeier/Lankl)
Verbesserung der Übertragungssicherheit auf physikalischer Ebene (Lindenmeier)
• Beeinträchtigungen der phys. Übertragungsstrecke (Störungen, Rauschen, Fading, Jamming)
• Elektromagnetische Koppelmechanismen, Übersprechen und Entkoppelmassnahmen
• Schirmung und Filterung
• Rauschquellen und Abhilfemassnahmen
• Antennendiversity und intelligente Antennen
Systemaspekte zur Verbesserung der Übertragungssicherheit (Lankl)
• Sichere Übertragungskanäle und störresistente Übertragungsverfahren (Spread Spectrum)
• Zugriffsverfahren (Raum, Zeit, Frequenz)
• Adaptive Entzerrung und Störungskompensation
• Eigenheiten von Modulationsverfahren
• Mehrfachempfang nach dem Multiple Input- Multiple Output (MIMO)-Verfahren

Literatur

Simon, Omura, Scholtz: “Spread Spectrum Communications Handbook”, McGraw-Hill, 2001

Leistungsnachweis
Gesamtprüfung: schriftliche Prüfung von 105 Minuten Dauer (sP-105) oder mündliche Prüfung von 45 Minuten Dauer (mP-45), davon Teilprüfung Übertragungssicherheit: Schriftliche Prüfung von 45 min Dauer (sP-45) oder mündliche Prüfung von 20 min Dauer (mP-20) und Teilprüfung „Moderne Verfahren der Kanalcodierung und Decodierung“: Schriftliche Prüfung von 60 min (sP-60) oder mündliche Prüfung von 25 min Dauer (mP-25)
Verwendbarkeit
• Pflichtmodul in der Vertiefungsrichtung „Sicherheitstechnik"
Dauer und Häufigkeit
Das Modul dauert 1 Trimester Das Modul beginnt jedes Studienjahr jeweils im HT Als Startzeitpunkt ist das 2. Studienjahr vorgesehen

Modulname	Modulnummer
Nachrichtentheorie und Übertragungssicherheit	1289

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Berthold Lankl	Pflicht	10

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
12532	VÜ	Übertragungssicherheit	Pflicht	3
13811	VÜ	Nachrichten- und Informationstheorie	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

• Mathematik A,B,C

• Kenntnisse der Signal- und Systemtheorie wie sie in den Vorlesungen „Signale und Kommunikationssysteme" und „Kommunikationstechnik I" (BA-Modul „Kommunikationstechnik") vermittelt werden sind wünschenswert.

• Hochfrequenztechnik 1 und 2, Übertragungssysteme der Hochfrequenztechnik

• Empfohlen: EMV in der Kommunikationstechnik

Qualifikationsziele

Lehrveranstaltung a): Nachrichten- und Informationstheorie
• Der Student / die Studentin soll die Fähigkeit erwerben mathematische Verfahren und Konzepte auf nachrichtentechnische Anwendungen zu übertragen. Dazu ist ein etwas höherer Grad an Abstraktion nötig als in den nachrichtentechnischen Pflichtfächern.
• Der Student / die Studentin kann optimale Empfangskonzepte entwerfen kennt deren bestimmende Parameter und kann deren Leistungsfähigkeit abschätzen.
• Der Student / die Studentin kann suboptimale Verfahren bewerten und den Verlust gegenüber optimalen Verfahren bestimmen
• Verständnis für abstraktere nachrichtentheoretische Konzepte und die Fähigkeit bekannte Übertragungsverfahren (z.B. aus der Vorlesung „Kommunikationstechnik I und II") hierin einzuordnen.
Lehrveranstaltung b): Übertragungssicherheit
• Der Student/ die Studentin kennt Verfahren und Methoden auf System- und Komponentenebene um die Übertragungssicherheit von Kommunikationssystemen zu bewerten und erlernt Fähigkeiten um Systeme mit erhöhter Übertragungssicherheit zu entwerfen.

• Die Studierenden gewinnen einen Einblick in die Problemstellungen der Sicherheit moderner Informations-Übertragungssysteme mit dem besonderen Hinblick auf drahtlose Systeme, welche in den letzten Jahren eine stetig zunehmende Bedeutung erlangt haben. Hierbei werden zuerst Einschränkungen der Informationsübertragungen durch Störungen sowie der Abhörsicherheit durch elektromagnetische Kopplungseffekte und Übersprechen betrachtet, woraufhin die technischen Lösungen zur Reduzierung dieser Einschränkungen dargestellt werden. Den Studierenden wird die Fähigkeit vermittelt, die Übertragungssicherheit gegebener Systeme einschätzen zu können und als Ingenieure die Strategien zur Verbesserung der Übertragungssicherheit zu beherrschen.

Inhalt

Lehrveranstaltung a): Nachrichten- und Informationstheorie:

- Kurze Wiederholung von Grundlagen der Wahrscheinlichkeitstheorie (bedingte WDF, Verbund-WDF, Bayes)
- Signalraumdarstellung (Basisfunktionsentwicklung, irrelevante Signalanteile)

o Vektordemodulator und Korrelationsdemodulator
- Detektionsverfahren (Maximum-a-Posteriori und Maximum-Likelihood Detektion)

o Minimale Euklidische Distanz
o Signalkonstellationen und effizienter Signalkonstallationsentwurf
- Union Bound als Abschätzung für die Detektionsfehlerwahrscheinlichkeit
- Optimaler Empfänger bei Intersymbolinterferenz

o Symbol- und Sequenzschätzverfahren (Viterbialgorithmus)
o Einfluß von farbigem Rauschen
- Zuverlässigkeitsinformation (Likelihood-Verhältnis)
- Kanalkapazität für den symmetrischen Binärkanal (BSC), den symmetrischen binären Auslöschungskanal (BSEC) und Multilevel-Signale bei AWGN

Lehrveransztaltung b): Übertragungssicherheit
Verbesserung der Übertragungssicherheit auf physikalischer Ebene (Lindenmeier)
- Beeinträchtigungen der phys. Übertragungsstrecke (Störungen, Rauschen, Fading, Jamming)
- Elektromagnetische Koppelmechanismen, Übersprechen und Entkoppelmassnahmen
- Schirmung und Filterung
- Rauschquellen und Abhilfemassnahmen
- Antennendiversity und intelligente Antennen

Systemaspekte zur Verbesserung der Übertragungssicherheit (Lankl)
- Sichere Übertragungskanäle und störresistente Übertragungsverfahren (Spread Spectrum)
- Zugriffsverfahren (Raum, Zeit, Frequenz)
- Adaptive Entzerrung und Störungskompensation
- Eigenheiten von Modulationsverfahren

Mehrfachempfang nach dem Multiple Input- Multiple Output (MIMO)-VerfahrenÜbertragungssicherheit:
Verbesserung der Übertragungssicherheit auf physikalischer Ebene (Lindenmeier)

- Beeinträchtigungen der phys. Übertragungsstrecke (Störungen, Rauschen, Fading, Jamming)
- Elektromagnetische Koppelmechanismen, Übersprechen und Entkoppelmassnahmen
- Schirmung und Filterung
- Rauschquellen und Abhilfemassnahmen
- Antennendiversity und intelligente Antennen

Systemaspekte zur Verbesserung der Übertragungssicherheit (Lankl)

- Sichere Übertragungskanäle und störresistente Übertragungsverfahren (Spread Spectrum)
- Zugriffsverfahren (Raum, Zeit, Frequenz)
- Adaptive Entzerrung und Störungskompensation
- Eigenheiten von Modulationsverfahren

• Mehrfachempfang nach dem Multiple Input- Multiple Output (MIMO)-Verfahren

Literatur

Lehrveranstaltung a): Nachrichten- und Informationstheorie
Wozencraft, Jacobs: „Principles of Communication Engineering", John Wiley 1965
Gallager: "Principles of Digital Communication", Cambridge University Press, 2008
Lehrveranstaltung b): Übertragungssicherheit
Simon, Omura, Scholtz: "Spread Spectrum Communications Handbook", McGraw-Hill, 2001

Leistungsnachweis

Schriftliche Prüfung von 90 min (2x45min) Dauer (sP-90)

Verwendbarkeit

• Wahlpflichtmodul für den Masterstudiengang EIT in der Vertiefungsrichtung "Kommunikationstechnik",

• Pflichtmodul für ME (M. Sc.) Studienrichtung „Moderne Verfahren sicherer Kommunikationssysteme (VSK)"

Dauer und Häufigkeit

Das Modul dauert ein Trimester.
Das Modul beginnt jedes Studienjahr im Herbsttrimester.
Als Beginn ist das Herbsttrimester im 1. Studienjahr vorgesehen.

Modulname	Modulnummer
Web Technologies	1306

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Michael Koch	Wahlpflicht	6

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	36	144	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
11901	VÜ	Web Technologies	Pflicht	3
Summe (Pflicht und Wahlpflicht)				3

Empfohlene Voraussetzungen
Voraussetzung für das Modul ist die Kenntniss von Grundlagen zu Rechnernetzen, wie sie z.B. in der entsprechenden Veranstaltung im Bachelor-Studium Informatik vermittelt werden.
Qualifikationsziele
Die Veranstaltung vermittelt die Grundlagen und praktische Kenntnisse der verschiedenen Techniken und Werkzeuge des World Wide Web (WWW).
Inhalt
In diesem Modul werden Techniken und Werkzeuge des World Wide Web (WWW) theoretisch und praktisch durch den Einsatz in Fallstudien und Projekten (Teil des Selbststudiums) vermittelt. Dabei werden je nach Ausrichtung sowohl aktuell verbreitete Technologien und Werkzeuge (z.B. HTML, CSS, Ajax, WordPress, ...) als auch neue Technologien und Werkzeuge wie z.B. des Semantik Web (z.B. RDF, Ontologien, ...) oder des Mobile Web (z.B. Mobile-Ajax, ...) betrachtet.
Leistungsnachweis
Notenschein (für vorlesungsbegleitende Leistungen) oder schriftliche Prüfung im Umfang von 60 Minuten.
Dauer und Häufigkeit
Das Modul dauert 1 Trimester.Das Modul startet normalerweise im Frühjahrstrimester, wird aber nicht jedes Studienjahr angeboten.
Sonstige Bemerkungen
Das Modul ist identisch mit dem gleichnamigen Wahlpflichtmodul im Master - kann also entweder im Bachelor oder im Master belegt werden.

Modulname	Modulnummer
Middleware und mobile Cloud Computing	1398

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Andreas Karcher	Pflicht	0

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	60	120	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
13981	VL	Middleware und mobile Cloud Computing	Pflicht	3
13982	UE	Middleware und mobile Cloud Computing	Pflicht	2
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

Vorausgesetzt werden Kenntnisse aus dem Bereich des Software Engineering, insbesondere der Objektorientierung (Modul Objektorientierte Programmierung) sowie der XML-Technologien.

Wünschenswert sind Grundkenntnisse in einer der objektorientierten Programmiersprache, wie z. B. Java, Scala, C++.

Qualifikationsziele

Das Modul Middleware und mobile Cloud Computing zielt darauf ab, den Studierenden vertiefend die Bedeutung der Integration als Kernaufgabe der Angewandten Informatik näher zu bringen. Die Teilnehmer erhalten neben einem grundlegenden Verständnis für die

Anforderungen an eine Middleware-basierte Integration tiefe theoretische Kenntnisse über Architektur, Aufbau und Anwendung aktueller Middlewarekonzepte. Zudem werden querschnittlich Aspekte von verteilten Systemen in diesem Zusammenhang betrachtet.

Im Übungsteil lernen die Teilnehmer parallel zur Vorlesung den praktischen Umgang mit Middleware-Technologien und Cloud-basierten, mobilen Anwendungen. Durch eigenständige Anwendung von unter anderem Remote Method Invocation (RMI), Common Object Request Broker Architecture (CORBA), .NET und Simple Object Access Protocol (SOAP) erhalten die Teilnehmer Methoden- und Fachkompetenz im Umgang mit diesen Technologien.

In der Kombination aus theoretischer Behandlung und praktischer Vertiefung versetzt das Modul die Teilnehmer in die Lage, verteilte Anwendungen auf der Basis von Middleware zu entwerfen und in die Praxis umzusetzen.

Inhalt
Moderne Enterprise Anwendungen basieren auf Standard-Middleware-Architekturen, wo Funktionalität zunehmend über Cloud-basierte Dienste plattformübergreifend den Clients # mehr und mehr auch mobilen Endgeräten # zur Verfügung gestellt wird. Das Modul bietet einen fundierten Einstieg in die aktuellen Basistechnologien. Hierbei wird das Wissen aus dem Modul der objektorientierten Programmierung um die fachwissenschaftliche Denkweise der Entwicklung von verteilten Anwendungen erweitert. Nach einer grundlegenden Einführung in die Integrationsanforderungen zunehmend verteilt strukturierter, internet-basierter betrieblicher Anwendungen vermittelt das Modul zunächst einen Überblick über die Grundarchitektur Middleware-basierter Systeme und geht dann im Folgenden tiefer auf die unterschiedlichen Integrationsparadigmen und -technologien ein. Aktuelle Middlewaredienste und Architekturkonzepte wie Verteilte Objektmodelle, Komponentenmodelle und Service Oriented Middleware (SOA) bilden den Schwerpunkt des zweiten Teils des Moduls. Hier werden jeweils zunächst die allgemeinen Prinzipien erläutert und dann anhand konkreter Beispiele Standard-Middleware-Technologien und deren zugrunde liegenden Konzepte vertieft. Der dritte Teil stellt das Cloud-Konzept in den Mittelpunkt und zeigt Schritt für Schritt an einfachen Beispielen die Entwicklung Cloud-basierter Dienste und deren Zugriff über mobile Clients (Apps). Die begleitende Übung bietet die Gelegenheit, aktuelle Technologien anhand einfacher Beispiele kennen zu lernen und erste praktische Erfahrung im Umgang mit Middleware und mobilen, Cloud-basierten Anwendungen zu sammeln.
Lehrmethoden
Das Modul unterteilt sich in eine Vorlesung und eine Übung pro Woche. Es werden sowohl Lehrmethoden des fremdgesteuerten als auch des selbstgesteuerten Lernens angewendet. Es wird auf die individuellen Voraussetzungen der Studierenden eingegangen, wobei hauptsächlich ein lehrgangsförmiger und kooperativer Unterricht mit Einzelarbeit stattfindet.
Leistungsnachweis
Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer. Die Art der Prüfung wird jeweils zu Beginn des Moduls bekannt gegeben.
Verwendbarkeit
Die im Wahlpflichtmodul erworbenen Kenntnisse sind elementar für die IT-technische Gestaltung von verteilten Informationssystemen und stellen somit eine Grundlage für

Masterstudiengänge im Bereich Informatik/Wirtschaftsinformatik/Ingenieurinformatik/ Cyber Sicherheit dar.
Dauer und Häufigkeit
Das Modul dauert 1 Trimester. Das Modul beginnt jedes Studienjahr jeweils im Wintertrimester.

Modulname	Modulnummer
Visual Computing	1489

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Helmut Mayer	Wahlpflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
11521	VÜ	Computer Vision	Pflicht	3
11523	VÜ	Bildverarbeitung für Computer Vision	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

- Kenntnisse der Mathematik und Physik.
- Grundkenntnisse der digitalen Signalverarbeitung sind hilfreich.

Qualifikationsziele

In der Vorlesung und den Übungen zu Bildverarbeitung für Computer Vision erwerben Studierende vertiefte Kenntnisse über Techniken der Bildverarbeitung, die in Computer Vision verwendet werden, auch in Form der praktischen Auswertung von Bildern.
Sie kennen grundlegende Methoden wie Bildtransformationen, Segmentierung, Binärbildverarbeitung sowie Merkmalsextraktion und können diese sinnvoll kombinieren. Damit können sie abschätzen, welche Methoden sich in Abhängigkeit von Faktoren wie Genauigkeit, Robustheit und Geschwindigkeit besonders gut für welches Einsatzgebiet eignet.

Mittels der Vorlesung und Übungen zu Computer Vision erwerben Studierende vertieftes Wissen über die Rekonstruktion von 3D Geometrie aus perspektiven Bildern. Sie kennen verschiedene Techniken, die eine Poseschätzung mit und ohne Wissen über den Aufbau der Kamera (Kalibrierung) ermöglichen. Sie können diese zusammen mit Wissen über Bildzuordnung und robusten statistischen Verfahren anwenden, um die relative Pose für Bildpaare auch bei groben Fehlern in der Zuordnung zu schätzen. Damit sind die Studierenden grundsätzlich in der Lage, die Posen für weit auseinander liegende Aufnahmen (wide-baseline) zu bestimmen.

Inhalt

Die Vorlesung Bildverarbeitung für Computer Vision geht von der Bildgewinnung aus. Es wird gezeigt, wie Bilder und Bildausschnitte mittels statistischer Maße, wie z.B. Varianz und Korrelationskoeffizient, charakterisiert werden können. Bildtransformationen verändern entweder die Radiometrie oder die Geometrie der Bilder. Mittels lokaler Transformationen werden Kanten hervorgehoben oder Störungen beseitigt. Die

Bildsegmentierung, die z.B. auf Grundlage einzelner Pixel oder Regionen-orientiert erfolgen kann, führt zu homogenen Bildbereichen. Für die Verarbeitung binärer Bilder, d.h. Bilder mit nur zwei Grauwerten, werden Verfahren vorgestellt, die spezielle Formen herausarbeiten (mathematische Morphologie). Auf Grundlage aller bis dahin vorgestellter Techniken wird es mögliche, Merkmale, d.h. nulldimensionale (0D)-Punkte, 1D-Kanten / Linien und 2D Flächen zu extrahieren. Für Flächen wird deren Umsetzung in Vektoren inkl. Graphbildung und Polygonapproximation aufgezeigt.

