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

Modulhandbuch des Studiengangs

Cyber - Sicherheit
(Master of Science)

an der
Universität der Bundeswehr München

(Version 2018)

Inhaltsverzeichnis

Modulname	Modulnummer
Netzsicherheit	5502

Konto	Plichtmodule - CYB 2018

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	Plichtmodule - CYB 2018

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	Plichtmodule - CYB 2018

Modulverantwortliche/r	Modultyp	Empf. Trimester
	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 zu Datenbanken, wie sie z.B. im Bachelor-Modul Einführung in die Praktische Informatik 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 wie Cloaking 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.

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

Dauer und Häufigkeit
Das Modul dauert 1 Trimester.

Modulname	Modulnummer
Systemsicherheit	5505

Konto	Plichtmodule - CYB 2018

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 die wesentlichen Mechanismen zur Umsetzung dieser Sicherheitsmaßnahmen im Betriebssystem

vorgestellt, typische Angriffe auf diese Mechanismen (z.B. Code Injection durch Buffer Overflow) und Gegenmaßnahmen (z.B. nicht ausführbarer Speicher). Dies wird ergänzt durch Maßnahmen zur Absicherung des Betriebssystems selbst (security kernels, secure boot, trusted computing). Im zweiten Teil der Veranstaltung werden spezielle Umgebungen für Betriebssysteme (z.B. mobile computing, cloud computing) und damit verbundene Sicherheitsaspekte betrachtet, sowie spezielle Mechanismen zur Isolation von Anwendungen (Container, virtuelle Maschinen) und zugehörige Angriffe und Schutzmaßnahmen.

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.

Leistungsnachweis
Schriftliche Prüfung mit 60 Minuten Dauer oder mündliche Prüfung mit 30 Minuten Dauer. Die Prüfungsform wird zu Beginn des Moduls festgelegt.
Dauer und Häufigkeit
Das Modul dauert 1 Trimester.

Modulname	Modulnummer
Kryptologie	5506

Konto	Plichtmodule - CYB 2018

Modulverantwortliche/r	Modultyp	Empf. Trimester
	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.

Ein thematischer Schwerpunkt der Vorlesung Kryptoanalyse sind lineare Codes, die mit algebraischen Methoden konstruiert werden und gute Eigenschaften haben. Hier wurde wieder einmal ein mathematisches Gebiet für Anwendungen produktiv, von dem man

es nicht gedacht hätte; auch wenn der vorliegende Fall nicht so spektakulär ist wie die Nutzbarmachung von Primzahlen, der Schwierigkeit der Faktorisierung, oder der Theorie der elliptischen Kurven für die Public Key-Kryptographie. In weiteren Schwerpunkt konzentrieren wir uns auf gute Faktorisierungs-Algorithmen (Hintergrund: Brechen des Kryptosystems RSA), einen "klassischen" (das quadratische Sieb) und einen aus dem Kontext des Quantencomputers (Algorithmus von Shor).
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	Plichtmodule - CYB 2018

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. 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	VÜ	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 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
Security- und IT- Management	5508

Konto	Plichtmodule - CYB 2018

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 2018

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. 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

- BSI IT-Grundschutz
- Grundlagen der angewandten Kryptographie
- Security Engineering
- Sicherheitsmodelle und -mechanismen und deren Umsetzung in verteilten Systemen und Rechnernetzen
- Sicherheit mobiler Endgeräte

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

- Security Incident Response mit Breach- und Malware-Analyse
- Social Engineering: Faktor Mensch in der Informationssicherheit aus Angreiferperspektive
- Identity & Access Management, Datenschutz und Privacy
- Sicherheit ausgelagerter Dienste (z.B. im Cloud Computing)

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.

Modulname	Modulnummer
Einführung in das Industrial Engineering	1008

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security

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

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
Integrierte Anwendungssysteme im Produkt Lifecycle Management	1168

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security

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

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
11681	VL	Integrierte Anwendungssysteme im Product Lifecycle Management	Pflicht	3
11682	UE	Integrierte Anwendungssysteme im Product Lifecycle Management	Pflicht	2
Summe (Pflicht und Wahlpflicht)				5

Qualifikationsziele

Das Modul bietet einen theoretisch fundierten und gleichzeitig praxisnahen Einblick in komplexe Einsatzfelder von Anwendungssystemen in produktzentrierten Wertschöpfungsketten. Die Teilnehmer erwerben die Fähigkeiten und Kenntnisse, die zur systematischen und modellbasierten Spezifikation, Entwicklung, Einführung und Anpassung integrierter Anwendungssysteme erforderlich sind. Dazu gehören das Grundverständnis der domänenspezifischen Anforderungen sowie allgemeine Grundlagen über Aufbau und Funktion der eingesetzten Standardsysteme. Den Überbau bilden die zu vermittelnden Kenntnisse und Fähigkeiten bezogen auf Modellbildung, Vorgehenssystematik, Referenzmodelle und Standards.

Inhalt

Im Modul Integrierte Anwendungssysteme im Product Lifecycle Management stehen industrielle, produktzentrierte Wertschöpfungsketten im Mittelpunkt der Betrachtung. Die rechnerbasierte Entwicklung und Verwaltung von komplexen Produkten und Systemen gehört bereits seit den Anfängen der Informatik zu deren wichtigsten Anwendungsfeldern. Wo der Rechner im Kontext des so genannten Computer Aided Design (CAD) ursprünglich das Zeichenbrett der Ingenieure ablöste und damit die Digitalisierung des kompletten Produktentwicklungsprozesses initiierte, gilt es heute mit Verfahren und Methoden der (Wirtschafts-) Informatik integrierte Anwendungssysteme zu konzipieren, zu entwickeln und an die sich permanent ändernden Randbedingungen von produzierenden Unternehmen anzupassen.
Das Aufgabenspektrum reicht dabei von der ersten Produktidee über die Gestaltung, die Produktion, den Vertrieb bis hinein in die Betriebs- und Wartungsphase der Produkte und Systeme - das so genannte Product Lifecycle Management (PLM). Die enorme Komplexität, die mit der Bereitstellung aller Daten und Dokumente in zunehmend