Die Vorlesung Computer Vision legt zuerst Grundlagen der projektiven Geometrie. Für das Einzelbild wird die Modellierung mittels Projektionsmatrix und Kollinearitätsgleichung dargestellt und daraus die Rekonstruktion der Orientierung auf Grundlage der Direkten Linearen Transformation und die hoch genaue Bündellösung abgeleitet. Die relative Orientierung des Bildpaars kann mittels Fundamentalmatrix, essentieller Matrix und Homographie direkt bestimmt werden, daneben wird aber auch die hoch genaue Bündellösung dargestellt. Für drei und mehr Bilder wird der Trifokaltensor vorgestellt. Da reale Kameras nicht der idealen Zentralperspektive entsprechen, wird auf Objektivfehler eingegangen. Um Bilder orientieren zu können, sind korrespondierende Punkte oder Linien in den Bildern notwendig. Hierfür werden Grundlagen der Bildzuordnung dargestellt. Darauf aufbauend wird dargestellt, wie Bildpaare, -tripel und -sequenzen automatisch orientiert werden können und welche Probleme hierbei auftreten. Die bei der Orientierung der Bilder entstehenden 3D Punkte füllen den Raum nur unzureichend. Um eine realistische 3D Darstellung zu ermöglichen, werden Verfahren zur dichten Tiefenschätzung vorgestellt. Zuletzt werden an Hand der 3D Rekonstruktion aus Bildern von Unmanned Aircraft Systems (UAS) und der (Echtzeit) Navigation Möglichkeiten aber auch Probleme dargestellt.

Leistungsnachweis

Schriftliche Prüfung von 60 min oder mündliche Prüfung von 20 min (normalerweise am Ende des FT). Voraussetzung für die Teilnahme an der Prüfung ist die erfolgreiche Bearbeitung von Übungen.

Verwendbarkeit

Das Modul gibt Grundlagen für praktische Anwendungen im Bereich von Visual Computing.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester.
Das Modul findet jedes Studienjahr im Frühjahrstrimester statt.
Das Modul ist für das Frühjahrstrimester im 1. Studienjahr vorgesehen.

Sonstige Bemerkungen

Die Vorlesungen und Übungen Bildverarbeitung für Computer Vision und Computer Vision liegen im Frühjahrstrimester im 1. Studienjahr.

Modulname	Modulnummer
Operations Research, Complex Analytics and Decision Support Systems (ORMS I)	1490

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Stefan Pickl	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10333	VÜ	Moderne Heuristiken	Wahlpflicht	3
12325	P	Praktikum Operations Research - Entscheidungsunterstützung II	Wahlpflicht	3
12326	SE	Seminar Ausgewählte Kapitel des Operations Research II	Wahlpflicht	3
14901	VÜ	Ausgewählte Kapitel des Operations Research und der Entscheidungstheorie	Pflicht	3
149010	VÜ	Spieltheorie: Einführung in die mathematische Theorie strategischer Spiele	Wahlpflicht	3
149014	B	Geschichte des Operations Research	Wahlpflicht	3
14902	VÜ	Diskrete Optimierung	Wahlpflicht	3
14904	VÜ	Scheduling	Wahlpflicht	3
14905	VÜ	Schwarmbasierte Verfahren	Wahlpflicht	3
14906	VÜ	Soft Computing A: Management Science and Complex System Analysis - System Dynamics and Strategic Planning	Wahlpflicht	3
14907	VÜ	Soft Computing B: Fuzzy Systems - Network Operations	Wahlpflicht	3
14908	VÜ	Soft Computing C: Natural Computing - Evolutionary Algorithms	Wahlpflicht	3
14909	VÜ	Soft Computing D: Neural Networks and Network Analysis	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				9

Qualifikationsziele
Studierende sollen in die Lage versetzt werden, Probleme im Bereich der industriellen Anwendung, der öffentlichen Verwaltung, der internationalen Konflikte und des

strategischen Managements als Operations Research zugehörige Probleme zu identifizieren und mit geeigneten Modellen und Lösungsverfahren zu behandeln.

Es ist das Ziel dieses Moduls, dass die Studierenden sicher mit den Standard Verfahren des Operations Research und der Computational Intelligence umgehen können. Im Rahmen des heutigen unterstützenden Rechnereinsatzes sollen Sie in der Lage sein, zukünftige Potentiale zu erkennen und damit verbundene Komplexitätsaspekte im Ramen eines modernen Komplexitätsmanagements mit Methoden des Soft Computing kompetent zu behandeln.

Inhalt

Die Veranstaltung führt in das weite fachliche Gebiet des Operations Research ein. Der quantitativen Beschreibung und Lösung von komplexen Entscheidungs-problemen kommt hierbei eine besondere Bedeutung zu (Operations Research im engeren Sinne). Ferner wird auf die Entwicklung von algorithmischen Verfahren und Lösungsstrategien großen Wert gelegt (im Rahmen einer anwendungsbetonten Mathematischen Programmierung/ Computational Intelligence). Die behandelten Modelle und Verfahren werden exemplarisch aus dem Bereich der industriellen Anwendung, der öffentlichen Verwaltung, der internationalen Konflikte und des strategischen Managements gewählt werden.

Das Gebiet "Computational Intelligence" umfasst Methoden der sogenannten subsymbolischen Informationsverarbeitung. Auch wenn derzeit noch keine allgemeingültige genaue wissenschaftliche Definition dieses Begriffes existiert, so dient er dazu, die Gebiete "Evolutionary Computation", "Fuzzy Computation" und "Neural Computation" zusammenzufassen. "Computational Intelligence" betont zum einen den algorithmischen Aspekt und zum anderen die Fundierung im Bereich der künstlichen Intelligenz, der Entscheidungstheorie und der multikriteriellen Optimierung.

Im Zentrum dieses Moduls steht die Vermittlung von grundlegenden Kenntnissen über die in diesen Bereichen angewendeten relevanten Algorithmen, Heuristiken und Methoden. Die praktischen Bezüge reichen von den Bereichen "Business Intelligence/Optimization" und "Experimental Design" (z.B. im Bereich einer vernetzten Operationsführung) bis hin zum "Algorithmic Engineering".

Eine inhaltliche Auswahl besteht aus folgenden Elementen: Einführung in die Problemstellung und Lösungsmethoden der allgemeinen Unternehmensforschung (inklusive Operations Management), Klassische Optimierungsverfahren (lineare, nichtlineare, dynamische und diskrete Optimierung, Spieltheoretische Modelle und Verfahren, Mathematische Programmierung, Theorie dynamischer und stochastischer Prozesse, Ausblick auf aktuelle Probleme der Logistik, Steuerung und Netzwerktheorie und Soft Computing).

Leistungsnachweis

Mündliche Prüfung von 30 min oder Notenschein. Die Art der Prüfung wird am Anfang des Moduls festgelegt und bekannt gegeben.

Dauer und Häufigkeit

Das Modul dauert 2 bis 3 Trimester. Es wird nicht regelmäßig angeboten.

Sonstige Bemerkungen
Neben der Pflichtveranstaltung "Ausgewählte Kapitel des Operations Research und der Entscheidungstheorie" müssen zwei Lehrveranstaltungen mit Übungen im Umfang von je 3 TWS besucht werden.

Modulname	Modulnummer
Ausgewählte Kapitel des OR: Data-driven Optimization	2994

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. rer. nat. Maximilian Moll	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
29941	VÜ	Ausgewählte Kapitel des Data-driven Optimization	Pflicht	3
29942	VÜ	Quantum Machine Learning & Optimization	Wahlpflicht	3
29943	SE	Seminar: Ausgewählte Kapitel des OR	Wahlpflicht	3
29944	P	Praktikum: Ausgewählte Kapitel des OR	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Grundlegende Kenntnisse in Methoden des Operations Research und des Data Minings oder der Statistik werden vorausgesetzt.

Qualifikationsziele

Studierende sollen in die Lage versetzt werden, sich selbstständig mit neuartigen Methoden der data-driven Optimization in Theorie und Praxis auseinander zu setzen. Hierzu sollen sie im Rahmen der Vorlesung, sowie vertiefend in Seminar und Praktikum, verschiedene Methoden analysieren und anwenden.

Hierbei soll nicht nur die Fähigkeit entwickelt werden Ansätze auf ihre theoretische Richtigkeit und praktische Anwendbarkeit zu beurteilen, sondern diese auf ein Problem hin anpassen zu können.

Schließlich soll das Identifizieren geeigneter Probleme und passender Lösungsansätze geschult werden.

Inhalt

Data-driven Optimization beschäftigt sich zukunftsweisend mit der Kombination von klassischen Optimierungsmethoden und daten-basierten Ansätzen. Im Gegensatz zu der klassischen Optimierung der letzten Jahrhunderte, die ausgehend von einem zu optimierenden Modell eine Lösung sucht, bietet das Data-driven Optimization die Möglichkeit, ohne eine exakte mathematische Abstrahierung des zugrunde liegenden Modells Optimierungsmethoden anzuwenden.

Das Modul bietet aufbauend auf dem vorhandenen Grundwissen einen vertiefenden Einblick in ausgewählte Themengebiete des data-driven Optimization. Neben der grundlegenden Problematik werden Themen aus dem Reinforcement Learning, Prescriptive Analytics und der konvexen Optimierung unter Unsicherheit behandelt.

Das Reinforcement Learning ist neben Supervised und Unsupervised Learning das dritte Teilgebiet des Machine Learnings und beschäftigt sich mit daten-basierten Ansätzen zu Problemen der klassischen Kontrolltheorie. Hierbei soll im Modul auch die Anwendung auf praxis-relevante Probleme herausgestellt werden, die über die bekannten Lösungen von Spielen, wie z.B. Go, hinausgehen.

Prescriptive Analytics stellt aufbauend auf Descriptive und Predictive Analytics die nützlichste und schwerste Stufe des Data Science dar. Hier müssen nicht nur datan-basierte Vorhersagen getroffen werden, sondern das zukünftige System auf eine gegebene Zielvorstellung hin optimiert werden. In der Vorlesung werden verschiedene grundsätzliche Herangehensweisen mit ihren Vor- und Nachteilen diskutiert, sowie die Abgrenzung zu Predictive Analytics konkretisiert.

Die konvexe Optimierung stellt ein zentrales Element des Operations Research und der modernen Entscheidungsunterstützung dar. In vielen Fällen sind jedoch die Parameter der Optimierungsmodelle nicht explizit bekannt, sondern müssen zunächst aus Daten abgeleitet werden. Die Vorlesung thematisiert, wie sich dies auf die zu wählenden Optimierungsverfahren auswirken muss.

Das Seminar greift aktuelle Publikationen zu den Themen der Vorlesung auf.

Im Praktikum setzen sich die Studierenden mit einer konkreten, praxis-nahen Problemstellung des data-driven Optimization auseinander.

In der Vorlesung Quantum Machine Learning and Optimization wird spezifisch auf die Verwendung von Quantum Computern für effizientere Algorithmen im Kontext der NISQ-Maschinen eingegangen.

Leistungsnachweis

Mündliche Prüfung von 30 min.

Zum Absolvieren des Moduls sind drei der vier Wahlpflichtveranstaltungen zu belegen.

Dauer und Häufigkeit

Das Modul dauert 2 Trimester. Es beginnt immer im Frühjahrstrimester.

Modulname	Modulnummer
Algorithmen und Komplexität	3491

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. rer. nat. Peter Hertling	Wahlpflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
150	60	90	5

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
34911	VÜ	Algorithmen und Komplexität	Wahlpflicht	5
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

Die Studierenden sollten Grundkenntnisse in Informatik besitzen, insbesondere schon einige Erfahrung mit Algorithmen haben und die Sprache der Mathematik beherrschen. Nützlich sind außerdem generell Grundkenntnisse zur theoretischen Informatik, wie sie in entsprechenden Modulen im Bachelorstudiengang Informatik vermittelt werden.

Qualifikationsziele

Die Studierenden sollen Algorithmen auf ihre Effizienz hinsichtlich Laufzeit und Speicherplatzverbrauch analysieren können. Sie sollen zu in der Praxis auftretenden Berechnungsproblemen effiziente Algorithmen entwerfen können. Schließlich sollen sie die wichtigsten Komplexitätsklassen kennen und mit den Begriffen der Reduktion von Berechnungsproblemen und der Vollständigkeit für eine Komplexitätsklasse vertraut sein, um für Berechnungsprobleme abschätzen zu können, wo diese in der Hierarchie der Komplexitätsklassen einzuordnen sind, das heißt, wieviel Rechenzeit und Speicherplatz man zu ihrer Lösung nach dem derzeitigen Wissensstand in etwa benötigt und welche anderen Probleme in etwa gleich schwer sind.

Inhalt

Techniken zur Algorithmenanalyse hinsichtlich Laufzeit und Speicherplatzverbrauch, insbesondere Rekursionsgleichungen. Techniken zum Entwurf von Algorithmen, auch Approximationsalgorithmen, Randomisierung, Heuristiken. Deterministische, nichtdeterministische und probabilistische Komplexitätsklassen, der Reduktionsbegriff für Berechnungsprobleme und die Vollständigkeit von Berechnungsproblemen für Komplexitätsklassen.

Leistungsnachweis

Schriftliche Prüfung von 90 Minuten oder mündliche Prüfung von 30 Minuten.

Dauer und Häufigkeit
Das Modul dauert 1 Trimester. Das Modul beginnt jedes Studienjahr jeweils im Frühjahrstrimester. Als Startzeitpunkt ist das Frühjahrstrimester im 1. Studienjahr vorgesehen.

Modulname	Modulnummer
Quantenkommunikation	3695

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. rer. nat. Wolfgang Hommel	Wahlpflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3695-V1	VÜ	Quantenkommunikation	Pflicht	3
3695-V2	P	Praktikum Quantenschlüsselaustausch	Wahlpflicht	3
3695-V3	SE	Seminar Quantentechnologien	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Grundlegende Kenntnisse in linearer Algebra, komplexen Zahlen sowie Interesse an Quantenphysik und -technologie. Grundwissen über Kryptographie ist hilfreich, aber nicht zwingend erforderlich.

Qualifikationsziele

Verständnis des Quantenschlüsselaustauschs (Quantum Key Distribution, QKD) und seiner mathematischen Modellierung über Zweizustandssysteme. Kenntnisse der wichtigsten Protokolle zum Schlüsselaustausch sowie von Postprocessing-Methoden des Schlüsselmaterials (Privacy Amplification, Quantum Error Correction). Überblick über mögliche Angriffe auf den Quantenschlüsselaustausch sowie Maßnahmen zu deren Abwehr. Verständnis der Herausforderungen bei der technologischen Umsetzung des Quantenschlüsselaustauschs.

Praktisches Verständnis davon, wie der Quantenschlüsselaustausch experimentell umgesetzt werden kann. Überblick über die aktuellen Entwicklungen in im Bereich Quantentechnologien.

Inhalt

Der Quantenschlüsselaustausch ist eine der wichtigsten Quantentechnologien.
Seine Bedeutung entsteht daraus, dass die Sicherheit auf physikalischen Prinzipien beruht, nicht wie bei konventioneller Kryptographie auf Annahmen über den Rechnenaufwand beim Lösen bestimmter mathematischer Probleme. Daher ist der Quantenschlüsselaustausch auch sicher gegenüber Angriffen von Quantencomputern. Dieses Modul bietet eine Einführung in die Theorie und Praxis dieser neuen und spannenden Technologie.

Vorlesung:

- Grundlegender Formalismus der Quantenmechanik für Zweizustandssysteme
- Wichtigste Protokolle zum Quantenschlüsselaustausch (BB84, Ekert91, COW-Protokoll)
- Technologische Umsetzung von Qubits für den Quantenschlüsselaustausch
- Postprocessing-Methoden des Schlüsselmaterials: Error Correction, Privacy Amplification
- Sicherheitsanalysen, Seitenkanäle und Quantum Hacking
- Quantenkommunikationsnetzwerke und Quantenrepeater

Praktikum:

- Durchführung eines QKD-Modellversuchs, der das BB84-Protokoll mit polarisiertem Licht in der Praxis umsetzt
- Detailliertes Wissen über die Schritte, die für ein QKD-Protokoll erforderlich sind
- Experimentelle Durchführung des Protokolls in Teams bestehend aus zwei Personen, die die Rolle von Sender und Empfänger übernehmen
- Versenden einer mit Quantenschlüsseln verschlüsselten Nachricht
- Verfassen eines Versuchsprotokolls

Seminar: Aktuelle Themen in den folgenden Bereichen:

- Verschiedene technologische Realisierungen des Quantenschlüsselaustausches
- Quantum Hacking
- Überblick über bestehende und geplante Quantenkommunikationsnetzwerke
- Ansätze zur Realisierung von Quantenrepeatern
- Standardisierung von Protokollen und Geräten zum QKD-Schlüsselmanagement
- Aktuelle technologische Fortschritte in den Bereichen Quantenmeteorologie, Quantensensoren und Quantencomputern

Leistungsnachweis

Schriftliche Prüfung (60 min) oder mündliche Prüfung (30 min) oder Notenschein. Die Prüfungsform wird zu Beginn des Moduls festgelegt.

Dauer und Häufigkeit

Das Modul wird jedes Jahr ab dem WT angeboten und dauert zwei Trimester. Die Vorlesung wird im WT angeboten, das Praktikum oder das Seminar im FT.

Modulname	Modulnummer
Quantencomputer in Theorie und Praxis	3820

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
PD Dr. Rupert Hölzl	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
12113	VÜ	Quantencomputer	Pflicht	3
38202	P	Praktikum Quantencomputer-Programmierung	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Generelles Interesse an Mathematik und Theorie. Grundlegende Kenntnisse in Linearer Algebra erforderlich. Grundlegende Python-Kenntnisse sind nützlich, aber nicht zwingend erforderlich.

Qualifikationsziele

Verständnis des theoretischen Modells des Quantencomputers und seiner besonderen Möglichkeiten und Herausforderungen. Verständnis für das Design von Quantenalgorithmen. Praktische Erfahrung im Implementieren dieser Algorithmen.

Inhalt

In der Vorlesung wird das Modell des Quantencomputers vorgestellt. Seit Jahrzehnten gibt es nämlich die Hoffnung, dass man durch Ausnutzen von quantenmechanischen Vorgängen Computer bauen kann, die bestimmte Berechnungsprobleme schneller lösen können als herkömmliche Computer. Zuerst werden einige mathematische Grundlagen gelegt, und es wird eine kurze Einführung in die notwendigen Begriffe der Quantenmechanik gegeben. Dann wird das Modell des Quantencomputers eingeführt, und es werden verschiedene Algorithmen für Quantencomputer behandelt, unter anderem der Algorithmus von Grover und der berühmte Faktorisierungalgorithmus von Shor. Auch komplexitätstheoretische Aspekte werden besprochen.

Das Praktikum bietet Gelegenheit zum Experimentieren mit ausgewählten Quantenalgorithmen, die in der Vorlesung präsentiert wurden. Für einfache Experimente wird der webbasierte Circuit Composer aus der IBM Q Experience demonstriert. Für komplexere Experimente kommt die Softwarebibliothek Qiskit für Python3 zum Einsatz. Dabei wird sowohl die Verwendung von Scripts auf der Kommandozeile als auch die

komfortablere Nutzung von Jupyter Notebooks gezeigt. Tests laufen auf dem lokalen Rechner, in der IBM-Cloud zur Simulation, oder auf einem echten Quantencomputer. Darüberhinaus wird die Beschreibungssprache OpenQASM für Quantenschaltkreise vorgestellt.
Leistungsnachweis
Notenschein: Das Praktikum muss erfolgreich absolviert werden. Zur Vorlesung findet eine mündliche (30 Min.) oder schriftliche (60 Min.) Prüfung statt. Die genauen Prüfungsmodalitäten werden zu Beginn des Moduls festgelegt.
Dauer und Häufigkeit
Das Modul wird alle zwei Jahre angeboten und dauert zwei Trimester.

Modulname	Modulnummer
Anwendungsgebiete der Data Science	3852

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. phil. Michaela Geierhos	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
38521	VÜ	Sentiment Analysis	Wahlpflicht	3
38522	VÜ	Social Media Mining	Wahlpflicht	3
38523	VÜ	Semantische Technologien	Wahlpflicht	3
38524	PRO	Modulprojekt Anwendungsgebiete der Data Science	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Die Studierenden sollen grundlegende Kenntnisse in Programmierung und Software-Entwurf sowie ein Grundverständnis von Algorithmen und Datenstrukturen haben.

Qualifikationsziele

Die Studierenden lernen Herausforderungen und Methoden beim Text Mining kennen und lernen die besprochenen Techniken anzuwenden. Zudem lernen sie theoretische Ansätze auf konkrete, praxisrelevante Fragestellungen zu übertragen. Für exemplarische Aufgabenstellungen können die Studierenden bestehende methodische Ansätze beurteilen und Weiterentwicklungen anregen resp. eigenständig umsetzen. Sie können begründet argumentieren und eine von ihnen selbständig gefundene Lösung vertreten und reflexiv bewerten.

Inhalt

- In der Vorlesung „Sentiment Analysis“ soll die schon umfangreiche Forschungsliteratur zum Opinion Mining aufgearbeitet werden. Dabei reichen die Ansätze von der Text- bis zur Wortebene, die Aufgaben sind das Erkennen von Subjektivität vs. Objektivität, das Bestimmen der Perspektive von Autoren, das Extrahieren ihrer Meinung. Datenquellen können Review-Seiten aus dem Internet sein, Blog-Posts und -kommentare, Nachrichten auf Twitter, gesprochene Sprache, usw.
- In der Vorlesung „Social Media Mining“ wird exemplarisch die Entwicklung eines Systems besprochen, welches über soziale Netzwerke direkt oder indirekt an Unternehmen adressierte Meldungen, Nachrichten oder Kommentare erfasst, klassifiziert und auswertet. Hierbei werden Textmining- und Klassifikationsverfahren mit Fokus auf Kurztexten diskutiert und der begleitenden Übung praktisch vertieft.

- Die Vorlesung „Semantische Technologien“ gibt einen Einblick in Grundlagen und praktische Anwendungen wissensbasierter Softewarelösung. Sie gibt einen breiten Überblick über den Nutzen und die Möglichkeiten dieser Technologien. Semantische Technologien versetzen uns nicht nur in die Lage, Informationen zu speichern und wiederzufinden, sondern sie gemäß ihrer Bedeutung und Funktion entsprechend auszuwerten, zu verbinden, zu Neuem zu verknüpfen und so flexibel und zielgerichtet anzuwenden.
- Im Modulprojekt setzen sich Studierende unter Anleitung selbständig mit Texten und Aufgaben zum Modulthema auseinander und präsentieren ihre Ergebnisse geeignet in mündlicher und/oder schriftlicher Form. Zu Beginn des Modulprojekts werden die geplanten Einzelthemen angekündigt und festgelegt, in welcher Form die Ergebnisse zu präsentieren sind.

Leistungsnachweis

Das gesamte Modul wird per Notenschein geprüft, mit Anteilen von je 3 ECTS-LP zu jeder der Vorlesungen (mit Übung) und im Modulprojekt. Die Studierenden können (je nach Angebot) entweder zwei Vorlesungen mit Übungen oder eine Vorlesung mit Übungen und ein Modulprojekt einbringen – was insgesamt die 6 ECTS-LP des Moduls ergibt.

Verwendbarkeit

Die hier erworbenen Kenntnisse und Fertigkeiten ergänzen die Ausbildung im Bereich der Softwaretechnik um einen Aspekt von hoher praktischer Bedeutung. Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit im Bereich Data Science.

Dauer und Häufigkeit

Das Modul dauert 1-2 Trimester und beginnt jedes Jahr im HT.

Sonstige Bemerkungen

Die Vorlesungen und das Praktikum werden nicht alle jedes Jahr angeboten, aber in jedem Jahr mindestens so viele Lehrveranstaltungen, dass 6 ECTS-Leistungspunkte erreichbar sind. Jeweils zu Beginn des Moduls wird den Studierenden das konkrete Angebot erläutert.

Modulname	Modulnummer
Analyse unstrukturierter Daten	3853

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. phil. Michaela Geierhos	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
38531	VÜ	Analyse unstrukturierter Daten	Pflicht	6
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen
Die Studierenden sollen grundlegende Programmierkenntnisse sowie ein Grundverständnis von Algorithmen und Datenstrukturen haben.

Qualifikationsziele
Die Studierenden lernen Herausforderungen und Methoden bei der Informationsbeschaffung und -extraktion kennen und lernen die besprochenen Analyse-Methoden anzuwenden. Sie lernen Verfahren der Analyse unstrukturierter Daten auf konkrete, praxisrelevante Fragestellungen (insb. im Bereich Wissensgewinnung) anzuwenden und können für exemplarische Aufgabenstellungen existierende Ansätze beurteilen und Weiterentwicklungen anregen resp. eigenständig umsetzen.

Inhalt
Dieses Modul gibt einen Einblick in die Herausforderungen und Verfahren, die bei der Analyse unstrukturierter Daten zum Einsatz kommen. Unstrukturierte Informationen sind in der Regel sehr textlastig, weshalb viele vorhersagende Analyse-Verfahren den Informationswert dieser Daten nicht nutzen können. Allerdings können textbasierte Medien (E-Mails, Webseiten-Inhalte, Fachartikel, Social Media Beiträge, etc.) u. a. dabei helfen, Trends zu erkennen, Wissen zu gewinnen und Fake News aufzudecken. Hierfür müssen Informationen identifiziert, extrahiert, aufbereitet und interpretiert werden. Die Herausforderung besteht darin, relevante Informationen zu erkennen, aus unstrukturierten Texten zu extrahieren und fehlende Informationen ggf. hinzufügen. In der Veranstaltung werden auch Themen wie die Informationsgewinnung aus unterschiedlichen Quellen sowie Fragen der Qualitätssicherung bei der Datenspeicherung und des Datenmanagements in wissensbasierten Strukturen behandelt. In der Übung werden theoretische und praktische Fragestellungen gleichermaßen adressiert. Der theoretische Teil dient zur Wiederholung der Vorlesungsinhalte. Im

praktischen Teil sind die Studierenden aufgefordert, ausgewählte Verfahren zur Analyse unstrukturierter Daten eigenständig zu implementieren. Für die Übungen sind Programmierkenntnisse erforderlich.
Leistungsnachweis
Schriftliche Prüfung von 60 Minuten oder mündliche Prüfung von 30 Minuten.
Verwendbarkeit
Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit im Bereich Data Science mit Fokus auf die Analyse unstrukturierter Daten.
Dauer und Häufigkeit
Das Modul dauert ein Trimester und beginnt jedes Jahr im HT.

Modulname	Modulnummer
Cryptography Engineering	5519

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Cornelius Greither	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
12111	VÜ	Algorithmische Zahlentheorie	Pflicht	5
12112	VÜ	Ausgewählte mathematische Methoden in Kryptographie und Codierungstheorie	Wahlpflicht	3
55191	VÜ	Post-Quantum Kryptographie	Wahlpflicht	3
55192	P	Implementierung und Anwendung kryptographischer Verfahren	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Grundlagen zur Kryptographie und Kryptoanalyse, wie sie z.B. im Modul Kryptologie vermittelt werden.

Qualifikationsziele

Die Studierenden erlernen fortgeschrittene Konzepte und Algorithmen der Kryptographie und können ihr Wissen im Bereich der Kryptographie in Gebieten ihrer Wahl vertiefen. Dies können algebraische Methoden für den Entwurf von kryptographischen Verfahren oder kryptoanalytischen Verfahren sein oder Algorithmen im Bereich der Quantencomputer sowie Verfahren, die auch bei Verwendung von Quantencomputern noch sicher sind. Auch praktische Erfahrungen bei der Implementierung von kryptographischen Verfahren und von Analyse-Verfahren werden vermittelt.

Inhalt

Die Veranstaltung "Algorithmische Zahlentheorie" befasst sich mit grundlegenden Begriffen und Algorithmen der algebraischen Zahlentheorie. (Stichworte: Primelemente, Primalitätstests, Faktorisierung, elliptische Kurven, u.a.). Ein Großteil dieser abstrakten Konzepte ist fundamental für die moderne Kryptographie (Public Key) und die Codierungstheorie. Der Schwerpunkt dieser Vorlesung ist zwar die systematische Erarbeitung der theoretischen Grundlagen und grundlegenden Algorithmen, es wird aber auch immer wieder auf Anwendungen eingegangen. Ergänzt werden diese durch zahlentheoretische Konzepte, die eventuell in einer Post-Quantencomputer-Epoche relevant sein könnten.

Die Veranstaltung "Ausgewählte mathematische Methoden der Kryptographie und Codierungstheorie" befasst sich mit ausgewählten und fortgeschrittenen Themen aus der Kryptographie und/oder der Codierungstheorie. Hierhin gehören kryptographische Verfahren, die auf zahlentheoretischen Ergebnissen aufsetzen, und "gute" Codes, die man mit Hilfe von algebraischen Kurven gefunden hat. Sowohl kryptographische als auch codierungstheoretische Inhalte sind vorgesehen; die Gewichtung zwischen diesen beiden Gebieten kann aber variieren.

Ein sehr wichtiges theoretisches Resultat von Peter Shor besagt, dass man mit Hilfe von Quantencomputern schnell große Zahlen faktorisieren kann und damit viele der heutzutage häufig verwendeten kryptographischen Verfahren brechen kann.
In der Vorlesung mit Übungen "Post-Quantum Kryptographie" soll zuerst dieses Resultat mit den notwendigen Grundlagen vorgestellt werden. Dann sollen einerseits quantenkryptographische Verfahren präsentiert werden und andererseits Verfahren, die sogar gegen Angriffe mit Hilfe von Quantencomputern resistent sind. Genannt seien: gitterbasierte Verfahren, codebasierte Verfahren, Hash-Verfahren und Verfahren, die auf multivariaten Polynomen basieren.

In dem Praktikum "Implementierung und Anwendung kryptographischer Verfahren" werden verschiedene kryptographische und kryptoanalytische Verfahren implementiert. Dabei werden auch verschiedene Anwendungsbereiche abgedeckt, z.B. Verschlüsselung von Nachrichten, Signatur-Verfahren, Authentizität von Nachrichten, Authentifikation von Kommunikationsteilnehmern sowie für diese Probleme geeignete Protokolle. Es werden auch Analyse-Verfahren und mögliche Angriffe auf kryptographische Protokolle implementiert und durchgespielt.

Leistungsnachweis

Schriftliche Prüfung mit 60 Minuten Dauer oder mündliche Prüfung mit 30 Minuten Dauer oder Notenschein. Die Prüfungsform wird zu Beginn des Moduls festgelegt.

Dauer und Häufigkeit

Das Modul dauert 1-2 Trimester.

Sonstige Bemerkungen

Es ist entweder die Vorlesung "Algorithmische Zahlentheorie" und eine der anderen Veranstaltungen zu belegen; oder die beiden anderen Vorlesungen und das Praktikum. Je nach Kombination der Veranstaltungen, ergibt sich die TWS-Summe 8 bzw. 9.

Modulname	Modulnummer
Industrial Security	5521

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
N.N.	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55211	VÜ	Internet of Things and Industrial Internet Security	Wahlpflicht	3
55212	P	Praktikum Sicherheit eingebetteter Systeme	Wahlpflicht	3
55213	VÜ	Trusted Computing	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Gute Kenntnisse der Hardwaresicherheit, wie im gleichnamigen Modul vermittelt. Gute Kenntnisse in imperativer und systemnaher Programmierung.

Qualifikationsziele

Studierende entwickeln ein vertieftes Verständnis für die aktuellen Sicherheitsdefizite bei den bislang in Consumer-Geräten und z.B. in Industrieproduktionsanlagen verbauten eingebetteten Systemen. Sie kennen Algorithmen und Protokolle aus dem Bereich Lightweight Cryptography, deren Einsatzgebiete und die mit ihnen verbundenen Kompromisse. Die Studierenden können das in IoT- und Industrie-4.0-Szenarien erreichte Sicherheitsniveau bewerten und geeignete Schutzmaßnahmen auswählen. Sie können eigene Seitenkanalanalysen durchführen und auf eingebetteten Systemen ablaufende Algorithmen gegen entsprechende Angriffe schützen.

Inhalt

Die Vorlesung Internet of Things and Industrial Internet Security vertieft die IT-Sicherheit eingebetteter Systeme im Kontext von Cyber-Physical Systems. Dabei werden zum einen Endanwender-Anwendungsgebiete wie Smart Homes und Bestandteile kritischer Infrastrukturen wie Smart Meters mit den dort eingesetzten Schutzmaßnahmen für Kommunikationsprotokolle, Manipulationssicherheit und Datenschutz betrachtet. Zum anderen werden industrielle Anwendungsgebiete wie vernetzte Produktionsanlagen und organisationsübergreifender Datenaustausch im Rahmen von Supply Chains und die mit ihnen verbundenen Risiken analysiert. Durch die beschränkte Leistungsfähigkeit der eingesetzten Embedded Systems müssen insbesondere bei der Anwendung kryptographischer Verfahren Kompromisse eingegangen werden; ausgewählte Algorithmen und ihre Anwendung in Form von

Kommunikationsprotokollen der Lightweight Cryptography werden eingeführt und bezüglich ihrer Sicherheitseigenschaften mit herkömmlichen Chiffren und Message Authentication Codes gegenübergestellt.

Das Praktikum Embedded Systems Security bietet die Möglichkeit, ausgewählte Angriffe und Gegenmaßnahmen, die im Modul Hardwaresicherheit behandelt werden, im Labor in kleinen Gruppen selbst durchzuführen und zu vertiefen. Der Quelltext der auf Kleinstrechnern laufenden Programme muss dabei z.B. gegen Timing-Angriffe und Messungen des Stromverbrauchs gehärtet werden. Weitere Aufgaben umfassen z.B. das Reverse-Engineering und Nachbilden von Protokollen, wie sie z.B. für Smart-Home-Geräte eingesetzt werden könnten.

Leistungsnachweis
Notenschein, der sich aus Teilleistungen zu den beiden Lehrveranstaltungen zusammensetzt. Die jeweilige Prüfungsform für die Teilleistungen wird zu Beginn des Moduls bzw. der Lehrveranstaltungen festgelegt.
Dauer und Häufigkeit
Das Modul dauert 1-2 Trimester.

Modulname	Modulnummer
Visual Computing (erweitert)	1152

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Helmut Mayer	Wahlpflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
11521	VÜ	Computer Vision	Pflicht	3
11522	VÜ	Computer Vision und Graphik	Wahlpflicht	3
11523	VÜ	Bildverarbeitung für Computer Vision	Pflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

- Kenntnisse der Mathematik und Physik.
- Grundkenntnisse der digitalen Signalverarbeitung sind hilfreich.

Qualifikationsziele

In der Vorlesung und den Übungen zu Bildverarbeitung für Computer Vision erwerben Studierende vertiefte Kenntnisse über Techniken der Bildverarbeitung, die in Computer Vision verwendet werden, auch in Form der praktischen Auswertung von Bildern.
Sie kennen grundlegende Methoden wie Bildtransformationen, Segmentierung, Binärbildverarbeitung sowie Merkmalsextraktion und können diese sinnvoll kombinieren. Damit können sie abschätzen, welche Methoden sich in Abhängigkeit von Faktoren wie Genauigkeit, Robustheit und Geschwindigkeit besonders gut für welches Einsatzgebiet eignet.

Mittels der Vorlesung und Übungen zu Computer Vision erwerben Studierende vertieftes Wissen über die Rekonstruktion von 3D Geometrie aus perspektiven Bildern. Sie kennen verschiedene Techniken, die eine Poseschätzung mit und ohne Wissen über den Aufbau der Kamera (Kalibrierung) ermöglichen. Sie können diese zusammen mit Wissen über Bildzuordnung und robusten statistischen Verfahren anwenden, um die relative Pose für Bildpaare auch bei groben Fehlern in der Zuordnung zu schätzen. Damit sind die Studierenden grundsätzlich in der Lage, die Posen für weit auseinander liegende Aufnahmen (wide-baseline) zu bestimmen.