verteilten und unternehmensübergreifenden PLM-Prozessen verbunden ist, ist ohne entsprechend integrierte Anwendungssystemlandschaft nicht mehr beherrschbar.
Das Modul vermittelt hier den Studierenden einen fundierten Einblick in die Anwendungssysteme des Product Lifecycle Managements. Dabei erfolgt zunächst eine allgemeine Einführung in die Anforderungen und die entsprechenden PLM-Wertschöpfungsketten. Darauf aufsetzend wird dann im zweiten Teil die Architektur und Schnittstellenproblematik typischer verteilter PLM-Anwendungssysteme vertieft und an Praxisbeispielen verdeutlicht.
Abschließend wird die Thematik der systematischen, unternehmensspezifischen Spezifikation, Ersterstellung und Anpassung (Customizing) von am Markt verfügbaren PLM-Anwendungssystemen auf der Basis von Standards und Referenzmodellen verankert.
Einblicke in konkrete Fallbeispiele und Industrieprojekte runden das Modul ab.

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
Durch die Behandlung unternehmensbezogener Problemfelder und praxisorientierter Beispiele bereitet das Modul auf die industrielle Praxis vor.
Dauer und Häufigkeit
Das Modul dauert 1 Trimester. Das Modul beginnt jedes Studienjahr jeweils im Herbsttrimester

Modulname	Modulnummer
Data Mining und IT- basierte Entscheidungsunterstützung	1231

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security

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

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)				5

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

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Andreas Karcher	Wahlpflicht	4

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

Qualifikationsziele

Das Modul *Middleware und mobile Cloud Computing* zielt darauf ab, den Studierenden 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 tiefere theoretische Kenntnisse über Architektur, Aufbau und Anwendung aktueller Middlewarekonzepte. Im Übungsteil lernen die Teilnehmer parallel zur Vorlesung den praktischen Umgang mit Middleware-Technologien und Cloud-basierten, mobilen Anwendungen. 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.
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.
Leistungsnachweis
Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer.
Verwendbarkeit
Die im Modul erworbenen Kenntnisse sind elementar für die IT-technische Gestaltung von verteilten Informatik-Systemen und stellen somit eine Grundlage für Masterstudiengänge im Bereich Informatik/ Wirtschaftsinformatik/ Ingenieurinformatik dar.
Dauer und Häufigkeit
Das Modul dauert 1 Trimester. Das Modul beginnt jedes Studienjahr jeweils im Wintertrimester.

Modulname	Modulnummer
Enterprise Architecture und IT Service Management	1507

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Andreas Karcher	Wahlpflicht	1

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

Hilfreich aber nicht zwingend erforderlich sind Grundkenntnisse der Service-orientierten Architektur (SOA).

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 zunächst in die Lage versetzt, das noch relativ junge Forschungsgebiet in seinem aktuellen Stand und seiner Bedeutung für die Gestaltung komplexer IT-Landschaften einordnen zu können. In der Vertiefung werden heute dominierende Standards 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 Kenntnisse zur 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 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 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 Management* wird die an Praxisbeispielen gespiegelte Anwendung von Rahmenwerken im Mittelpunkt dieses Modulschwerpunktes stehen. Anwendungsexperten aus unterschiedlichen Bereichen werden zusätzlich tiefere Einblicke in den aktuellen Stand geben.

Leistungsnachweis

Schriftl. (60 min) oder mündl. (30 min) oder leistungsbezogener Notenschein. Die Art der Prüfung wird jeweils zu Beginn des Moduls bekannt gegeben.

Verwendbarkeit

Das Modul ist die Grundlage für weiterführende und vertiefende Veranstaltungen und wissenschaftliche Arbeiten im Kontext der Gestaltung und Anpassung komplexer IT-Landschaften.

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

Modulverantwortliche/r	Modultyp	Empf. Trimester
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
Compilerbau	3647

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security

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

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 vermittelt die notwendigen theoretischen Grundlagen um Programmiersprachen kompetent anhand typischer LL/LR Grammatiken zu spezifizieren. Die spezifizierten Grammatiken werden dann durch Werkzeuge automatisch in korrespondierende Lexer und Parser transformiert. Im Anschluss widmet sich die Vorlesung dem Thema der Codegenerierung, welche durch möglichst einfache Techniken illustriert wird.
Leistungsnachweis
Schriftliche Prüfung 60 Minuten
Dauer und Häufigkeit
Das Modul dauert 1 Trimester und beginnt jedes Jahr im HT.

Modulname	Modulnummer
Compilerbau (erweitert)	3648

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security

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

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 vermittelt die notwendigen theoretischen Grundlagen um Programmiersprachen kompetent anhand typischer LL/LR Grammatiken zu spezifizieren. Die spezifizierten Grammatiken werden dann durch Werkzeuge automatisch in korrespondierende Lexer und Parser transformiert. Im Anschluss widmet sich die Vorlesung dem Thema der Codegenerierung, welche durch möglichst einfache Techniken illustriert wird.
Leistungsnachweis
Schriftliche Prüfung 60 Minuten
Dauer und Häufigkeit
Das Modul dauert 2 Trimester und beginnt jedes Jahr im HT.

Modulname	Modulnummer
Benutzbare Sicherheit	3665

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security

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 und Privatsphäre	Pflicht	4
36652	SE	Seminar Empirische Forschungsmethoden in der IT-Sicherheit	Pflicht	2
36653	P	Praktikum Design sicherer und benutzbarer Systeme	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 die Grundlagen benutzbarer Sicherheit (Grundbegriffe, Sicherheitsmechanismen, Bedrohungsmodelle) vermittelt. Sie erarbeiten sich tiefgehende, methodische Kenntnisse, welche es ihnen ermöglichen, Konzepte und Systeme hinsichtlich Sicherheit und Benutzbarkeit zu evaluieren. Basierend auf dem theoretischen Grundlage- und Methodenwissen wird im praktischen Teil des Moduls die

Fähigkeit zur Konzeption und praktischen Umsetzung sicherer und benutzbarer Systeme erworben.