Das Ziel der Vorlesung und Seminarübung zu Computer Vision und Graphik besteht darin, den Studierenden vertieftes Wissen zu Techniken der automatischen Extraktion von Objekten aus Bildern zu vermitteln. Weiterhin bekommen die Studierenden die Fähigkeit, dichte Tiefendaten durch Bildzuordnung zu generieren, mittels derer realistische 3D Visualisierungen erzeugt werden können. Die Studierenden erhalten

neben breitem Wissen zur aussehensbasierten Extraktion auf Grundlage von ähnlichem Aussehen und ähnlicher Anordnung von kleinen Bildausschnitten insbesondere ein Verständnis der Möglichkeiten, die sich durch eine Kopplung von Computer Vision und Graphik in Form von generativen Modellen ergeben. Mittels eines Vortrags lernen die Studierenden die Einordnung eines spezifischen Themas in den Rahmen der Techniken von Computer Vision und Graphik.

Inhalt

Die Vorlesung Bildverarbeitung für Computer Vision geht von der Bildgewinnung aus. Es wird gezeigt, wie Bilder und Bildausschnitte mittels statistischer Maße, wie z.B. Varianz und Korrelationskoeffizient, charakterisiert werden können. Bildtransformationen verändern entweder die Radiometrie oder die Geometrie der Bilder. Mittels lokaler Transformationen werden Kanten hervorgehoben oder Störungen beseitigt. Die Bildsegmentierung, die z.B. auf Grundlage einzelner Pixel oder Regionen-orientiert erfolgen kann, führt zu homogenen Bildbereichen. Für die Verarbeitung binärer Bilder, d.h. Bilder mit nur zwei Grauwerten, werden Verfahren vorgestellt, die spezielle Formen herausarbeiten (mathematische Morphologie). Auf Grundlage aller bis dahin vorgestellter Techniken wird es mögliche, Merkmale, d.h. nulldimensionale (0D)-Punkte, 1D-Kanten / Linien und 2D Flächen zu extrahieren. Für Flächen wird deren Umsetzung in Vektoren inkl. Graphbildung und Polygonapproximation aufgezeigt.

Die Vorlesung Computer Vision legt zuerst Grundlagen der projektiven Geometrie. Für das Einzelbild wird die Modellierung mittels Projektionsmatrix und Kollinearitätsgleichung dargestellt und daraus die Rekonstruktion der Orientierung auf Grundlage der Direkten Linearen Transformation und die hoch genaue Bündellösung abgeleitet. Die relative Orientierung des Bildpaars kann mittels Fundamentalmatrix, essentieller Matrix und Homographie direkt bestimmt werden, daneben wird aber auch die hoch genaue Bündellösung dargestellt. Für drei und mehr Bilder wird der Trifokaltensor vorgestellt. Da reale Kameras nicht der idealen Zentralperspektive entsprechen, wird auf Objektivfehler eingegangen. Um Bilder orientieren zu können, sind korrespondierende Punkte oder Linien in den Bildern notwendig. Hierfür werden Grundlagen der Bildzuordnung dargestellt. Darauf aufbauend wird dargestellt, wie Bildpaare, -tripel und -sequenzen automatisch orientiert werden können und welche Probleme hierbei auftreten. Die bei der Orientierung der Bilder entstehenden 3D Punkte füllen den Raum nur unzureichend. Um eine realistische 3D Darstellung zu ermöglichen, werden Verfahren zur dichten Tiefenschätzung vorgestellt. Zuletzt werden an Hand der 3D Rekonstruktion aus Bildern von Unmanned Aircraft Systems (UAS) und der (Echtzeit) Navigation Möglichkeiten aber auch Probleme dargestellt.

Die Vorlesung Computer Vision und Graphik führt zuerst in die Modellbildung für die Objektextraktion mit Objekten (Geometrie und Radiometrie), Relationen, Kontext und Ebenen der Extraktion ein. Für die aussehensbasierte Objektextraktion werden Verfahren zur Detektion und Beschreibung von kleinen Bildausschnitten, z.B. SIFT, und zum Vergleich der Anordnung, wie z.B. Schätzung der Homographie mit RANSAC oder Hough-Transformation vorgestellt. Generative Modelle beruhen auf einer möglichst realistischen Visualisierung. Hierfür werden verschiedene Techniken der (Computer) Graphik vorgestellt und es wird aufgezeigt, wie diese in Graphik-Hardware realisiert werden. Die Extraktion der Objekte beruht auf a priori Annahmen (Priors) über die Geometrie und Radiometrie der Objekte. Der Vergleich von Visualisierung und realem Bild führt zu Likelihoods. Die Modelle werden auf Grundlage der Priors statistisch

modifiziert und die Lösung als MAP (Maximum a posteriori) Schätzung bestimmt. Hierfür werden Techniken wie (Reversible Jump) Markov Chain Monte Carlo (MCMC) verwendet. Es wird die Extraktion topographischer Objekte, vor allem Gebäudefassaden und Vegetation aus terrestrischen Daten, aber auch von Straßen aus Luft- und Satellitenbildern dargestellt. Weitere Anwendungen werden in Seminarvorträgen vorgestellt und diskutiert.

Leistungsnachweis
Schriftliche Prüfung von 90 min oder mündliche Prüfung von 30 min (normalerweise am Ende des HT). Voraussetzung für die Teilnahme an der Prüfung ist die erfolgreiche Bearbeitung von Übungen und Seminarübungen.
Verwendbarkeit
Das Modul gibt Grundlagen für praktische Anwendungen im Bereich von Visual Computing.
Dauer und Häufigkeit
Das Modul dauert 2 Trimester. Das Modul beginnt jedes Studienjahr jeweils im Frühjahrstrimester. Als Startzeitpunkt ist das Frühjahrstrimester im 1. Studienjahr vorgesehen.
Sonstige Bemerkungen
Die Vorlesungen und Übungen Bildverarbeitung für Computer Vision und Computer Vision liegen im Frühjahrstrimester im 1. und die Seminarübung Computer Vision und Graphik im Herbsttrimester des 2. Studienjahres.

Modulname	Modulnummer
Erweiterte Digitale Forensik	1162

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. rer. nat. Harald Baier	Wahlpflicht	4

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
11621	VL	Erweiterte Digitale Forensik (Vorlesung)	Pflicht	3
11622	UE	Erweiterte Digitale Forensik (Übung)	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Das Modul 5505 muss bestanden sein und das Modul 3824 soll bestanden sein. Die Studierenden müssen mit den Grundlagen der IT-Forensik vertraut sein, insbesondere mit IT-forensisch relevanten Spuren und deren Analyse auf Datenträger- und Dateisystemebene.

Qualifikationsziele

Die Studierenden erwerben fortgeschrittene Kenntnisse und Fähigkeiten zur Durchführung einer IT-forensischen Untersuchung. Dazu gehören weitergehende Themen wie Hashfunktionen und Approximate Matching zur Erkennung bzw. Wiedererkennung von Artefakten, fortgeschrittene Dateisystemanalyse am Beispiel ext4, Linux-Analyse und fortgeschrittene Hauptspeicheranalyse.

Inhalt

Die Studierenden lernen fortgeschrittene Betriebssystemforensik am Beispiel von Linux kennen und arbeiten insbesondere mit Linux-Artefakten. Weiterführende Betrachtungen zur Sicherung und Analyse des Hauptspeichers werden mittels des Linux-Betriebssystems und des Frameworks Volatility behandelt. Weiterhin wird der Einsatz von kryptographischen sowie ähnlichkeitserhaltenden Hashfunktionen zur automatisierten (Wieder-)erkennung von Datenstrukturen betrachtet. Im Kontext der Dateisystemforensik wird ein aktuelles Dateisystem analysiert, beispielsweise ext4 wegen seiner Bedeutung für Android. Weiterhin wird ein aktuelles Themengiebt (z.B. Mobilfunkforensik, Netzwerkforensik, Automotive Forensik) bearbeitet.

Leistungsnachweis

Notenschein: Die Übung muss bestanden werden (unbenotete Prüfungsvorleistung). Die Prüfungsleistung ist eine mündliche Prüfung.

Verwendbarkeit
Die im Modul vermittelten Techniken der digitalen Forensik sind in der Beweissicherung und der Zuordnung von Vorfällen im digitalen Zeitalter unerlässlich. Die gelernte Methodik lässt sich auf bisher unbekannte IT-forensische Fragestellungen übertragen.
Dauer und Häufigkeit
Das Modul dauert ein Trimester und beginnt jedes Jahr im WT.

Modulname	Modulnummer
Data Mining und IT- basierte Entscheidungsunterstützung	1231

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Stefan Pickl	Pflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	60	120	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
12311	VÜ	Data Mining und IT-basierte Entscheidungsunterstützung	Pflicht	5
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen

Grundkenntnisse zu mathematischen Methoden des Operations Research und der Statistik wie sie z.B. im Bachelor Informatik bzw. Wirtschaftsinformatik vermittelt werden.

Qualifikationsziele

Lernziele sind das kompetente Beherrschen grundlegender Verfahren und Methoden sowie ihrer praktischen Anwendung in den unter Inhalte dargestellten Bereichen.

Inhalt

Die Studierenden sollen in dieser Veranstaltung mit den IT-basierten und entscheidungstheoretischen Grundlagen im Bereich der modernen Datenanalyse vertraut gemacht werden; insbesondere im Hinblick auf die Strukturierung von Entscheidungsproblemen, die Entwicklung von geeigneten Analyseverfahren zur Erforschung von komplexen datenbasierten Zusammenhängen ("Exploratory Analysis"). Data Mining bedeutet dabei das Extrahieren von impliziten, noch unbekannten Informationen aus Rohdaten. Dazu sollten IT-Systeme in die Lage versetzt werden, Datenbanken und Datenansammlungen (z.B. im Bereich der Geoinformatik) automatisch nach Gesetzmäßigkeiten und Mustern zu durchsuchen und einen Abstraktionsprozess durchzuführen, der als Ergebnis aussagekräftige Informationen liefert. Insbesondere das heutige maschinelle Lernen und das Verfahren des "Datafarming" stellen dafür die Werkzeuge und Techniken zur Verfügung, die in den Bereich des modernen Wissensmanagements (bis zur Begriffsanalyse) und "Datamining" hineinführen.

Literatur

- Decision Support Systems Developing Web-Enabled Decision Support Systems, Abhijit A. Pol and Ravindra K. Ahuja. Dynamic Ideas 2007.
- Exploratory Data Analysis Making Sense of Data: A Practical Guide to Exploratory Data Analysis and Data Mining, Glenn J. Myatt. John Wiley, 2006.
- Spatial Data Analysis Spatial Data Analysis - Theory and Practice, Robert Haining, Cambridge University Press 2003.

- Data Mining Data Mining: Practical Machine Learning Tools and Techniques (Second Edition) Ian H. Witten, Eibe Frank. Morgan Kaufmann 2005.
- Data Mining: A Knowledge Discovery, K. Cios, W. Pedrycz, R. Swiniarski Springer, 2007.
- Data Mining Introductery and Advanced Topics, Margaret Dunham, Prentice Hall, 2003.
- Advances in Knowledge Discovery and Data Mining, U. Fayyad, G. Piatetsky-Shapiro, P. Smyth, R. Uthurusamy, editors , MIT Press, 1996.
- Data Mining: Concepts and Techniques, Jiawei Han, Micheline Kamber. Morgan Kaufmann, 2006.
- Principles of Data Mining, David J. Hand, Heikki Mannila and Padhraic Smyth. MIT Press, 2000. Daniel T. Larose,
- Discovering Knowledge in Data: An Introduction to Data Mining, John Wiley 2004. Robert Nisbet, John Elder, IV and Gary Miner.
- Handbook of Statistical Analysis and Data Mining Applications. Elsevier 2009.
- Statistical Learning - Machine Learning Trevor Hastie, Robert Tibshirani, Jerome Friedman,
- The Elements of Statistical Learning: Data Mining, Inference, and Prediction, Springer Verlag, 2001. Mehmed Kantardzic, Data Mining: Concepts, Models, Methods, and Algorithms, Wiley-IEEE Press, 2002.

Weiterführende Literatur:

- Zeitreihenanalyse Time Series Analysis. Hamilton 1994.
- Reinforcement Lernen und Spieltheorie Reinforcement Learning: An Introduction. Sutton and Barto: MIT Press 1998.
- Fun and Games: A Text on Game Theory. Binmore, Linster, Houghton Mifflin 2000.
- Statistik Bayesian Data Analysis. Gelman, Carlin, Stern, Rubin: Chapman 1995. Introduction to Mathematical Statistics. Hogg, Craig: Prentice Hall 2004.
- Principles of Statistics. Bulmer: Dover 1979.
- Probability, Random Variables and Stochastic Proc., Papoulis, McGraw, Hill 2002.

Leistungsnachweis

Mündliche (20min) oder schriftliche (60min) Modulprüfung.

Verwendbarkeit

Die Vorlesung kann durch weiterführende Veranstaltungen im Bereich der Datenanalyse fortgeführt werden, z.B. im Bereich der modernen Begriffsanalyse, des Algorithmic Engineering, im Rahmen von Spezialvorlesungen der Numerik und Statistik sowie der Geoinformatik. Ebenfalls bestehen enge Bezüge zu wissenschaftlichen Forschungsgebieten im Bereich der Künstlichen Intelligenz.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester.
Das Modul beginnt jedes Studienjahr jeweils im Wintertrimeste

Modulname	Modulnummer
Visual Computing	1489

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Helmut Mayer	Wahlpflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
11521	VÜ	Computer Vision	Pflicht	3
11523	VÜ	Bildverarbeitung für Computer Vision	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

- Kenntnisse der Mathematik und Physik.
- Grundkenntnisse der digitalen Signalverarbeitung sind hilfreich.

Qualifikationsziele

In der Vorlesung und den Übungen zu Bildverarbeitung für Computer Vision erwerben Studierende vertiefte Kenntnisse über Techniken der Bildverarbeitung, die in Computer Vision verwendet werden, auch in Form der praktischen Auswertung von Bildern.
Sie kennen grundlegende Methoden wie Bildtransformationen, Segmentierung, Binärbildverarbeitung sowie Merkmalsextraktion und können diese sinnvoll kombinieren. Damit können sie abschätzen, welche Methoden sich in Abhängigkeit von Faktoren wie Genauigkeit, Robustheit und Geschwindigkeit besonders gut für welches Einsatzgebiet eignet.

Mittels der Vorlesung und Übungen zu Computer Vision erwerben Studierende vertieftes Wissen über die Rekonstruktion von 3D Geometrie aus perspektiven Bildern. Sie kennen verschiedene Techniken, die eine Poseschätzung mit und ohne Wissen über den Aufbau der Kamera (Kalibrierung) ermöglichen. Sie können diese zusammen mit Wissen über Bildzuordnung und robusten statistischen Verfahren anwenden, um die relative Pose für Bildpaare auch bei groben Fehlern in der Zuordnung zu schätzen. Damit sind die Studierenden grundsätzlich in der Lage, die Posen für weit auseinander liegende Aufnahmen (wide-baseline) zu bestimmen.

Inhalt

Die Vorlesung Bildverarbeitung für Computer Vision geht von der Bildgewinnung aus. Es wird gezeigt, wie Bilder und Bildausschnitte mittels statistischer Maße, wie z.B. Varianz und Korrelationskoeffizient, charakterisiert werden können. Bildtransformationen verändern entweder die Radiometrie oder die Geometrie der Bilder. Mittels lokaler Transformationen werden Kanten hervorgehoben oder Störungen beseitigt. Die

Bildsegmentierung, die z.B. auf Grundlage einzelner Pixel oder Regionen-orientiert erfolgen kann, führt zu homogenen Bildbereichen. Für die Verarbeitung binärer Bilder, d.h. Bilder mit nur zwei Grauwerten, werden Verfahren vorgestellt, die spezielle Formen herausarbeiten (mathematische Morphologie). Auf Grundlage aller bis dahin vorgestellter Techniken wird es mögliche, Merkmale, d.h. nulldimensionale (0D)-Punkte, 1D-Kanten / Linien und 2D Flächen zu extrahieren. Für Flächen wird deren Umsetzung in Vektoren inkl. Graphbildung und Polygonapproximation aufgezeigt.

Die Vorlesung Computer Vision legt zuerst Grundlagen der projektiven Geometrie. Für das Einzelbild wird die Modellierung mittels Projektionsmatrix und Kollinearitätsgleichung dargestellt und daraus die Rekonstruktion der Orientierung auf Grundlage der Direkten Linearen Transformation und die hoch genaue Bündellösung abgeleitet. Die relative Orientierung des Bildpaars kann mittels Fundamentalmatrix, essentieller Matrix und Homographie direkt bestimmt werden, daneben wird aber auch die hoch genaue Bündellösung dargestellt. Für drei und mehr Bilder wird der Trifokaltensor vorgestellt. Da reale Kameras nicht der idealen Zentralperspektive entsprechen, wird auf Objektivfehler eingegangen. Um Bilder orientieren zu können, sind korrespondierende Punkte oder Linien in den Bildern notwendig. Hierfür werden Grundlagen der Bildzuordnung dargestellt. Darauf aufbauend wird dargestellt, wie Bildpaare, -tripel und -sequenzen automatisch orientiert werden können und welche Probleme hierbei auftreten. Die bei der Orientierung der Bilder entstehenden 3D Punkte füllen den Raum nur unzureichend. Um eine realistische 3D Darstellung zu ermöglichen, werden Verfahren zur dichten Tiefenschätzung vorgestellt. Zuletzt werden an Hand der 3D Rekonstruktion aus Bildern von Unmanned Aircraft Systems (UAS) und der (Echtzeit) Navigation Möglichkeiten aber auch Probleme dargestellt.