Inhalt

Technologie kann nicht die alleinige Lösung für Herausforderungen im Bereich IT-Sicherheit und Privatsphäre 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 Sicherheit. Daher ist es wichtig, dass Sicherheits- und Datenschutzexperten 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 den Datenschutz sicherer Systeme ein.

Dieses Modul vermittelt die theoretischen, methodischen und praktischen Grundlagen für das Design sicherer und benutzbarer Systeme. Hierfür dienen drei Lehrveranstaltungen:

Benutzbare Sicherheit und Privatsphäre – Diese Vorlesung gibt einen Überblick über Herausforderungen hinsichtlich Benutzbarkeit und User Interfaces sicherer und benutzbarer Systeme. Die Studierenden erhalten einen Überblick über Sicherheits-Mechanismen, mentale Modelle der Benutzer, eine Einführung in die Modellierung von Bedrohungen und einen Überblick über Forschungsmethoden. Die Lehrveranstaltung richtet sich sowohl an Studierende, die an Sicherheit und Datenschutz interessiert sind und mehr über Benutzbarkeit erfahren möchten, als auch an Studierende, die an Benutzbarkeit interessiert sind, aber mehr über Sicherheit und Datenschutz erfahren möchten.

Empirische Forschungsmethoden in der IT-Sicherheit – Die Evaluation und die Bewertung von sicheren und die Privatsphäre schützenden Systemen und Mechanismen ist unerlässlich, um ihre Stärken und Schwächen zu verstehen. Dies erfordert ein breites Wissen in der Forschungsmethodik. In diesem Seminar werden die Studierenden mit verschiedenen Studientypen (z.B. deskriptive Studien, relationale Studien, experimentelle Studien) und verschiedenen Studienparadigmen (u.a. Ethnographie, Laborstudien, Feldstudien, Deployments) vertraut gemacht. Ergänzt wird die Lehrveranstaltung durch einen Überblick über gängige Forschungsmethoden, wie Fragebögen, Interviews, Beobachtungen, Experience Sampling und Crowdsourcing. Die Studierenden arbeiten an ausgewählten Themen: Insbesondere werden sie eine detaillierte Einführung in eine der Methoden geben und ausgewählte Forschungsbeispiele vorstellen, welche diese Methoden anwenden. Stärken, Schwächen und Anwendungsbereiche der verschiedenen Methoden werden im Rahmen der Lehrveranstaltung diskutiert.

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 erhalten eine detaillierte Einführung in den benutzer-zentrierten Designprozess. In kleinen 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
Offensive Sicherheitsüberprüfungen	5509

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security

Modulverantwortliche/r	Modultyp	Empf. Trimester
	Wahlpflicht	4

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55091	VÜ	Penetration Testing	Pflicht	3
55092	VÜ	Social Engineering	Wahlpflicht	3
55093	P	Penetration Testing	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

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. Neben technischen Angriffsvarianten kennen die Studierenden Testverfahren, die den Faktor Mensch mit einbeziehen. Sie kennen die Phasen und Methoden von Security-Awareness-Kampagnen und können diese unter Priorisierung identifizierter Risiken für Organisationen konzipieren und durchführen.

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.

In der Vorlesung Social Engineering werden Social-Engineering-Angriffe mit und ohne Rechnerunterstützung vertieft. Nach einer Analyse typischer menschlicher Eigenschaften wie Hilfsbereitschaft oder Respekt vor Autorität, die von Angreifern als Schwächen ausgenutzt werden können, wird eine Reihe von passiven Angriffsvarianten (z.B. Dumpster Diving, Shoulder Surfing, Baiting) und aktiven Angriffswegen (z.B. Pretexting, Phishing) im Detail und auf Basis von Fallstudien analysiert. Zu allen Angriffsvarianten werden mögliche technische und organisatorische Gegenmaßnahmen mit ihren praktischen Grenzen betrachtet. Auf dieser Basis werden Methoden vermittelt, die zur Planung und Durchführung von Security-Awareness-Kampagnen eingesetzt werden können. Ebenso werden die Spezifika und ethischen Aspekte von Social-Engineering-Pentests 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

Schriftliche Prüfung mit 60 Minuten Dauer oder mündliche Prüfung mit 30 Minuten Dauer. 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 beiden Wahlpflichtveranstaltungen zu belegen.

Modulname	Modulnummer
Maschinennahe Softwareanalyse	5510

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security

Modulverantwortliche/r	Modultyp	Empf. Trimester
	Wahlpflicht	2

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55101	VÜ	Schwachstellenanalyse und -beseitigung	Pflicht	3
55102	VÜ	Software Reverse Engineering und Exploitentwicklung	Wahlpflicht	3
55103	P	Schwachstellenanalyse und Exploitentwicklung	Wahlpflicht	3
55104	VÜ	Statische und dynamische Code-Analyse	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

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

Qualifikationsziele

Die Studierenden kennen verschiedene Konzepte, Techniken und Werkzeuge aus dem Bereich der maschinennahen Softwareanalyse. Dies beinhaltet den Überblick über verschiedene Konzepte aus dem Bereich der Schwachstellenanalyse, der Funktionsweise aktueller Angriffsmethoden und Schutzmechanismen. Sie kennen verschiedene Techniken aus diesen Bereichen und können diese umsetzen. Je nach gewählten Wahlpflichtveranstaltungen haben die Studierenden ein vertieftes Verständnis von sowohl statischen als auch dynamischen Methoden zur Analyse eines gegebenen Programms, der Exploitentwicklung und des Reverse Engineering.

Inhalt

Im Rahmen der Vorlesung mit Übungen "Schwachstellenanalyse und -beseitigung" werden verschiedene Arten von Schwachstellen vorgestellt und Verfahren erläutert, um Schwachstellen und Verfahrensfehler in bestehenden Prozessen und Verfahrensabläufen mit dem Ziel zu identifizieren, die analysierten Prozesse oder Verfahren zu optimieren bzw. präventiv auf mögliche Fehlentwicklungen rechtzeitig einzuwirken. Dazu gehören Bestandsaufnahme der IT-Risiken, Vulnerability Scans, Sicherheitsüberprüfungen, Penetration Tests, Schadensanalysen sowie maßgeblichen Normen, z.B. IEC 62443.