Leistungsnachweis

Schriftliche Prüfung von 60 min oder mündliche Prüfung von 20 min (normalerweise am Ende des FT). Voraussetzung für die Teilnahme an der Prüfung ist die erfolgreiche Bearbeitung von Übungen.

Verwendbarkeit

Das Modul gibt Grundlagen für praktische Anwendungen im Bereich von Visual Computing.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester.
Das Modul findet jedes Studienjahr im Frühjahrstrimester statt.
Das Modul ist für das Frühjahrstrimester im 1. Studienjahr vorgesehen.

Sonstige Bemerkungen

Die Vorlesungen und Übungen Bildverarbeitung für Computer Vision und Computer Vision liegen im Frühjahrstrimester im 1. Studienjahr.

Modulname	Modulnummer
Digitale Forensik	1551

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. rer. nat. Harald Baier	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
15511	VL	Digitale Forensik (VL)	Pflicht	3
15512	UE	Digitale Forensik (UE)	Pflicht	3
15513	SE	Seminar Ausgewählte Themen der digitalen Forensik	Pflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Das Modul 5505: Systemsicherheit muss bestanden sein. Die Studierenden müssen mit den Grundlagen der IT-Forensik vertraut sein, insbesondere mit IT-forensisch relevanten Spuren und deren Analyse auf Datenträger- und Dateisystemebene.

Qualifikationsziele

Die Studierenden kennen die allgemeine IT-forensische Vorgehensweise und können diese bei der Durchführung IT-forensischer Analysen anwenden sowie in einem Gutachten dokumentieren. Sie kennen wichtige Spurenquellen im Betriebssystem Windows und können diese auswerten. Die Studierenden kennen Datenformate von verbreiteten Anwendungen und können diese analysieren. Sie wissen Sicherungs- und Analyseverfahren des Hauptspeichers und können diese anwenden. Wesentliche Anti-Forensik-Ansätze sind den Studierenden bekannt, und sie können diese bewerten. Weiterhin können die Studierenden Speichertechnologien erklären und digitale Spuren eingebetteter Systeme IT-forensisch sichern und auswerten.

Inhalt

Die Studierenden lernen die Betriebssystemforensik am Beispiel von Windows kennen und arbeiten insbesondere mit der Windows-Registry sowie Windows-Artefakten. Im Kontext der Anwendungsforensik wird das SQLite Datenbankformat behandelt und für Anwendungen wie Firefox, Thunderbird, Skype analysiert. Die Sicherung und Analyse des Hauptspeichers wird mittels des Windows-Betriebssystems und des Frameworks Volatility behandelt. Auf dem Gebiet der Anti-Forensik lernen die Studierenden die gängigen Kategorien von antiforensischen Maßnahmen kennen und bewerten. Flashbasierte Speichertechnologien sowie der direkte Zugriff auf einen Datenträger und die zugehörige Auswertung sind low-level Fertigkeiten, die die Studierenden einsetzen.

An Hand der Erstellung eines Gutachtens für ein Fallbeispiel werden die gelernten Inhalte praktisch und umfassend geübt. Im Seminar erarbeiten die Teilnehmer selbständig Kenntnisse zu vertieften und speziellen Themen auf dem Gebiet der digitalen Forensik. Jeder Teilnehmer gibt eine Seminararbeit im LNCS-Format ab und präsentiert diese. Es findet auch ein Peer-Review der eingereichten Seminararbeiten statt.
Leistungsnachweis
Notenschein: Die Übung und das Seminar müssen bestanden werden (unbenotete Prüfungsvorleistung). Die Prüfungsleistung ist die Erstellung eines Gutachtens an Hand bereitgestellter Images. Weitere Details zu den Prüfungsleistungen werden zu Beginn des Moduls bekannt gegeben.
Verwendbarkeit
Die im Modul vermittelten Techniken der digitalen Forensik sind in der Beweissicherung und der Zuordnung von Vorfällen im digitalen Zeitalter unerlässlich. Die gelernte Methodik lässt sich auf bisher unbekannte IT-forensische Fragestellungen übertragen.
Dauer und Häufigkeit
Das Modul dauert 2 Trimester.

Modulname	Modulnummer
Compilerbau	3647

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Stefan Brunthaler	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
36471	VL	Compilerbau	Pflicht	2
36472	UE	Compilerbau	Pflicht	4
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen
Von den Studierenden werden Kenntnisse in der maschinennahen Programmierung vorausgesetzt, wie sie z.B. in der gleichnamigen Bachelorveranstaltung vermittelt werden.
Qualifikationsziele
Studierende erwerben fundierte Kenntnisse sowohl über theoretische Grundlagen des Compilerbaus, als auch deren praktische Anwendung zur systematischen, Werkzeug-unterstützten Erstellung von Compilern.
Inhalt
Die Vorlesung Compilerbau orientiert sich am Buch "Essentials of Compilation" von Prof. Siek an der Indiana University, Bloomington. Es wird ein Compiler erstellt, der schrittweise eine Untermenge von Scheme bzw. Racket nach Intel x86-64 übersetzt. Dabei wird die Untermenge von Scheme didaktisch optimal ebenfalls schrittweise um zusätzliche Fähigkeiten erweitert, die dann wiederum eine Änderung der einzelnen Übersetzungsschritte nach sich zieht. Der Fokus der Vorlesung liegt daher mehr auf dem Thema Codegenerierung, im Speziellen, Register Allokation, Instruction Selection und Peephole Optimization. Das Thema Typ-Überprüfung wird ebenfalls ausführlich behandelt.
Leistungsnachweis
Schriftliche Prüfung 120 Minuten oder Notenschein.
Dauer und Häufigkeit
Das Modul dauert 1 Trimester.

Modulname	Modulnummer
Compilerbau (erweitert)	3648

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Stefan Brunthaler	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
36471	VL	Compilerbau	Pflicht	2
36472	UE	Compilerbau	Pflicht	4
36481	P	Praktikum Compilerbau	Pflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Von den Studierenden werden Kenntnisse in der maschinennahen Programmierung vorausgesetzt, wie sie z.B. in der gleichnamigen Bachelorveranstaltung vermittelt werden.

Qualifikationsziele

Studierende erwerben fundierte Kenntnisse sowohl über theoretische Grundlagen des Compilerbaus, als auch deren praktische Anwendung zur systematischen, Werkzeug-unterstützten Erstellung von Compilern.

Inhalt

Die Vorlesung Compilerbau orientiert sich am Buch "Essentials of Compilation" von Prof. Siek an der Indiana University, Bloomington. Es wird ein Compiler erstellt, der schrittweise eine Untermenge von Scheme bzw. Racket nach Intel x86-64 übersetzt. Dabei wird die Untermenge von Scheme didaktisch optimal ebenfalls schrittweise um zusätzliche Fähigkeiten erweitert, die dann wiederum eine Änderung der einzelnen Übersetzungsschritte nach sich zieht.

Der Fokus der Vorlesung liegt daher mehr auf dem Thema Codegenerierung, im Speziellen, Register Allokation, Instruction Selection und Peephole Optimization. Das Thema Typ-Überprüfung wird ebenfalls ausführlich behandelt.

Das Praktikum Compilerbau vertieft die Kenntnisse des Compilerbaus und bietet folgende Erweiterungen des in der VL & UE erstellten Compilers:

1. Fokus Syntax: Erstellen eines einfachen Frontends anhand des Buchs "Beautiful Racket" fuer eine einfache Untermenge von Pascal. Diese Untermenge von Pascal soll auf die vom Compiler unterstützte Untermenge von Racket abgebildet werden.

2. Fokus Optimierung: Erstellen eines einfachen, automatischen Instruction Selection Mechanismus basierend auf KURS Baumgrammatiken und Baumautomaten.
3. Fokus Sicherheit: Implementierung aufwändigerer und vollständigerer Verteidigungen aus dem Bereich sprachbasierter Sicherheit.

Die Richtungen können in Zweier-Gruppen bearbeitet werden und abschließend nach einer Präsentation vor allen Teilnehmern besprochen.

Leistungsnachweis
Notenschein.
Dauer und Häufigkeit
Das Modul dauert 2 Trimester.

Modulname	Modulnummer
Quantenkommunikation	3695

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. rer. nat. Wolfgang Hommel	Wahlpflicht	2

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3695-V1	VÜ	Quantenkommunikation	Pflicht	3
3695-V2	P	Praktikum Quantenschlüsselaustausch	Wahlpflicht	3
3695-V3	SE	Seminar Quantentechnologien	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Grundlegende Kenntnisse in linearer Algebra, komplexen Zahlen sowie Interesse an Quantenphysik und -technologie. Grundwissen über Kryptographie ist hilfreich, aber nicht zwingend erforderlich.

Qualifikationsziele

Verständnis des Quantenschlüsselaustauschs (Quantum Key Distribution, QKD) und seiner mathematischen Modellierung über Zweizustandssysteme. Kenntnisse der wichtigsten Protokolle zum Schlüsselaustausch sowie von Postprocessing-Methoden des Schlüsselmaterials (Privacy Amplification, Quantum Error Correction). Überblick über mögliche Angriffe auf den Quantenschlüsselaustausch sowie Maßnahmen zu deren Abwehr. Verständnis der Herausforderungen bei der technologischen Umsetzung des Quantenschlüsselaustauschs.

Praktisches Verständnis davon, wie der Quantenschlüsselaustausch experimentell umgesetzt werden kann. Überblick über die aktuellen Entwicklungen in im Bereich Quantentechnologien.

Inhalt

Der Quantenschlüsselaustausch ist eine der wichtigsten Quantentechnologien.
Seine Bedeutung entsteht daraus, dass die Sicherheit auf physikalischen Prinzipien beruht, nicht wie bei konventioneller Kryptographie auf Annahmen über den Rechnenaufwand beim Lösen bestimmter mathematischer Probleme. Daher ist der Quantenschlüsselaustausch auch sicher gegenüber Angriffen von Quantencomputern. Dieses Modul bietet eine Einführung in die Theorie und Praxis dieser neuen und spannenden Technologie.

Vorlesung:

- Grundlegender Formalismus der Quantenmechanik für Zweizustandssysteme
- Wichtigste Protokolle zum Quantenschlüsselaustausch (BB84, Ekert91, COW-Protokoll)
- Technologische Umsetzung von Qubits für den Quantenschlüsselaustausch
- Postprocessing-Methoden des Schlüsselmaterials: Error Correction, Privacy Amplification
- Sicherheitsanalysen, Seitenkanäle und Quantum Hacking
- Quantenkommunikationsnetzwerke und Quantenrepeater

Praktikum:

- Durchführung eines QKD-Modellversuchs, der das BB84-Protokoll mit polarisiertem Licht in der Praxis umsetzt
- Detailliertes Wissen über die Schritte, die für ein QKD-Protokoll erforderlich sind
- Experimentelle Durchführung des Protokolls in Teams bestehend aus zwei Personen, die die Rolle von Sender und Empfänger übernehmen
- Versenden einer mit Quantenschlüsseln verschlüsselten Nachricht
- Verfassen eines Versuchsprotokolls

Seminar: Aktuelle Themen in den folgenden Bereichen:

- Verschiedene technologische Realisierungen des Quantenschlüsselaustausches
- Quantum Hacking
- Überblick über bestehende und geplante Quantenkommunikationsnetzwerke
- Ansätze zur Realisierung von Quantenrepeatern
- Standardisierung von Protokollen und Geräten zum QKD-Schlüsselmanagement
- Aktuelle technologische Fortschritte in den Bereichen Quantenmeteorologie, Quantensensoren und Quantencomputern

Leistungsnachweis
Schriftliche Prüfung (60 min) oder mündliche Prüfung (30 min) oder Notenschein. Die Prüfungsform wird zu Beginn des Moduls festgelegt.
Dauer und Häufigkeit
Das Modul wird jedes Jahr ab dem WT angeboten und dauert zwei Trimester. Die Vorlesung wird im WT angeboten, das Praktikum oder das Seminar im FT.

Modulname	Modulnummer
Reverse Engineering	3819

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Johannes Kinder	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
38191	VL	Reverse Engineering	Pflicht	2
38192	P	Reverse Engineering	Pflicht	4
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Von den Studierenden werden Kenntnisse in der maschinennahen Programmierung vorausgesetzt, wie sie z.B. in der gleichnamigen Bachelor-Veranstaltung vermittelt werden.

Grundlagen von Betriebssystemen, wie sie z.B. in der Bachelorvorlesung Einführung in Betriebssysteme vermittelt werden.

Qualifikationsziele

Die Studierenden erwerben die Fähigkeit, passende Werkzeuge und Methoden zur Analyse von geschützten Programmen zu bewerten und auszuwählen, sowie die praktische Fähigkeit, Programme manuell zu analysieren bzw. für eine automatisierte Analyse vorzubereiten. Sie können dabei wiederkehrende Aufgaben identifizieren und geeigneten Mechanismen (z.B. Skripte/Plugins) zur Unterstützung entwickeln. Dies ermöglicht ihnen, in kompilierten Programmen ohne Zugriff auf Quelltext effektiv nach Informationen oder Schwachstellen zu suchen.

Inhalt

Die Vorlesung behandelt aktuelle Themengebiete des Reverse Engineerings, insbesondere relevante Grundlagen, wie Maschinensprache, Disassemblierung, Debugging, und die Semantik von Instruktionen. Ein Schwerpunkt wird auf die Analyse des Kontrollflusses gesetzt, und wie das Verhalten von Code zur Laufzeit vorhergesagt werden kann. Dabei sind sowohl interaktive statische und/oder dynamische Methoden, als auch automatische Methoden von Interesse.

Darüber hinaus beschäftigt sich die Vorlesung mit verschiedenen Schutzmechanismen (Obfuscations), die ein Reverse Engineering verhindern sollen, und effektiven Gegenmaßnahmen. Dies beinhaltet z.B. sog. „Packer“, die verschlüsselte Programme

zur Laufzeit in den Arbeitsspeicher entpacken, sowie „Virtualizer“, die einen zufälligen Interpreter für jedes Programm erzeugen.

Im Praktikum Reverse Engineering lernen die Studierenden, die in der Vorlesung vermittelten Techniken umzusetzen. Hierbei werden verschiedene aktuelle Tools eingesetzt, um komplexe Probleme aus der Praxis eigenständig bzw. in kleinen Teams zu lösen.

Leistungsnachweis
Notenschein oder schriftliche Prüfung mit 60 Minuten Dauer oder mündliche Prüfung mit 20 Minuten Dauer. Die Prüfungsform wird zu Beginn des Moduls festgelegt.
Verwendbarkeit
Die manuelle oder automatisierte Analyse von Programmen mittels Reverse Engineering ist in der praktischen Sicherheitsanalyse von Software in vielen Bereichen unumgänglich.
Dauer und Häufigkeit
Das Modul dauert 1 Trimester.

Modulname	Modulnummer
Cyber Network Capabilities Methoden	3822

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Hartmut König	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3822 -V1	VÜ	CNC Methoden	Pflicht	3
3822 -V2	P	Praktikum CNC Methoden	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Grundlegende Kenntnisse zu Betriebssystemen und Rechnernetzen, wie sie z. B. im Bachelor-Modul Einführung in die Technische Informatik vermittelt werden, sowie Kenntnisse zu den Grundlagen der IT-Sicherheit aus den Pflichtfächern des Studiengangs. Die Anwendung von CNC-Methoden erfordert darüber hinaus detaillierte Kenntnisse der rechtlichen Rahmenbedingungen ihres Einsatzes. Deshalb wird empfohlen, das Modul Rechtliche Grundlagen CNC vorher (falls angeboten), in Begleitung zu diesem Modul oder danach unbedingt zu belegen.

Qualifikationsziele

Die Studierenden lernen die wichtigsten CNC-Methoden, u.a. die Grundlagen für die Informationstechnische Überwachung (Quellen-TKÜ und Onlinedurchsuchung), die Funktionsweise von Schwachstellen und Exploits und den sicheren Umgang mit diesen, Maßnahmen nach §100i StPO, Messenger-Überwachung, Gewinnung von OSINT-Daten und die dafür eingesetzten Werkzeuge kennen. Sie können die Einsatzfelder der Methoden eingrenzen, lernen die notwendigen Voraussetzungen und Schritte ihres Einsatzes kennen. Darüber hinaus erwerben sie praktische Fähigkeiten im Umgang mit CNC-Systemen und Werkzeugen.

Inhalt

Die Vorlesung behandelt die wichtigsten CNC-Methoden, stellt die Randbedingungen ihres Einsatzes vor, und erläutert die dafür notwendige Infrastruktur. Sie verweist auch auf die rechtlichen Rahmenbedingungen, die ausführlich im Modul *Rechtliche Grundlagen CNC* behandelt werden. Sie stellt die verschiedenen Phasen der Durchführung von CNC-Maßnahmen vor (Aufklärung, Einbringung, Datengewinnung, Rückstandsfreies Löschen) und erläutert wichtige Arbeitstechniken, z. B. Aufklärung auf dem Gerät, unentdecktes Bewegen im Netz, u.a.

Im Praktikum CNC-Methoden lernen die Studierenden, die in der Vorlesung vermittelten Techniken praktisch anzuwenden. Sie werden in die Nutzung verschiedener CNC-Systeme und Werkzeuge eingeführt, um komplexere Probleme aus der Praxis eigenständig bzw. in kleinen Teams zu lösen.
Leistungsnachweis
Notenschein, zu dessen Erwerb das Praktikum erfolgreich absolviert und zur Vorlesung eine schriftliche (90 Min) oder mündliche (20 Min) Prüfung abgelegt werden muss. Der genaue Prüfungsmodus wird zu Beginn des Moduls festgelegt.
Verwendbarkeit
Das Beherrschen von CNC-Methoden und -Werkzeugen und der sichere und verantwortungsvolle Umgang mit diesen ist essentielle Voraussetzung für einen Einsatz in der der Telekommunikationsüberwachung sowie der Weiterentwicklung dieser Methoden.
Dauer und Häufigkeit
Das Modul dauert ein Trimester.