Im Praktikum "Schwachstellenanalyse und Exploitentwicklung" werden verschiedene Arten von Schwachstellen vorgestellt und anhand realer Beispiele implementiert. Die zu analysierenden Schwachstellentypen werden jeweils besprochen und entsprechende Analyse- und Exploitingmethoden vorgestellt. In vielen Fällen wird darüber hinaus Eigenrecherche und Autodidaktik zur Lösung der Aufgaben notwendig sein. Unter anderem werden die folgenden Themen behandelt:

- Entwicklung eines eigenen Fuzzers
- Implementierung von Exploits
- Umgehung von Schutzmechanismen wie DEP und ASLR
- Reverse Engineering von proprietären Binärdateien

Die Vorlesung mit Übungen "Software Reverse Engineering und Exploitentwicklung" hat die Untersuchung unbekannter Software zum Thema, deren Funktionsweise analysiert werden soll, um z.B. Schwachstellen aufzudecken oder um das Verhalten von Malware zu analysieren. Unter "Software Reverse Engineering" versteht man dabei das Vorgehen, aus Binärcode die zugrundeliegenden Software-Anforderungen und Intentionen zurückzugewinnen. Dies setzt im Allgemeinen die Erstellung von äquivalenten Quell- oder Pseudocode voraus. Ferner werden die theoretischen und praktischen Grundlagen für die Funktionsweise und die Entwicklung von Explosivs vermittelt.

Im Rahmen der Vorlesung werden Konzepte, Techniken und Werkzeuge aus dem Bereich Software Reverse Engineering vorgestellt, z.B. statische und dynamische Methoden zur Analyse von Binärprogrammen, indem typische Werkzeuge wie Disassembler und Debugger zum Einsatz kommen. Es wird auch verdeutlicht, mit welchen Schwierigkeiten Software Reverse Engineering zu kämpfen hat und wo seine Grenzen liegen, z.B. im Bereich automatisierter Decompiler. Es werden Techniken angesprochen, um sich gegen Software Reverse Engineering zu schützen, z.B. Code-Verschleierung (Obfuscation) gegen statische Analyse und Anti-Debugging-Techniken gegen dynamische Analyse. Ferner wird vorgestellt, wie sich Schwachstellen in Binärprogrammen aufspüren lassen, wie sich diese trotz aktueller Schutzmechanismen ausnutzen lassen und welche Werkzeuge für die Explodiert-Entwicklung wichtig sind, z.B. Exploit-Frameworks etc.

In der Vorlesung "Statische und dynamische Code-Analyse" werden unter anderem die folgenden Themen und Techniken aus dem Bereich der Code-Analyse behandelt:

- Statische und dynamische Analyse von Programmen
- Analyse von Kontroll- und Datenfluss
- Symbolische Ausführung
- Taint Tracking
- Virtual Machine Introspection
- Binary Instrumentation
- Program Slicing
- Überblick zu existierenden Analysewerkzeugen

In den Übungen zur Vorlesung werden die vorgestellten Konzepte und Techniken praktisch angewandt.

Leistungsnachweis
Schriftliche Prüfung mit 60 Minuten Dauer oder mündliche Prüfung mit 30 Minuten Dauer. Die Prüfungsform wird zu Beginn des Moduls festgelegt.
Dauer und Häufigkeit
Das Modul dauert 1-2 Trimester.

Modulname	Modulnummer
Automatisierung in der Angriffserkennung	5511

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security

Modulverantwortliche/r	Modultyp	Empf. Trimester
	Wahlpflicht	4

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55111	VÜ	Autonome Sicherheitsmaßnahmen	Pflicht	3
55112	VÜ	Frühwarnsysteme	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen
Gute Kenntnisse im Bereich Netzsicherheit, wie im gleichnamigen Modul vermittelt.

Qualifikationsziele
Studierende kennen diejenigen technischen Teilbereiche der Angriffsdetektion und -bearbeitung, die beim aktuellen Stand der Technik einen hohen Grad an Automatisierung zulassen. Sie kennen ausgewählte Methoden u.a. für Security Self-Governance, Self-Organization und Self-Stabilization und können diese beispielsweise für verteilte Intrusion Detection Systeme umsetzen. Sie kennen Ansätze für Context-Aware Security und können deren Stärken und Risiken einschätzen. Studierende kennen Systemarchitekturen, Kommunikationsprotokolle und Sensorkonzepte für Frühwarnsysteme und wissen, wie deren Meldungen unter Berücksichtigung von Fehlerraten z.B. in Risikomanagement-, Security-Monitoring- und Krisenmanagement-Abläufe integriert werden können. Sie können die Zuverlässigkeit verschiedener Arten von Datenquellen für Frühwarnsysteme bewerten und anhand von Fallstudien evaluieren.

Inhalt
Die Vorlesung Autonome Sicherheitsmaßnahmen behandelt Algorithmen und Methoden, um Angriffserkennungsverfahren und Reaktionen auf erkannte Angriffe möglichst weitgehend zu automatisieren. Entsprechende Sicherheitsmechanismen kommen dort zum Einsatz, wo ein menschliches Eingreifen nicht möglich oder sinnvoll ist, beispielsweise weil sich die zu schützenden Systeme nicht in Kommunikationsreichweite befinden, die Operateure nicht für IT-Angriffe ausgebildet sind oder so viele Instanzen im Einsatz sind, dass eine manuelle Administration praktisch unmöglich wird. In der Vorlesung werden zunächst Methoden aus dem Bereich des netzbasierten Security-Monitoring behandelt, u.a. verteilte IDS-Systeme, Anomalie- und Malware-Detektion, kollaborative Sicherheitsmechanismen und Context-Aware Security. Darauf aufbauend werden autonome Sicherheitsmaßnahmen in anderen Domänen, insbesondere im Kontext ihrerseits autonomer Systeme, betrachtet.