Modulname	Modulnummer
Rechtliche Grundlagen Cyber Network Capabilities	3823

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Hartmut König	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
3823-V1	VL	Rechtliche Grundlagen CNC	Pflicht	4
3823-V2	UE	Rechtliche Grundlagen CNC (Übung)	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Keine.

Qualifikationsziele

Die Studierenden lernen die rechtlichen Grundlagen für die informationstechnische Überwachung (Quellen-TKÜ und Onlinedurchsuchung) durch Polizei und Nachrichtendienste in Deutschland kennen und werden befähigt, die rechtlichen Rahmenbedingungen bei der Anwendung von CNC-Methoden in der Praxis richtig einzuschätzen und im Sinne eines angemessenen, grundrechtskonformen Interessenausgleichs zu beurteilen.

Das Modul sollte vor bzw. nach oder in Begleitung des Moduls CNC-Methoden belegt werden.

Inhalt

Die Vorlesung vermittelt Grundkenntnisse zu

- den im Zusammenhang mit Quellen-TKÜ und Onlinedurchsuchung stehenden grundrechtlichen Anforderungen
- Artikel 10 Gesetz
- den §§ 100 ff. StPO
- sowie den einschlägigen weiteren Regelungen der Strafprozessordnung (StPO), des Telekommunikationsgesetzes (TKG), des Telemediengesetzes (TMG) und den rechtlichen Grundlagen zur Durchführung einer Telekommunikationsüberwachung aus dem BKA-Gesetz, dem Bundesverfassungsschutzgesetz, dem BND-Gesetz, dem BSI-Gesetz und dem Zollfahndungsgesetz (ZfDG) als Teil der Gesamtrechtsordnung zwecks eigenständiger Einordnung und Beurteilung entsprechender Sachverhalte
- unter Berücksichtigung einschlägiger Rechtsprechung.

Des Weiteren sollen die Studierenden die TKÜ-Verordnung und die Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation (TR TKÜV) kennenlernen und Beispiele aus der Praxis an Hand dieser Vorschriften sicher bewerten können. Abschließend wird auf den Errichtungserlass der ZITiS eingegangen.
Leistungsnachweis
Notenschein
Verwendbarkeit
Für den sicheren und verantwortungsvollen Umgang und den Einsatz von CNC-Methoden und -Werkzeugen ist es unabdingbar, den rechtlichen Rahmen und die einschlägigen Rechtsvorschriften zu kennen und Sachverhalte in der informationstechnischen Überwachung klar beurteilen und einordnen zu können.
Dauer und Häufigkeit
Das Modul dauert ein Trimester.

Modulname	Modulnummer
Statische Programmanalyse	3838

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Johannes Kinder	Wahlpflicht	4

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	84	96	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
38381	VÜ	Statische Programmanalyse	Pflicht	4
38382	P	Praktikum Statische Programmanalyse	Pflicht	3
Summe (Pflicht und Wahlpflicht)				7

Empfohlene Voraussetzungen

Vorausgesetzt werden Grundkenntnisse der mathematischen Logik wie sie im Bachelor vermittelt werden. Darüber hinaus sind für das Praktikum Kenntnisse in funktionalen Programmiersprachen (z.B. Scala) hilfreich, aber nicht notwendig.

Qualifikationsziele

Die Studierenden kennen die wichtigsten Konzepte und Techniken aus dem Bereich der statischen Programmanalyse. Sie erwerben ein Verständnis der mathematischen Grundlagen sowie der Chancen und Grenzen dieser Verfahren. Sie sind ebenso in der Lage, einfache statische Analysen selbst umzusetzen.

Inhalt

Statische Programmanalysen sind in modernen Entwicklungsprozessen ein häufig eingesetztes Werkzeug zur automatischen Fehlersuche. Ursprünglich hauptsächlich im Bereich der sicherheitskritischen Software verwendet, findet man kommerzielle Tools zunehmend als Teil von Continuous-Integration Plattformen. Viele führende Softwarefirmen beschäftigen mittlerweile Teams, die angepasste Software für die statische Analyse der eigenen Code-Basis entwickelt und pflegt.

Statische Programmanalyse bezeichnet Verfahren, die automatisch Software untersuchen, um bestimmte Eigenschaften zu überprüfen oder automatisch Fehler zu finden. Dabei wird die Software nicht ausgeführt, sondern ausschließlich der Programmcode (Quelltext oder Maschinensprache) betrachtet. Die zu Grunde liegende Idee ist, mit Hilfe von mathematischen Verfahren die Semantik des Programms zu approximieren, und so Fehler und Schwachstellen auszuschließen oder zu finden.

Die Vorlesung Statische Programmanalyse gibt einen Überblick über die relevanten Grundlagen und stellt dann ausgewählte Anwendungen vor. Abgedeckte Themen sind unter anderem:

- Automatische Fehlersuche
- Datenflussanalyse
- Kontrollflussanalyse
- Pointeranalyse
- Abstrakte Interpretation

Im begleitenden Praktikum Statische Programmanalyse lernen die Studierenden, Techniken der statischen Analyse selbst für eine einfache Programmiersprache zu implementieren.

Leistungsnachweis
Notenschein

Verwendbarkeit
Statische Programmanalysen sind weit verbreitet, Einsatzgebiete sind unter anderem die automatische Fehlersuche zur Entwicklungszeit, Security Audits von binärer Third-Party Software, Compileroptimierungen und Unterstützung und Automatisierung innerhalb von Entwicklungsumgebungen.

Dauer und Häufigkeit
Das Modul dauert ein Trimester.

Modulname	Modulnummer
Dynamische Programmanalyse	3849

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Johannes Kinder	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	84	96	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
38491	VÜ	Dynamische Programmanalyse	Pflicht	4
38492	P	Praktikum Fuzzing	Pflicht	3
Summe (Pflicht und Wahlpflicht)				7

Empfohlene Voraussetzungen

Von den Studierenden werden Kenntnisse in der maschinennahen Programmierung vorausgesetzt, wie sie in der gleichnamigen Bachelor-Veranstaltung vermittelt werden. Kenntnisse in der Programmiersprache Python sind hilfreich, aber nicht notwendig.

Qualifikationsziele

Die Studierenden kennen verschiedene Konzepte und Werkzeuge der dynamischen Programmanalyse. Dies beinhaltet das Verständnis verschiedener Verfahren zur automatischen Suche nach Fehlern, insbesondere des automatischen Fuzz Testings. Sie können verschiedene Techniken aus diesen Bereichen umsetzen und ihre Vor- und Nachteile abwägen.

Inhalt

Dynamische Programmanalysen bezeichnen zusammenfassend Verfahren, die automatisch Software zur Laufzeit untersuchen um Informationen über das Programmverhalten zu bekommen, wie z.B. welche Eingaben zu Programmabstürzen führen, oder ob die Software vertrauliche Informationen ausgeben kann. Dynamische Programmanalysen basieren teils auf Zufallsverfahren, teils auf logischer Charakterisierung der Eingaben. Sie werden in der Praxis eingesetzt um Fehler und Schwachstellen in Software zu verhindern oder zu erkennen.

Die Vorlesung behandelt unter anderem die folgenden Themen und Techniken:

- Fuzzing (Mutation-based, Grammar-based)
- Coverage Feedback
- Taint Tracking
- Binary Instrumentation
- Symbolic Execution

Im Praktikum Fuzzing lernen die Studierenden den Stand der Technik und praktische Herausforderungen im Fuzztesting kennen. Als Teil des Praktikums wenden die Studenten bestehende Systeme an und entwickeln auch einen eigenen Fuzzer und eigene Teststrategien. In vielen Fällen wird Eigenrecherche und Autodidaktik zur Lösung der Aufgaben notwendig sein.
Leistungsnachweis
Notenschein
Verwendbarkeit
Dynamische Programmanalyse und Fuzzing sind in der Praxis weit verbreitet und werden ergänzend zur manuellen Analyse von Programmen eingesetzt.
Dauer und Häufigkeit
Das Modul dauert ein Trimester.

Modulname	Modulnummer
Mobile Security	5513

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Gabi Dreo Rodosek	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
11972	VÜ	Mobile Kommunikationssysteme	Pflicht	3
55131	VÜ	Sichere mobile Systeme	Wahlpflicht	3
55132	VÜ	Sensorik und Manipulationsdetektion	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Für die Veranstaltungen im Modul werden grundlegende Kenntnisse in Rechnernetzen vorausgesetzt, wie sie z.B. im Bachelor-Modul Einführung in die Technische Informatik vermittelt werden.

Qualifikationsziele

Die Studierenden erhalten ein umfassendes Wissen der Funktionsweise mobiler Kommunikationsnetze. Sie können die wichtigsten Grundlagen drahtloser Kommunikationstechniken erläutern und die verschiedenen Verfahren und Systeme kategorisieren. Je nach erfolgter Auswahl innerhalb des Moduls haben sie vertiefte Kenntnisse in Bezug auf die Sicherheitsaspekte der Übertragungswege oder der Hardware-Komponenten. Sie sind in der Lage, die Wirksamkeit von Sicherheitsmaßnahmen einzuordnen und Sicherheitseigenschaften von mobilen Kommunikationssystemen zu bewerten. Sie erhalten eine erste Orientierung zum Vorgehen bei der Absicherung von mobilen Systemen durch Auswahl der Technologie und Konfiguration des Systems und den Einsatz spezieller Sicherheitsmechanismen.

Inhalt

Die Pflichtveranstaltung behandelt die wesentlichen Techniken zur Realisierung von mobiler (drahtloser) Kommunikation mit dem Schwerpunkt auf IT-Systemen. Dazu gehören die Funkübertragungstechniken, insbesondere die zellenbasierten Funksysteme, die Medienzugriffsverfahren, die die gemeinsame Nutzung des Funkraums koordinieren (Multiplexverfahren, Kollisionserkennung und -vermeidung), und die mobilen Varianten der Vermittlungsschicht (mobile IP, ad-hoc networking, Routingverfahren) und der Transportschicht (flow control, quality of service). Daneben werden die verschiedenen Arten der verwendeten mobilen Kommunikationssysteme vorgestellt: Drahtlose Telekommunikationssysteme (u.a. GSM, UMTS, LTE), Satellitensysteme, Rundfunksysteme (DAB, DVB) und drahtlose lokale Netze (u.a. WLAN, Bluetooth).

In der Wahlpflichtveranstaltung „Sichere Mobile Systeme“ werden zum einen verschiedene Kommunikationsstandards (u.a. WLAN, Bluetooth, und IEEE 802.15.4) vorgestellt, die im Bereich IoT ihren Einsatz finden, welche Einschränkungen sie haben und welche Sicherheitsaspekte sie erfüllen. Zum anderen werden konkrete Anwendungen wie elektronische Ausweise, Gesundheitskarte und mobiles Bezahlen näher betrachtet.

Ergänzend zu den Grundlagen werden in der Vorlesung Sensorik und Manipulationsdetektion Algorithmen, Protokolle und Paradigmen für den Einsatz von Sensornetzen sowie deren Absicherung vorgestellt. Dabei werden Konzepte wie etwa Lokalisierung, Zeitsynchronisation und datenzentrische Ansätze betrachtet sowie Lösungen für System-Software, Aggregation, Routing und Datenverteilung aus der Perspektive von Sensornetzen betrachtet. Ferner behandelt die Vorlesung Grundlagen, Systeme und Verfahren zur Detektion von Manipulationen. Dies beinhaltet die gesicherte Informationsübertragung in verteilten Systemen sowie die Bestätigung und Überprüfung von detektierten Ereignissen durch verschiedene Methoden.

Leistungsnachweis
Notenschein
Dauer und Häufigkeit
Das Modul dauert 2 Trimester.

Modulname	Modulnummer
Cryptography Engineering	5519

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Cornelius Greither	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
12111	VÜ	Algorithmische Zahlentheorie	Pflicht	5
12112	VÜ	Ausgewählte mathematische Methoden in Kryptographie und Codierungstheorie	Wahlpflicht	3
55191	VÜ	Post-Quantum Kryptographie	Wahlpflicht	3
55192	P	Implementierung und Anwendung kryptographischer Verfahren	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Grundlagen zur Kryptographie und Kryptoanalyse, wie sie z.B. im Modul Kryptologie vermittelt werden.

Qualifikationsziele

Die Studierenden erlernen fortgeschrittene Konzepte und Algorithmen der Kryptographie und können ihr Wissen im Bereich der Kryptographie in Gebieten ihrer Wahl vertiefen. Dies können algebraische Methoden für den Entwurf von kryptographischen Verfahren oder kryptoanalytischen Verfahren sein oder Algorithmen im Bereich der Quantencomputer sowie Verfahren, die auch bei Verwendung von Quantencomputern noch sicher sind. Auch praktische Erfahrungen bei der Implementierung von kryptographischen Verfahren und von Analyse-Verfahren werden vermittelt.

Inhalt

Die Veranstaltung "Algorithmische Zahlentheorie" befasst sich mit grundlegenden Begriffen und Algorithmen der algebraischen Zahlentheorie. (Stichworte: Primelemente, Primalitätstests, Faktorisierung, elliptische Kurven, u.a.). Ein Großteil dieser abstrakten Konzepte ist fundamental für die moderne Kryptographie (Public Key) und die Codierungstheorie. Der Schwerpunkt dieser Vorlesung ist zwar die systematische Erarbeitung der theoretischen Grundlagen und grundlegenden Algorithmen, es wird aber auch immer wieder auf Anwendungen eingegangen. Ergänzt werden diese durch zahlentheoretische Konzepte, die eventuell in einer Post-Quantencomputer-Epoche relevant sein könnten.

Die Veranstaltung "Ausgewählte mathematische Methoden der Kryptographie und Codierungstheorie" befasst sich mit ausgewählten und fortgeschrittenen Themen aus der Kryptographie und/oder der Codierungstheorie. Hierhin gehören kryptographische Verfahren, die auf zahlentheoretischen Ergebnissen aufsetzen, und "gute" Codes, die man mit Hilfe von algebraischen Kurven gefunden hat. Sowohl kryptographische als auch codierungstheoretische Inhalte sind vorgesehen; die Gewichtung zwischen diesen beiden Gebieten kann aber variieren.

Ein sehr wichtiges theoretisches Resultat von Peter Shor besagt, dass man mit Hilfe von Quantencomputern schnell große Zahlen faktorisieren kann und damit viele der heutzutage häufig verwendeten kryptographischen Verfahren brechen kann.
In der Vorlesung mit Übungen "Post-Quantum Kryptographie" soll zuerst dieses Resultat mit den notwendigen Grundlagen vorgestellt werden. Dann sollen einerseits quantenkryptographische Verfahren präsentiert werden und andererseits Verfahren, die sogar gegen Angriffe mit Hilfe von Quantencomputern resistent sind. Genannt seien: gitterbasierte Verfahren, codebasierte Verfahren, Hash-Verfahren und Verfahren, die auf multivariaten Polynomen basieren.

In dem Praktikum "Implementierung und Anwendung kryptographischer Verfahren" werden verschiedene kryptographische und kryptoanalytische Verfahren implementiert. Dabei werden auch verschiedene Anwendungsbereiche abgedeckt, z.B. Verschlüsselung von Nachrichten, Signatur-Verfahren, Authentizität von Nachrichten, Authentifikation von Kommunikationsteilnehmern sowie für diese Probleme geeignete Protokolle. Es werden auch Analyse-Verfahren und mögliche Angriffe auf kryptographische Protokolle implementiert und durchgespielt.

Leistungsnachweis

Schriftliche Prüfung mit 60 Minuten Dauer oder mündliche Prüfung mit 30 Minuten Dauer oder Notenschein. Die Prüfungsform wird zu Beginn des Moduls festgelegt.

Dauer und Häufigkeit

Das Modul dauert 1-2 Trimester.

Sonstige Bemerkungen

Es ist entweder die Vorlesung "Algorithmische Zahlentheorie" und eine der anderen Veranstaltungen zu belegen; oder die beiden anderen Vorlesungen und das Praktikum. Je nach Kombination der Veranstaltungen, ergibt sich die TWS-Summe 8 bzw. 9.

Modulname	Modulnummer
Offensive Sicherheitsüberprüfungen	5523

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Arno Wacker	Wahlpflicht	4

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
270	108	162	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55091	VÜ	Penetration Testing	Pflicht	6
55093	P	Penetration Testing	Pflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Gute Kenntnisse in den Bereichen Netzsicherheit und Systemsicherheit, wie in den gleichnamigen beiden Modulen vermittelt.

Qualifikationsziele

Die Studierenden können organisationsinterne Überprüfungen der IT-Sicherheitseigenschaften von Systemen, Diensten und Netzen planen und durchführen. Sie beherrschen Testmethoden auf Netz-, Anwendungs- und Systemebene und haben ausgewählte aktuelle Werkzeuge für diesen Zweck kennengelernt. Sie kennen die Aufgabenbereiche und Randbedingungen von Red Teams und Pentesting-Dienstleistern.

Inhalt

Die Vorlesung Penetration Testing führt in die Aufgabengebiete von Pentesting- bzw. Red-Teams ein. Für verschiedene Anwendungsgebiete wie das Sicherheitstesten einzelner Systeme, komplexerer IT-Dienste und ganzer Rechnernetze und IT-Infrastrukturen werden die Vor- und Nachteile verschiedener Testvarianten wie Whitebox- und Blackbox-Tests analysiert. Unter Orientierung an bewährten Good-Practice-Dokumentationen wie OWASP und OSSTMM werden praxisrelevante Angriffsvarianten von der Reconnaissance-Phase bis zum Einbringen von Exploit-Payloads behandelt. Ebenso werden die strukturierte Erstellung von Pentesting-Berichten und deren Auswertung durch die auftraggebende Organisation betrachtet.