Die Vorlesung Frühwarnsysteme behandelt die Auswertung dedizierter Sensoren und öffentlich zugänglicher Informationsquellen mit dem Ziel, Schadensereignisse so früh wie möglich zu erkennen und strukturiert darauf zu reagieren, insbesondere durch automatisierte gezielte Informationsverbreitung und die Unterstützung der Reaktionskoordination. Frühwarnsysteme werden in der Informationssicherheit klassisch im Bereich des Internet-Monitoring eingesetzt; weltweit verteilte Honeypot- und IDS-Architekturen tragen z.B. dazu bei, neue massenhaft eingesetzte Malware und DDoS-Angriffe zu erkennen und die erforderlichen Reaktionen darauf zu priorisieren. Zunehmend werden Datenquellen wie soziale Netzwerke aber auch ausgewertet, um klassische Informationskanäle für die Frühwarnung in anderen Domänen, beispielsweise dem Krisenmanagement bei Naturkatastrophen, Anschlägen und politischen Umstürzen, zu ergänzen. In der Vorlesung wird forschungsnah auf aktuelle Algorithmen und Werkzeuge zur Frühwarnung und deren Grenzen eingegangen.

Leistungsnachweis

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

Dauer und Häufigkeit

Das Modul dauert 1 Trimester.

Modulname	Modulnummer
Softwareanalyse und -härtung	5512

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security

Modulverantwortliche/r	Modultyp	Empf. Trimester
	Wahlpflicht	3

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55121	VÜ	Malware-Analyse	Pflicht	3
55122	VÜ	Operating System Hardening und System Intrusion Detection	Wahlpflicht	3
55123	VÜ	Seitenkanalangriffe gegen Software	Wahlpflicht	3
55124	P	IT-Forensik	Wahlpflicht	3
55125	P	Malware-Analyse	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Es werden grundlegende Kenntnisse in der maschinennahen Programmierung, zu Betriebssystemen und Rechnernetzen vorausgesetzt, wie sie beispielsweise in den gleichnamigen Bachelor-Veranstaltungen vermittelt werden.

Qualifikationsziele

Die Studierenden kennen verschiedene Konzepte, Techniken und Werkzeuge aus dem Bereich der Softwareanalyse mit dem Schwerpunkt auf Schadsoftware, verschiedenen Angriffsmöglichkeiten sowie der Verhinderung und Erkennung von Eindringversuchen. Die Studierenden entwickeln - in Abhängigkeit von der gewählten Wahlveranstaltung - folgende Fähigkeiten:

- Erkennen von Schadprogrammen
- Selbständige Durchführung von statischen und dynamischen Malware-Analysen
- Aufbau einer sicheren Umgebung für die Malware-Analyse (Sandbox)
- Sicherer Einsatz der Techniken und Tools der Malware-Analyse
- Erfassung, Analyse und Aufbereitung relevanter Daten im Rahmen der IT-Forensik
- Härtung von Betriebssystemen

Inhalt

In der Vorlesung "Malware-Analyse" wird ein tiefergehendes Verständnis von Aufbau und Funktionsweise von Malware, also Viren, Trojaner, Spyware, Spam etc. vermittelt, um Schadsoftware identifizieren zu können und um geeignete Schutzmechanismen zu entwerfen. Im Einzelnen werden die folgenden Themen behandelt:

- Malware-Arten und Ziele der Malware-Analyse
- Grundlagen des Reverse Engineering
- Statische Malware-Analyse (u.a. Anomalien in PE Headers und Metadaten, Integritätsprüfung mit Haching-Algorithmen, Prüfung digitaler Signaturen, Import-, Export- und Ressourcen-Analyse, Durchführung von Code-Analysen)
- Dynamische Malware-Analyse (u.a. Analyse der Prozess-Aktivität einschließlich Memory Dumps, API und Event Monitoring, Sandboxing, Debugging)
- Dynamische Analyse von Netzwerkdaten (u.a. Offline Traffic-Analyse, Netzwerk-Simulation)
- Script-Analyse

Im Praktikum "Malware-Analyse" werden die Kenntnisse aus der gleichnamigen Vorlesung praktisch umgesetzt und das Verhalten von Malware in einer sicheren Umgebung (Sand box) untersucht. Über Reverse Engineering wird versucht, den ursprünglichen Programmcode der Schadsoftware wiederherzustellen. Das Aufsetzen einer Sandbox-Umgebung und die zu untersuchende Malware werden jeweils besprochen und entsprechende Analysemethoden vorgestellt. In vielen Fällen wird darüber hinaus Eigenrecherche und Autodidaktik zur Lösung der Aufgaben notwendig sein.

In der Vorlesung mit Übungen "Operating System Hardening und System Intrusion Detection" werden Ansätze, Verfahren und Prozesse vorgestellt, um die Angriffsfläche eines Softwaresystems auf Seiten des Betriebssystems zu reduzieren. Zu den gängigen Härtungsmethoden gehören beispielsweise:

- Entfernung oder Deaktivierung von für den Betrieb nicht zwingend erforderlichen Softwarekomponenten und Diensten
- Mandatory Access Control und restriktive Zuweisung von Zugriffsrechten (z.B. Verwendung unprivilegierter Benutzerkonten zur Ausführung von Server-Prozessen)
- Durchsetzung straffer Systemrichtlinien
- Nutzung kryptographischer Verfahren
- Verwendung möglichst fehlerfreier Software ohne bekannte Verwundbarkeiten
- Zufällige Zuweisung von Adressbereichen im virtuellen Speicher für Programmbibliotheken (ASLR) und Programme (PIE)
- Verwendung von chroot für die Ausführung von Software
- Nutzung von Antivirus-Lösungen und Firewalls

Intrusion Detection Systems (IDS) erhöhen komplementär dazu die Sicherheit durch Erkennung von Eindringversuchen. Es werden u.a. die folgenden Verfahren vorgestellt und in den Übungen erprobt:

- Host-basierte IDS
- Netzwerk-basierte IDS
- Hybride IDS
- Honeypots

Unter Seitenkanalangriffen versteht man Angriffsmethoden, die sensitive Informationen (z.B. kryptographische Schlüssel) nicht durch einen direkten Angriff zu ermitteln versucht,

sondern indirekt durch Beobachtung der Hardware, um charakteristische Muster z.B. im Stromverbrauch, Prozessoraktivität oder anderen Parametern sowie Korrelationen zwischen den beobachteten Daten und den sensitiven Informationen zu finden. In der Vorlesung mit Übungen "Seitenkanalangriffe gegen Software" werden verschiedene Methoden für Seitenkanalangriffe vorgestellt, die sich gegen Softwaresysteme richten. Dazu gehören:

- Laufzeitangriffe (u.a. gegen RSA, AES)
- Cachebasierte Angriffe (u.a. gegen OpenSSL)
- Power Analysis (Simple und Differential Power Analysis)
- Template-Attacken

Daneben werden Methoden zum Schutz vor solchen Angriffen vorgestellt.

Im Praktikum "IT-Forensik" werden Verfahren zur Sammlung, Analyse und Aufbereitung digitaler Spuren in IT-Systemen vorgestellt und anhand konkreter Fallbeispiele praktisch erprobt. Ein Schwerpunkt liegt auf dem Bereich der Analyse von Dateisystemen; dazu kommen verschiedene Arten von Dateisystemen zur Anwendung. Es wird eingeübt, wie relevante Daten erfasst, analysiert und aufbereitet werden können. Darüber hinaus werden weitere Themen aus dem Bereich der digitalen Forensik behandelt (z.B. Browser- und Anwendungsforensik sowie Netzwerkforensik). In vielen Fällen wird darüber hinaus Eigenrecherche und Autodidaktik zur Lösung der Aufgaben notwendig sein.

Leistungsnachweis

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

Dauer und Häufigkeit

Das Modul dauert 1-3 Trimester.

Sonstige Bemerkungen

Neben der Pflichtveranstaltung "Malware-Analyse" muss eine weitere der genannten Veranstaltungen belegt werden.

Modulname	Modulnummer
Cryptography Engineering	5519

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Cornelius Greither	Wahlpflicht	4

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	Wahlpflicht	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.

Modulname	Modulnummer
Security Engineering	5520

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security

Modulverantwortliche/r	Modultyp	Empf. Trimester
	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	162	108	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55201	VÜ	Formale Methoden der Informationssicherheit	Wahlpflicht	3
55202	P	Sichere Softwareentwicklung	Wahlpflicht	3
55203	VÜ	User-Centric Security and Privacy-by-Design	Wahlpflicht	3
55204	VÜ	Schutz digitaler Identitäten	Wahlpflicht	3
55205	VÜ	Cloud Computing Security	Wahlpflicht	3
55206	P	Datenschutz und Privacy	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Es werden Kenntnisse in der Programmierung und im Software Engineering vorausgesetzt, wie sie u.a. in den Bachelor-Veranstaltungen "Einführung in die Informatik I und II", "Objektorientierte Programmierung" und "Einführung in Software Engineering" vermittelt werden.

Qualifikationsziele

Die Studierenden kennen verschiedene Konzepte, Techniken und Werkzeuge aus dem Bereich des systematischen Entwurfs und der Implementierung sicherer Systeme mit dem Schwerpunkt auf IT-Sicherheit. Die Studierenden vertiefen - in Abhängigkeit von den gewählten Wahlveranstaltungen - diese Kenntnisse im formalen Entwurf bzw. der Überprüfung von IT-Sicherheit, im Entwurf und der Implementierung sicherer Software und von Cloud-Systemen und/oder im Datenschutz sowie dem Schutz digitaler Identitäten.

Inhalt

Das zuverlässige Funktionieren komplexer Software-Systeme ist gerade für die Sicherheit von technischen Systemen besonders relevant. Bei modernen Industrieanlagen und im Verkehrsbereich drohen als Folge des Versagens Gefahren für Menschen und Umwelt. Bei der Kommunikation und Verwaltung von Daten sowie beim Zahlungsverkehr drohen, aufgrund fehlerhaften Verhaltens entsprechender informationstechnischer Systeme (IT-Systeme), Bruch der Vertraulichkeit, Verlust oder Verfälschung von Daten und, in fast

allen Fällen, erhebliche wirtschaftliche Nachteile. Letztere entstehen nicht nur aus den Schäden, die durch schlecht konzipierte bzw. fehlerhaft realisierte Systeme verursacht werden, sondern auch durch den zusätzlichen Aufwand für die Behebung von Mängeln. Daher wurden national und international verbindliche Kriterien und Standards für die Beurteilung der Betriebssicherheit (Safety) und der Informationssicherheit (Security) von informationsverarbeitenden Systemen definiert. Bei der Beurteilung der Korrektheit eines Systems nach diesen Kriterien kommt dem Entwicklungsprozess eine zentrale Rolle zu. In unterschiedlicher Ausprägung erfordern die hohen Evaluationsstufen dieser Kriterien den Einsatz formaler Methoden zur Erstellung mathematisch nachweisbar korrekter IT-Systeme. In der Vorlesung "Formale Methoden der Informationssicherheit" werden u.a. die folgenden Ansätze besprochen:

- formale Modellierung von sicherheitskritischen Systemen,
- formale Spezifikation von Sicherheitsanforderungen
- mathematisch fundierte Sicherheitsanalysen
- theoretische Grundlagen der schrittweisen Softwareentwicklung.

Unter anderem werden folgende Themen behandelt und in den Übungen eingeübt:

- Grundlagen von formalen Methoden für IT-Sicherheit
- Erstellung und Prüfung formaler Sicherheitsmodelle im Rahmen von ITSEC/CC
- Mechanismen und formale Modelle der Zugriffskontrolle
- Ansätze zur Informationsflusskontrolle
- formale Modellierung und Analyse von Sicherheitsprotokollen
- Modellierung von Vertrauensbeziehungen in verteilten Systemen

Im Praktikum "Sichere Softwareentwicklung" befassen sich die Studierenden mit grundlegenden Angriffsvektoren von Hackern, Crackern und Schadsoftware-Autoren. Am Beispiel unsicherer Programmierung ("Buffer- und Integer-Overflows", "Script Injection", "Cross-Site-Scripting" etc.) wird die Verwundbarkeit von Software demonstriert und an praktischen Beispielen verdeutlicht. In Einzelprojekten werden die Prinzipien des sicheren Software-Entwurfs und der sichereren Programmierung praktisch erprobt. Dabei werden der "Security Development Cycle" von Microsoft und Methoden eingesetzt, die die Güte solcher Prozesse zu messen und zu verbessern gestatten. In vielen Fällen wird Eigenrecherche und Autodidaktik zur Lösung der Aufgaben notwendig sein.