Das Praktikum Penetration Testing stellt auf Basis einer Praktikumsinfrastruktur (abgeschottete Laborumgebung) Aufgaben, in denen die Studierenden als fiktiver Auftragnehmer eines technischen Penetrationstests fungieren. Mithilfe ausgewählter bereitgestellter Softwarewerkzeuge müssen die für Pentests ausgewählten Systeme, Dienste und Subnetze erkundet und auf verschiedenste Verwundbarkeiten untersucht

werden, ohne den Betrieb der übrigen Infrastruktur zu beeinträchtigen. Für einige Überprüfungen müssen eigene Werkzeuge bzw. Skripte/Payloads konzipiert und implementiert werden. Über die gewählte Vorgehensweise, die einzelnen Schritte der Durchführung und die zu priorisierenden Ergebnisse ist eine Ausarbeitung zu erstellen, die vom Stil her an Pentest-Berichte angelehnt ist.
Leistungsnachweis
Notenschein
Dauer und Häufigkeit
Das Modul dauert 1-2 Trimester.

Modulname	Modulnummer
Privacy-Enhancing Cryptography	5548

Konto	Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Mark Manulis	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	72	108	6

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55481	VÜ	Advanced Cryptography	Pflicht	4
55482	SE	Seminar Research Trends in Privacy Tech	Pflicht	2
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Von den Studierenden werden grundlegende Kenntnisse von kryptographischen Verfahren und mathematischen Grundlagen aus dem Pflichtmodul "Kryptologie" sowie ein generelles Interesse an Privacy Tech und an der Verwendung von kryptographischen Verfahren zum Schutz der Privatheit vorausgesetzt.

Qualifikationsziele

Die Studierenden kennen verschiedene Konzepte und Verfahren zum Schutz der Privatheit mittels kryptographischer Methoden und beherrschen den Umgang mit entsprechender Sicherheitsmodellierung und -beweisführung. Sie sind in der Lage die technischen Lösungen zum Schutz der Privatheit kritisch zu analysieren und kennen den aktuellen Stand in Forschung und Entwicklung rund um die Technologien zum Schutz der Privatheit und deren Anwendungen.

Inhalt

Advanced Cryptography: In dieser Vorlesung werden moderne kryptographischen Methoden sowie weiterführende kryptographischen Verfahren und Protokolle vorgestellt. Neben der Funktionsweise wird auch auf die beweisbare Sicherheit der Verfahren eingegangen. Dazu werden moderne Methoden zur Sicherheitsmodellierung und -beweisführung (z.B. kryptographische Reduktionen) eingeführt. Aus der Sicht der beweisbaren Sicherheit werden sowohl die bereits bekannten Verfahrensklassen wie Einwegfunktionen, Hashfunktionen, digitale Signaturen und Verschlüsselungsverfahren wiederholt sowie neue Verfahren, wie etwa authenticated encryption, signcryption, zero-knowledge Protokolle, Identifikationsverfahren und Schlüsselvereinbarungsprotokolle vorgestellt. Zudem werden neue mathematischen Grundlagen und Verfahren basierend auf elliptischen Kurven und bilinearen Abbildungen eingeführt. In Übungen werden die Methoden der beweisbaren Sicherheit sowie die Funktionsweise von eingeführten Verfahren anhand von Rechen- und Beweisbeispielen anschaulich dargestellt.

Seminar Research Trends in Privacy Tech: In diesem Seminar wird den Studierenden ein Einblick in aktuelle Forschungsfelder rund um die technologischen Aspekte der Privacy gewährt. Die Schwerpunkte liegen bei Verfahren, Technologien und Anwendungen zum Schutz der Privatheit von Nutzern, deren Daten und digitalen Transaktionen. Zu Beginn der Veranstaltung wird eine Auswahlliste von aktuellen Themen vorgestellt, die von Studierenden über die Dauer der Veranstaltung ausgearbeitet und am Ende vorgetragen werden. Die Arbeiten sollen sich auf eine Auswahl relevanter Forschungsartikeln (aus bekannten Tagungen) und Open-Source Quellen (z.B. Softwarebibliotheken) stützen. Mögliche Themen rund um Privacy Tech sind etwa private messaging, anonymous communications, computing on encrypted data, secure multi-party computation, privacy in distributed ledgers und blockchain, electronic payments and cryptocurrencies, e-voting, privacy in IoT-Anwendungen, usw.

In allen Lehrveranstaltungen werden die Lehrmaterialien in englischer Sprache zur Verfügung gestellt. Die Veranstaltungen werden zum Teil auch in englischer Sprache gehalten.

Literatur

Katz, J. and Lindell, Y. Introduction to Modern Cryptography (2nd Edition), Chapman & Hall/CRC Cryptography and Network Security Series, 2014.

Leistungsnachweis

Notenschein, der zwei Teilleistungen umfasst. Die Prüfungsform wird zu Beginn des Moduls festgelegt.

Verwendbarkeit

Die hier erworbenen Kenntnisse und Fertigkeiten ergänzen die Ausbildung in IT-Sicherheit um die wichtigen technologischen Aspekte der Privatheit und entsprechenden kryptographischen Verfahren. Die Veranstaltungen fördern analytisches Denken nach Security & Privacy by Design und vermitteln die Fähigkeiten technische Verfahren zum Schutz der Privatheit zu entwerfen und ihr Einsatz in digitalen Anwendungen zu planen. Die Teilnahme an den Lehrveranstaltungen dieses Wahlpflichtmoduls ermöglicht den Studierenden die Übernahme einer Master-Arbeit im Überschneidungsbereich des technologischen Privacy-Schutzes und angewandter Kryptographie.

Dauer und Häufigkeit

Das Modul dauert 1 Trimester und wird im HT angeboten. Als Startzeitpunkt ist das 1. Studienjahr vorgesehen.

Modulname	Modulnummer
Seminarmodul CYB	5501

Konto	Seminar - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Arno Wacker	Pflicht	1

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
150	24	126	5

Empfohlene Voraussetzungen

Keine formalen Voraussetzungen, aber je nach Themengebiet sind Kenntnisse aus Modulen bestimmter Fächer wesentliche Grundlage. Wenn ein Vertiefungsfeld gewählt wird, dann ist es empfehlenswert, das Seminar zu einem Thema dieses Vertiefungsfeldes zu belegen.

Qualifikationsziele

Die Studierenden haben Kenntnisse zu vertieften und speziellen fachlichen Themen des jeweiligen Themengebiets. Zusätzlich erwerben sie folgende Schlüsselqualifikationen:

- Die Fähigkeit, anspruchsvolle englische Originalliteratur zu lesen und zu verstehen.
- Die Fähigkeit, vor einem Fachpublikum einen Vortrag zu einem nichttrivialen wissenschaftlichen Thema zu entwerfen (also auch didaktisch richtig zu gestalten) und ihn unter Einsatz üblicher Medien abzuhalten.
- Die Fähigkeit, zu Diskussionen über wissenschaftlichen Themen beizutragen.
- Die Fähigkeit, Texte von ca. 15-30 Seiten zu verfassen, i.d.R. zur Erklärung wissenschaftlicher Inhalte.

Inhalt

Seminare behandeln wechselnde fachliche Themen, die auf Lehrstoffen aus dem Master-Studium aufbauen. Die Themen können schon vorhandene fachliche Interessen und Schwerpunkte vertiefen. Die Seminare werden in Kleingruppen durchgeführt. Die angebotenen Seminare werden vor Beginn des Moduls hochschulöffentlich bekannt gegeben. In der Regel arbeitet jeder Teilnehmer einen Vortrag zu vorgegebener Literatur aus und präsentiert ihn in der Gruppe, die anschließend Fragen dazu stellt.

Leistungsnachweis

Ein benoteter Schein, für den im einzelnen folgende Leistungen zu erbringen sind:

- Abhalten eines Vortrags
- Erstellen einer Ausarbeitung zum Vortrag
- Teilnahme an den Diskussionen zu allen Vorträgen

Die Note ergibt sich i.W. aus der Qualität des Vortrags und der Ausarbeitung.

Verwendbarkeit
Das Seminarmodul stärkt die Fähigkeit der Studierenden zur wissenschaftlichen Recherche und zur Präsentation wissenschaftlicher Erkenntnisse. Es versetzt die Studierenden verstärkt in die Lage, sich Erkenntnis und Wissen selbstständig aktiv zu erarbeiten und zu reflektieren, statt diese überwiegend rezeptiv aufzunehmen. Durch die exemplarische Vertiefung der im Studium behandelten Inhalte werden Studierende an die Forschung herangeführt, die für eine universitäre Ausbildung unverzichtbar ist.
Dauer und Häufigkeit
Das Modul dauert 1 Trimester. Seminare werden in jedem Trimester angeboten. Es wird empfohlen, das Seminar im 2., 3. oder 4. Fachtrimester zu belegen.
Sonstige Bemerkungen
Aus den jeweils angebotenen Seminaren zu unterschiedlichen Themen ist eines auszuwählen. Zum Arbeitsaufwand: Der Hauptaufwand liegt in der Aufarbeitung eines Themas und der einmaligen Ausarbeitung des eigenen Vortrags. Dabei entfallen von den 126 Stunden Workload jeweils etwa 2/3 auf das Durcharbeiten der Literatur, und 1/3 auf das Erstellen der Vortragsfolien und Ausarbeitung.

Modulname	Modulnummer
Masterarbeit CYB	5500

Konto	Masterarbeit - CYB 2022

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. rer. nat. Wolfgang Hommel	Pflicht	5

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
900	0	900	30

Empfohlene Voraussetzungen
Vorausgesetzt werden die allgemeinen Kenntnisse aus dem Master-Studium.

Qualifikationsziele
Die Studierenden können eine anspruchsvolle Aufgabe selbständig analysieren und mit wissenschaftlichen Methoden bearbeiten. Sie haben Erfahrung in der Entwicklung von Lösungsstrategien und in der Dokumentation ihres Vorgehens. Sie haben in einem speziellen Forschungsgebiet der Cyber-Sicherheit vertiefende praktische Erfahrung gesammelt.

Inhalt
In der Master-Arbeit soll eine Aufgabe aus einem begrenzten Problemkreis unter Anleitung selbständig mit bekannten Methoden wissenschaftlich bearbeitet werden. In der Arbeit sind die erzielten Ergebnisse systematisch zu entwickeln und zu erläutern. Sie wird in der Regel individuell und eigenständig durch die Studierenden bearbeitet, kann aber je nach Thema auch in Gruppen von bis zu drei Studierenden bearbeitet werden.

Leistungsnachweis
Es ist eine schriftliche Ausarbeitung zu erstellen und diese ist im Rahmen eines Kolloquiums zu präsentieren. Die Präsentation findet als Vortrag von ca. 20-30 Minuten Dauer mit daran anschließenden Fragen statt. Die Präsentation wird benotet und geht in die Modulnote ein.

Verwendbarkeit
Die Anfertigung der Master-Arbeit bereitet auf eigenständige systematisch durchgeführte Arbeitsvorgänge in der beruflichen Tätigkeit oder der wissenschaftlichen Forschung vor.

Dauer und Häufigkeit
Das Modul dauert 2 Trimester. Das Modul beginnt jedes Studienjahr jeweils im Wintertrimester. Als Startzeitpunkt ist das Wintertrimester im 2. Studienjahr vorgesehen.

Modulname	Modulnummer
Seminar studium plus, Training	1008

Konto	Studium+ Master

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr. Ina Ulrike Paul	Pflicht	

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
150	72	78	5

Qualifikationsziele

***studium plus*-Seminare:**

Die Studierenden erwerben personale, soziale oder methodische Kompetenzen, um das Studium als starke, mündige Persönlichkeit zu verlassen. Die studium plus-Seminare bereiten die Studierenden dadurch auf ihre Berufs- und Lebenswelt vor und ergänzen die im Studium erworbenen Fachkenntnisse.

Durch die Vermittlung von Horizontwissen wird die eingeschränkte Perspektive des Fachstudiums erweitert. Dadurch lernen die Studierenden, das im Fachstudium erworbene Wissen in einem komplexen Zusammenhang einzuordnen und in Relation zu den anderen Wissenschaften zu sehen.

Durch die exemplarische Auseinandersetzung mit gesellschaftsrelevanten Fragen erwerben die Studierenden die Kompetenz, diese kritisch zu bewerten, sich eine eigene Meinung zu bilden und diese engagiert zu vertreten. Das dabei erworbene Wissen hilft, Antworten auch auf andere gesellschaftsrelevante Fragestellungen zu finden.

Durch die Steigerung der Partizipationsfähigkeit wird die mündige Teilhabe an sozialen, kulturellen und politischen Prozessen der modernen Gesellschaft gefördert.

***studium plus*-Trainings:**

Die Studierenden erwerben personale, soziale und methodische Kompetenzen, um als Führungskräfte auch unter komplexen und teils widersprüchlichen Anforderungen handlungsfähig zu bleiben bzw. um ihre Handlungskompetenz wiederzuerlangen.

Damit ergänzt das Trainingsangebot die im Rahmen des Studiums erworbenen Fachkenntnisse insofern, als diese fachlichen Kenntnisse von den Studierenden in einen berufspraktischen Kontext eingebettet werden können und Möglichkeiten zur Reflexion des eigenen Handelns angeboten werden.

Inhalt

Kurzbeschreibung:

Die **Seminare** vermitteln Einblicke in aktuelle Themen und neue Wissensgebiete. Sie finden wöchentlich während an einem - mit der jeweiligen Fakultät vereinbarten - Wochentag in den sog. Blockzeiten oder auch am Wochenende statt, wobei den Studierenden die Wahl frei steht.

Die **Trainings** entsprechen den Trainings für Führungskräfte in modernen Unternehmen und finden immer am Wochenende statt.

Langbeschreibung:

Die ***studium plus*-Seminare** bieten Lerninhalte, die Horizont- oder Orientierungswissen vermitteln bzw. die Partizipationsfähigkeit steigern. Sämtliche Inhalte sind auf den Erwerb personaler, sozialer oder methodischer Kompetenzen ausgerichtet. Sie bilden die Persönlichkeit und erhöhen die Beschäftigungsfähigkeit.

Bei der Vermittlung von Horizontwissen werden die Studierenden beispielsweise mit den Grundlagen anderer, fachfremder Wissenschaften vertraut gemacht, sie lernen Denkweisen und "Kulturen" der fachfremden Disziplinen kennen. Bei der Vermittlung von Orientierungswissen steigern die Studierenden ihr Reflexionsniveau, indem sie sich exemplarisch mit gesellschaftsrelevanten Themen auseinandersetzen. Bei der Vermittlung von Partizipationswissen steht der Einblick in verschiedene soziale und politische Prozesse im Vordergrund.

Einen detaillierten Überblick bietet das jeweils gültige Seminarangebot von *studium plus*, das von Trimester zu Trimester neu erstellt und den Erfordernissen der künftigen Berufswelt sowie der Interessenslage der Studierenden angepasst wird.

Die ***studium plus*-Trainings** bieten berufsrelevante und an den Themen der aktuellen Führungskräfteentwicklung von Organisationen und Unternehmen orientierte Lerninhalte.

Einen detaillierten und aktualisierten Überblick bietet das jeweils gültige Trainingsangebot von *studium plus*.

Leistungsnachweis

***studium plus*-Seminare:**

- In Seminaren werden Notenscheine erworben.
- Die Leistungsnachweise, durch die der Notenschein erworben werden kann, legt der/die Dozent/in in Absprache mit dem Zentralinstitut studium plus vor Beginn des Einschreibeverfahrens für das Seminar fest. Hierbei sind folgende wie auch weitere Formen sowie Mischformen möglich: Klausur, mündliche Prüfung, Hausarbeit, Referat, Projektbericht, Gruppenarbeit, Mitarbeit im Kurs etc. Bei Mischformen erhält der Studierende verbindliche Angaben darüber, mit welchem prozentualen Anteil die jeweilige Teilleistungen gewichtet werden.
- Der Erwerb des Scheins ist an die regelmäßige Anwesenheit im Seminar gekoppelt.
- Bei der während des Einschreibeverfahrens stattfindenden Auswahl der Seminare durch die Studierenden erhalten diese verbindliche Informationen über die Modalitäten des Scheinerwerbs für jedes angebotene Seminar.

***studium plus*-Trainings:**

- Die Trainings sind unbenotet, die Zuerkennung der ECTS-Leistungspunkte ist aber an die Teilnahme an der gesamten Trainingszeit gekoppelt.

Dieses Modul geht nur mit 3 ECTS-Punkten in die Gesamtnotenberechnung ein!

Verwendbarkeit
Das Modul ist für sämtliche Masterstudiengänge gleichermaßen geeignet.
Dauer und Häufigkeit
Das Modul dauert 2mal 1 Trimester. Das Modul findet statt im ersten Studienjahr jeweils im Frühjahrstrimester und im Herbsttrimester. Als Startzeitpunkt ist das Frühjahrstrimester im 1. Studienjahr vorgesehen.