Inzwischen gibt es eine Vielzahl fortschrittlicher Security-Techniken und -Methoden, um Daten, Systeme und Netzwerke abzusichern. Allerdings setzen sie meist ein tiefes Systemverständnis und detaillierte Kenntnisse voraus, über die durchschnittliche Nutzer aber im Allgemeinen nicht verfügen. Die Vorlesung mit Übungen "User-Centric Security and Privacy-by-Design" erörtert dieses Problem und stellt Ansätze und Lösungen vor, die Benutzerfreundlichkeit von Security-Techniken und -Methoden zu steigern und so häufige Nutzerfehler zu vermeiden. Im Rahmen der Vorlesung werden u.a. die folgenden Themen behandelt und in den Übungen eingeübt:

- Privacy-by-Default und Privacy-by-Design (Grundeinstellungen müssen datenschutzfreundlich sein)
- Richtlinien für User-Centric Security
- Analyse praktischer Beispiele hinsichtlich User-Centric Security

Die Vorlesung mit Übungen "Schutz digitaler Identitäten" behandelt das Problem, dass digitale Identitäten vermehrt für Betrugsdelikte missbraucht werden und der Identitätsdiebstahl zu den häufigsten Bedrohungen im Internet zählt. Aufgrund der steigenden Zahl von Transaktionen und der gleichzeitig steigenden Komplexität der digitalen Vorgänge, die mit digitalen Identitäten verknüpft sind, den steigenden Erwartungen und Anforderungen der Nutzer an digitale Identitäten sowie wachsenden gesetzlichen und vertraglichen Anforderungen wird der Schutz digitaler Identitäten immer wichtiger. Im Rahmen der Vorlesung und der Übungen werden grundlegende und fortgeschrittene Techniken zum Schutz digitaler Identitäten vorgestellt, u.a. die folgenden Themen:

- Schutz durch und für biometrische Daten
- Identity-Protection-Ansätze (z.B. mobile Endgeräte als Security-Tokens, Vereinheitlichung digitaler Identitäten, behavioral biometrics)
- Identity and Access Management (IAM) und "IAM as a Service" (IAMaaS)

Unter Cloud Computing versteht man die Bereitstellung von IT-Infrastruktur wie beispielsweise Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung über das Internet. Die Vorlesung mit Übungen "Cloud Computing Security" setzt sich mit Security-Risiken im Umfeld von Cloud Computing auseinander, u.a.:

- Verletzung der Vertraulichkeit und Integrität der Daten
- Löschung von Daten (z.B. aufgrund gesetzlicher Regelungen)
- Ungenügende Mandantentrennung
- Verletzung der Compliance
- Verletzung von Datenschutzgesetzen

In der Vorlesung werden dazu u.a. die folgenden Lösungen und Gegenmaßnahmen vorgestellt und in den Übungen an praktischen Beispielen eingeübt:

- Kontrollmechanismen für Cloud Computing Security (abschreckende, präventive, erkennende und korrigierende)
- Identitätsmanagement
- Datenschutz
- Zugriffskontrolle
- Schutz gegen Seitenkanalangriffe
- Verschlüsselung (u.a. homomorphe Verschlüsselung)

Datenschutz ist angesichts technologischer Entwicklungen, informationeller Globalisierung und eines komplexen rechtlichen Rahmens ein zentraler Compliance-Aspekt und betrifft Unternehmen ebenso wie die öffentliche Verwaltung sowie die Bundeswehr. Der inhaltliche Fokus des Praktikums "Datenschutz und Privacy" liegt auf der EU-Datenschutz-Grundverordnung und dem nationalen Datenschutzrecht. Ergänzend werden komplementäre Rechtsbereiche mit relevanten Querbezügen (u.a. Arbeitsrecht, Persönlichkeitsschutz und Telekommunikationsrecht) behandelt. In praktischen Übungen werden technischen Aspekte der Datensicherheit sowie zum Datenschutzmanagement umgesetzt. In vielen Fällen wird Eigenrecherche und Autodidaktik zur Lösung der Aufgaben notwendig sein.

Leistungsnachweis
Notenschein, der sich aus Teilprüfungen der belegten Veranstaltungen zusammensetzt.
Dauer und Häufigkeit
Das Modul dauert 1-2 Trimester.
Sonstige Bemerkungen
Es müssen drei der genannten Veranstaltungen belegt werden.

Modulname	Modulnummer
Human Factors in Cyber Security	5522

Konto	Wahlpflicht Vertiefungsfeld Enterprise Security

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr.-Ing. Verena Nitsch	Wahlpflicht	3

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55221	VÜ	Risikomanagement und Fehlerprävention	Wahlpflicht	3
55222	VÜ	Cyberpsychologie	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Es sind keine besonderen Vorkenntnisse notwendig.

Qualifikationsziele

Die Studierenden lernen Mechanismen der menschlichen Informationsverarbeitung und Handlungsmotivation kennen. Sie können Methoden des Risikomanagements und der Human Error Analyse fachgerecht einsetzen sowie systematisch Maßnahmen zur Erhöhung der Handlungssicherheit entwickeln und in Unternehmen einführen. Weiterhin sind die Studierenden vertraut mit den psychologischen Grundlagen der Cyberkriminalität und in der Lage, diese in der Entwicklung gezielter Gegenmaßnahmen zu berücksichtigen.

Inhalt

Der Mensch kann sowohl eine Sicherheitslücke als auch eine wirksame Barriere gegen Cyberattacken darstellen. In den Lehrveranstaltungen Risikomanagement und Fehlerprävention sowie Cyberpsychologie wird der Faktor Mensch in der Cybersicherheit näher beleuchtet. Die beiden Veranstaltungen behandeln entsprechend cybersicherheitsrelevante Aspekte des Risikomanagements sowie der angewandten Psychologie.