Übersicht des Studiengangs: Konten und Module

Legende:

FT	= Fachtrimester des Moduls
PrFT	= frühestes Trimester, in dem die Modulprüfung erstmals abgelegt werden kann
Nr	= Konto- bzw. Modulnummer
Name	= Konto- bzw. Modulname
M-Verantw.	= Modulverantwortliche/r
ECTS	= Anzahl der Credit-Points

FT	PrFT	Nr	Name	M-Verantw.	ECTS
		7	**Pflichtmodule - CYB 2022**		**44**
1	1	5502	Netzsicherheit	G. Dreo Rodosek	6
1	2	5503	Hardwaresicherheit	K. Buchenrieder	6
1	4	5504	Datenschutz und Privacy	A. Wacker	6
2	2	5505	Systemsicherheit	G. Teege	6
1	2	5506	Kryptologie	A. Wacker	6
2	2	5507	Anwendungssicherheit	W. Hommel	6
2	3	5508	Security- und IT- Management	U. Lechner	8
		8 -10	**Überkonto Wahlpflicht - CYB 2022**		**36**
1	6	3459	Grundlagen der Informationssicherheit	W. Hommel	6
		8	**Wahlpflicht Vertiefungsfeld Enterprise Security (ES) CYB - 2022**		**30**
1	2	1008	Einführung in das Industrial Engineering	O. Rose	9
3	7	1034	Softwareentwicklungsumgebungen	M. Minas	6
4	4	1162	Erweiterte Digitale Forensik	H. Baier	6
1	1	1231	Data Mining und IT- basierte Entscheidungsunterstützung	S. Pickl	6
6	6	1306	Web Technologies	M. Koch	6
0	1	1398	Middleware und mobile Cloud Computing	A. Karcher	6
4	4	1446	Identitätsmanagement	D. Pöhn	6
0	1	1507	Enterprise Architecture und IT Service Management	A. Karcher	6
1	2	1518	Formale Entwicklung korrekter Software	B. Elbl	6
3	4	1551	Digitale Forensik	H. Baier	9
3	5	3584	Language-based Security	S. Brunthaler	6
3	1	3647	Compilerbau	S. Brunthaler	6
3	1	3648	Compilerbau (erweitert)	S. Brunthaler	9
4	3	3665	Benutzbare Sicherheit	F. Alt	9
2	5	3695	Quantenkommunikation	W. Hommel	6
3	3	3819	Reverse Engineering	J. Kinder	6
3	4	3820	Quantencomputer in Theorie und Praxis	R. Hölzl	6
4	4	3838	Statische Programmanalyse	J. Kinder	6
3		3849	Dynamische Programmanalyse	J. Kinder	6
3	5	5519	Cryptography Engineering	C. Greither	9
4	3	5523	Offensive Sicherheitsüberprüfungen	A. Wacker	9
		9	**Wahlpflicht Vertiefungsfeld Public Security (PS) - CYB 2022**		**30**
1	2	1008	Einführung in das Industrial Engineering	O. Rose	9
1	3	1033	Simulationstechnik	O. Rose	9
2	3	1144	Knowledge Discovery in Big Data	M. Geierhos	6

6	6	1306	Web Technologies	M. Koch	6
3	3	1394	Aviation Management, Computational Networks and System Dynamics	S. Pickl	6
0	1	1398	Middleware und mobile Cloud Computing	A. Karcher	6
3	4	1490	Operations Research, Complex Analytics and Decision Support Systems (ORMS I)	S. Pickl	9
1	2	1518	Formale Entwicklung korrekter Software	B. Elbl	6
3	3	2461	Ökonomie und Recht der Informationsgesellschaft	S. Koos	5
3	3	2994	Ausgewählte Kapitel des OR: Data-driven Optimization	M. Moll	9
4	3	3665	Benutzbare Sicherheit	F. Alt	9
4	4	3850	Natural Language Processing	M. Geierhos	6
1	4	3851	Information Retrieval	M. Geierhos	6
3	4	3852	Anwendungsgebiete der Data Science	M. Geierhos	6
3	3	3853	Analyse unstrukturierter Daten	M. Geierhos	6
3	4	5513	Mobile Security	G. Dreo Rodosek	6
3	3	5514	Staatliche IT-Sicherheit	U. Lechner	6
3	4	5521	Industrial Security	N. N.	6
3	0	5548	Privacy-Enhancing Cryptography	M. Manulis	6
		10	**Wahlpflicht Vertiefungsfeld Security Intelligence (SI) CYB - 2022**		**30**
2	3	1032	Analytische Modelle	M. Siegle	9
1	1	1037	Informations- und Codierungstheorie	P. Hertling	6
2	3	1144	Knowledge Discovery in Big Data	M. Geierhos	6
2	3	1152	Visual Computing (erweitert)	H. Mayer	9
3	3	1220	Quellencodierung und Kanalcodierung	A. Knopp	5
1	1	1231	Data Mining und IT- basierte Entscheidungsunterstützung	S. Pickl	6
8	2	1243	Signal- und Informationsverarbeitung	A. Knopp	8
0	3	1253	Sicherheit in der Kommunikationstechnik	B. Lankl	6
10	3	1289	Nachrichtentheorie und Übertragungssicherheit	B. Lankl	6
6	6	1306	Web Technologies	M. Koch	6
0	1	1398	Middleware und mobile Cloud Computing	A. Karcher	6
2	2	1489	Visual Computing	H. Mayer	6
3	4	1490	Operations Research, Complex Analytics and Decision Support Systems (ORMS I)	S. Pickl	9
3	3	2994	Ausgewählte Kapitel des OR: Data-driven Optimization	M. Moll	9
2	2	3491	Algorithmen und Komplexität	P. Hertling	5
2	5	3695	Quantenkommunikation	W. Hommel	6
3	4	3820	Quantencomputer in Theorie und Praxis	R. Hölzl	6
3	4	3852	Anwendungsgebiete der Data Science	M. Geierhos	6
3	3	3853	Analyse unstrukturierter Daten	M. Geierhos	6
3	5	5519	Cryptography Engineering	C. Greither	9
3	4	5521	Industrial Security	N. N.	6
		11	**Wahlpflicht Vertiefungsfeld Cyber Network Capabilities (CNC) CYB - 2022**		**30**
2	3	1152	Visual Computing (erweitert)	H. Mayer	9
4	4	1162	Erweiterte Digitale Forensik	H. Baier	6
1	1	1231	Data Mining und IT- basierte Entscheidungsunterstützung	S. Pickl	6
2	2	1489	Visual Computing	H. Mayer	6
3	4	1551	Digitale Forensik	H. Baier	9

3	1	3647	Compilerbau	S. Brunthaler	6
3	1	3648	Compilerbau (erweitert)	S. Brunthaler	9
2	5	3695	Quantenkommunikation	W. Hommel	6
3	3	3819	Reverse Engineering	J. Kinder	6
3	3	3822	Cyber Network Capabilities Methoden	H. König	6
3	3	3823	Rechtliche Grundlagen Cyber Network Capabilities	H. König	6
4	4	3838	Statische Programmanalyse	J. Kinder	6
3		3849	Dynamische Programmanalyse	J. Kinder	6
3	4	5513	Mobile Security	G. Dreo Rodosek	6
3	5	5519	Cryptography Engineering	C. Greither	9
4	3	5523	Offensive Sicherheitsüberprüfungen	A. Wacker	9
3	0	5548	Privacy-Enhancing Cryptography	M. Manulis	6
		11	**Seminar - CYB 2022**		**5**
1	0	5501	Seminarmodul CYB	A. Wacker	5
		12	**Masterarbeit - CYB 2022**		**30**
5	5	5500	Masterarbeit CYB	W. Hommel	30
		99MA	**Verpflichtendes Begleitstudium plus**		**5**
	0	1008	Seminar studium plus, Training	I. Paul	5

Übersicht des Studiengangs: Lehrveranstaltungen

Legende:

FT	= Fachtrimester der Veranstaltung
Nr	= Veranstaltungsnummer
Name	= Veranstaltungsname
Art	= Veranstaltungsart
P/Wp	= Pflicht / Wahlpflicht
TWS	= Trimesterwochenstunden

FT	Nr	Name	Art	P/Wp	TWS
	10342	Seminar Ausgewählte Kapitel der Software-Entwicklung	Seminar	Pf	2
	11443	Research Topics in Data Science	Seminar	WPf	3
	11445	Datenethik und -sicherheit	Seminar	WPf	3
	11446	Data Science Praktikum	Praktikum	WPf	3
	13943	Computational Networks	Vorlesung/Übung	WPf	3
	149010	Spieltheorie: Einführung in die mathematische Theorie strategischer Spiele	Vorlesung/Übung	WPf	3
	14902	Diskrete Optimierung	Vorlesung/Übung	WPf	3
	14904	Scheduling	Vorlesung/Übung	WPf	3
	14906	Soft Computing A: Management Science and Complex System Analysis - System Dynamics and Strategic Planning	Vorlesung/Übung	WPf	3
	14907	Soft Computing B: Fuzzy Systems - Network Operations	Vorlesung/Übung	WPf	3
	14909	Soft Computing D: Neural Networks and Network Analysis	Vorlesung/Übung	WPf	3
	35841	Praktikum Language-based Security	Praktikum	Pf	4
	35842	Seminar Language-based Security	Seminar	Pf	2
	38202	Praktikum Quantencomputer-Programmierung	Praktikum	Pf	3
	38382	Praktikum Statische Programmanalyse	Praktikum	Pf	3
	38491	Dynamische Programmanalyse	Vorlesung/Übung	Pf	4
	38492	Praktikum Fuzzing	Praktikum	Pf	3
	38524	Modulprojekt Anwendungsgebiete der Data Science	Projekt	WPf	3
	55093	Penetration Testing	Praktikum	Pf	3
	55132	Sensorik und Manipulationsdetektion	Vorlesung/Übung	WPf	3
	55191	Post-Quantum Kryptographie	Vorlesung/Übung	WPf	3
	55192	Implementierung und Anwendung kryptographischer Verfahren	Praktikum	WPf	3
	55211	Internet of Things and Industrial Internet Security	Vorlesung/Übung	WPf	3
	55212	Praktikum Sicherheit eingebetteter Systeme	Praktikum	WPf	3
	55213	Trusted Computing	Vorlesung/Übung	Pf	3
	55481	Advanced Cryptography	Vorlesung/Übung	Pf	4
	55482	Seminar Research Trends in Privacy Tech	Seminar	Pf	2
1	10081	Produktionsmanagement in der Fertigung	Vorlesung	Pf	3
1	10082	Ressourceneinsatzplanung für die Fertigung	Vorlesung	Pf	3
1	10101	Ausgewählte Kapitel der IT-Sicherheit	Vorlesung/Übung	Pf	3
1	10102	Netzsicherheit	Vorlesung/Übung	Pf	3
1	10103	Praktikum Netzsicherheit	Praktikum	Pf	3
1	10311	Eingebettete Systeme	Vorlesung/Übung	Pf	3
1	10331	Parallele und verteilte Simulation	Vorlesung/Übung	Pf	3
1	10333	Moderne Heuristiken	Vorlesung/Übung	WPf	3

1	1037	Informations- und Codierungstheorie	Vorlesung/Übung	WPf	5
1	11432	Sicherheit in der Informationstechnik	Vorlesung/Übung	Pf	3
1	12311	Data Mining und IT-basierte Entscheidungsunterstützung	Vorlesung/Übung	Pf	5
1	12431	Signalverarbeitung	Vorlesung/Übung	Pf	4
1	13981	Middleware und mobile Cloud Computing	Vorlesung	Pf	3
1	13982	Middleware und mobile Cloud Computing	Übung	Pf	2
1	15071	Enterprise Architecture und IT Service Management	Vorlesung	Pf	3
1	15072	Enterprise Architecture und IT Service Management	Übung	Pf	2
1	15171	Entwurf Verteilter Systeme	Vorlesung/Übung	WPf	5
1	15174	Spezifikation	Vorlesung/Übung	WPf	5
1	36471	Compilerbau	Vorlesung	Pf	2
1	36472	Compilerbau	Übung	Pf	4
1	36481	Praktikum Compilerbau	Praktikum	Pf	3
1	36651	Benutzbare Sicherheit	Vorlesung/Übung	Pf	3
1	36653	Praktikum Design sicherer und benutzbarer Systeme	Praktikum	Pf	3
1	55061	Einführung in die Kryptographie	Vorlesung/Übung	Pf	3
2	10083	Praktikum Produktionsplanung und -steuerung	Praktikum	Pf	3
2	10104	IT-Forensik	Vorlesung/Übung	Pf	3
2	10106	Sicherheitsmanagement	Vorlesung/Übung	Pf	3
2	10107	Sichere vernetzte Anwendungen	Vorlesung/Übung	Pf	3
2	10244	Praktikum Modellbildung und Simulation	Praktikum	WPf	4
2	10321	Quantitative Modelle	Vorlesung/Übung	Pf	5
2	10332	Entscheidungsunterstützende Modellbildung und Simulation	Vorlesung/Übung	WPf	3
2	11441	Knowledge Discovery	Vorlesung/Übung	WPf	3
2	11442	Methoden der Data Science	Vorlesung/Übung	WPf	3
2	11521	Computer Vision	Vorlesung/Übung	Pf	3
2	11523	Bildverarbeitung für Computer Vision	Vorlesung/Übung	Pf	3
2	12325	Praktikum Operations Research - Entscheidungsunterstützung II	Praktikum	WPf	3
2	12326	Seminar Ausgewählte Kapitel des Operations Research II	Seminar	WPf	3
2	12432	Informationsverarbeitung	Vorlesung/Übung	Pf	4
2	149014	Geschichte des Operations Research	Blockveranstaltung	WPf	3
2	15172	Methoden und Werkzeuge	Vorlesung/Übung	WPf	5
2	29942	Quantum Machine Learning & Optimization	Vorlesung/Übung	WPf	3
2	34911	Algorithmen und Komplexität	Vorlesung/Übung	WPf	5
2	38191	Reverse Engineering	Vorlesung	Pf	2
2	55031	Embedded Systems Security	Vorlesung/Übung	Pf	3
2	55042	Privacy Enhancing Technologies	Vorlesung/Übung	Pf	3
2	55051	Betriebssystemsicherheit	Vorlesung/Übung	Pf	3
2	55062	Kryptoanalyse	Vorlesung/Übung	Pf	3
2	55071	Language-based Security	Vorlesung	Pf	3
2	55131	Sichere mobile Systeme	Vorlesung/Übung	WPf	3
3	10122	Software-Entwicklungsumgebungen	Vorlesung/Übung	WPf	3
3	10322	Verlässliche Systeme	Vorlesung/Übung	WPf	3
3	10323	Zuverlässigkeitstheorie	Vorlesung/Übung	WPf	3
3	10334	Verifikation und Validierung von Modellen	Vorlesung/Übung	WPf	3
3	10471	IT-Governance	Vorlesung/Übung	Pf	5

3	11444	Big Data Management	Vorlesung/Übung	WPf	3
3	11522	Computer Vision und Graphik	Vorlesung/Übung	WPf	3
3	11972	Mobile Kommunikationssysteme	Vorlesung/Übung	Pf	3
3	12111	Algorithmische Zahlentheorie	Vorlesung/Übung	Pf	5
3	12201	Quellencodierung und Kanalcodierung	Vorlesung/Übung	WPf	5
3	12322	Aviation Management: Safety und Security	Vorlesung/Übung	WPf	3
3	12324	System Dynamics	Vorlesung/Übung	WPf	3
3	12531	Moderne Verfahren der Kanalcodierung und Decodierung	Vorlesung/Übung	Pf	3
3	12532	Übertragungssicherheit	Vorlesung/Übung	Pf	3
3	13811	Nachrichten- und Informationstheorie	Vorlesung/Übung	Pf	3
3	14901	Ausgewählte Kapitel des Operations Research und der Entscheidungstheorie	Vorlesung/Übung	Pf	3
3	14908	Soft Computing C: Natural Computing - Evolutionary Algorithms	Vorlesung/Übung	WPf	3
3	15511	Digitale Forensik (VL)	Vorlesung	Pf	3
3	15512	Digitale Forensik (UE)	Übung	Pf	3
3	24611	Ökonomie und Recht der Informationsgesellschaft	Vorlesung/Seminar	WPf	2
3	29941	Ausgewählte Kapitel des Data-driven Optimization	Vorlesung/Übung	Pf	3
3	29943	Seminar: Ausgewählte Kapitel des OR	Seminar	WPf	3
3	29944	Praktikum: Ausgewählte Kapitel des OR	Praktikum	WPf	3
3	3665-V1	Sichere Mensch-Maschine Schnittstellen	Vorlesung/Übung	Pf	3
3	38192	Reverse Engineering	Praktikum	Pf	4
3	3822 -V1	CNC Methoden	Vorlesung/Übung	Pf	3
3	3822 -V2	Praktikum CNC Methoden	Praktikum	Pf	3
3	3823-V1	Rechtliche Grundlagen CNC	Vorlesung	Pf	4
3	3823-V2	Rechtliche Grundlagen CNC (Übung)	Übung	Pf	2
3	38521	Sentiment Analysis	Vorlesung/Übung	WPf	3
3	38531	Analyse unstrukturierter Daten	Vorlesung/Übung	Pf	6
3	55091	Penetration Testing	Vorlesung/Übung	Pf	6
3	55141	Schutz von kritischen Infrastrukturen	Vorlesung/Übung	Pf	3
3	55144	Internationale Sicherheitsarchitekturen und Krisenmanagement im Cyberraum	Seminar	Pf	3
4	11621	Erweiterte Digitale Forensik (Vorlesung)	Vorlesung	Pf	3
4	11622	Erweiterte Digitale Forensik (Übung)	Übung	Pf	3
4	12112	Ausgewählte mathematische Methoden in Kryptographie und Codierungstheorie	Vorlesung/Übung	WPf	3
4	12113	Quantencomputer	Vorlesung/Übung	Pf	3
4	14461	Identitätsmanagement	Vorlesung/Übung	Pf	3
4	14462	Seminar Identitätsmanagement	Seminar	Pf	3
4	14905	Schwarmbasierte Verfahren	Vorlesung/Übung	WPf	3
4	15513	Seminar Ausgewählte Themen der digitalen Forensik	Seminar	Pf	3
4	3695-V1	Quantenkommunikation	Vorlesung/Übung	Pf	3
4	38381	Statische Programmanalyse	Vorlesung/Übung	Pf	4
4	38501	Natural Language Processing	Vorlesung/Übung	Pf	3
4	38502	Praktikum Natural Language Processing	Praktikum	Pf	3
4	38511	Information Retrieval	Vorlesung/Übung	Pf	6
4	38522	Social Media Mining	Vorlesung/Übung	WPf	3
4	38523	Semantische Technologien	Vorlesung/Übung	WPf	3

4	55041	Datenschutz	Vorlesung/Übung	Pf	3
5	3695-V2	Praktikum Quantenschlüsselaustausch	Praktikum	WPf	3
5	3695-V3	Seminar Quantentechnologien	Seminar	WPf	3
6	11901	Web Technologies	Vorlesung/Übung	Pf	3