In der Veranstaltung Risikomanagement und Fehlerprävention werden u.a. wahrnehmungs-, sozial- und organisationspsychologische Prozesse auf der Ebene des Individuums (z.B. Attributionsfehler), sowie der Gruppe (z.B. Gruppendenken) und der Organisation (z.B. Sicherheitskultur) beleuchtet, die Fehlerentstehung fördern und die Wirksamkeit von technischen Schutzmaßnahmen in Unternehmen einschränken. Etablierte Methoden der Risiko- bzw. Fehleranalyse (FMEA, SWOT, bzw. RCA, HFACS) werden behandelt und mittels Fallstudien vertieft. Fehlerpräventionsmaßnahmen, die

speziell die Risikowahrnehmung und –einschätzung betreffen, wie Security Awareness Training und Verhaltensmodifikationen, werden diskutiert.

Cyberkriminelle nutzen nicht nur technische, sondern vor allem auch menschliche Schwächen aus. Die Veranstaltung Cyberpsychologie bietet dementsprechend einen Überblick über relevante psychologische Aspekte der Cyberkriminalität. Techniken des Social Engineering werden vorgestellt und diskutiert mit einem Fokus auf zugrundeliegenden psychologischen Mechanismen, u.a. Hilfsbereitschaft, Zugehörigkeitsgefühl, Disinhibition, Technikvertrauen und digitale Kompetenz. Handlungsmotivationen und Verhaltensmuster von Cyberkriminellen, sowie situationale Einflüsse auf cyberkriminelles Verhalten werden näher beleuchtet.

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

Modulname	Modulnummer
Einführung in das Industrial Engineering	1008

Konto	Wahlpflicht Vertiefungsfeld Public Security

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

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)				8

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, die Studierenden mit speziellen Techniken der Modellentwicklung und rechnergestützter Simulation vertraut zu machen. Insbesondere sollen sie Studierenden dabei lernen, wie Qualität, Zuverlässigkeit und Leistungsfähigkeit komplexer Simulationsmodelle durch Auswahl entsprechender Entwurfs- und Testmethoden gewährleistet werden können.

Inhalt

In den Lehrveranstaltungen dieses Moduls wird der Einsatz von Modellierungsmethoden und Techniken rechnergestützter Simulation unter besonderen Randbedingungen bzw. für spezielle Verwendungszwecke behandelt. Dabei handelt es sich einmal um:

- Maßnahmen zur Sicherstellung der Gültigkeit und Qualität von Modellen und deren Ergebnissen hinsichtlich eines bestimmten Verwendungszwecks (Verifikation und Validierung von Modellen),
- um Techniken zur Kopplung von Modellkomponenten oder Modellen, sowie deren verteilte oder parallele Ausführung auf mehreren Prozessoren oder Rechnern aus Gründen der Erhöhung der Leistungsfähigkeit oder auch der Zuverlässigkeit (Parallele und verteilte Simulation),

- Vorgehensweisen und Methoden zum Einsatz von Simulation als ein Hilfsmittel zu Entscheidungsfindungen, welche meist unter Realzeit-bedingungen zu erfolgen haben und zu verlässlichen Ergebnissen führen müssen.

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 dem Gebiet der Modellbildung und Simulation. Da außerdem in nahezu allen Disziplinen zunehmend rechnergestützte Simulation als Hilfsmittel für Analysen und bewertende Untersuchungen eingesetzt wird, erleichtert es den Studierenden bei Auswahl dieses Moduls Einschätzung des Potentials von Simulation und deren Anwendungen in vielen Fachgebieten.
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.

Modulname	Modulnummer
Operations Research	1036

Konto	Wahlpflicht Vertiefungsfeld Public Security

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Stefan Pickl	Pflicht	5

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10361	VL	Operations Research	Pflicht	3
10362	UE	Operations Research	Pflicht	2
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen
Kenntnisse in Analysis und Linearer Algebra, wie sie beispielsweise in den Modulen Analysis und Lineare Algebra vermittelt werden.

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 zughörige Probleme zu identifizieren und mit geeigneten Modellen und Lösungsverfahren zu behandeln. Es ist das Ziel des Moduls, dass die Studierenden sicher mit den Standardverfahren des Operations Research umgehen können. Im Rahmen des heutigen unterstützenden Rechnereinsatzes sollen sie in der Lage sein, zukünftige Potentiale zu erkennen und damit verbundene Komplexitätsaspekte kompetent zu behandeln.

Inhalt
Die Veranstaltung führt in das weite fachliche Gebiet des Operations Research ein. Der quantitativen Beschreibung und Lösung von komplexen Entscheidungsproblemen 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). 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. Eine inhaltliche Auswahl besteht aus folgenden Elementen: Einführung in die Problemstellung und Lösungsmethoden der allgemeinen Unternehmensforschung, 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.

Leistungsnachweis
Schriftliche Prüfung von 60 Minuten Dauer.
Dauer und Häufigkeit
Das Modul dauert 1 Trimester.Das Modul beginnt jedes Studienjahr im Wintertrimester.

Modulname	Modulnummer
Formale Entwicklung korrekter Software	1166

Konto	Wahlpflicht Vertiefungsfeld Public Security

Modulverantwortliche/r	Modultyp	Empf. Trimester
	Wahlpflicht	0

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
360	120	240	12

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
11661	VÜ	Entwurf Verteilter Systeme	Wahlpflicht	5
11662	VÜ	Methoden und Werkzeuge	Wahlpflicht	5
11663	VÜ	Modulprojekt	Wahlpflicht	4
11664	VÜ	Spezifikation	Wahlpflicht	5
Summe (Pflicht und Wahlpflicht)				10

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.
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 6 ECTS zu jeder der Vorlesungen (mit Übung) und im Modulprojekt. Die Studenten können (je nach Angebot) entweder zwei Vorlesungen mit Übungen oder eine Vorlesung mit Übungen und ein Modulprojekt einbringen - was insgesamt die 12 ECTS des Moduls ergibt.

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

Modulname	Modulnummer
Web Technologies	1306

Konto	Wahlpflicht Vertiefungsfeld Public Security

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)				5

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

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

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Andreas Karcher	Wahlpflicht	4

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

Qualifikationsziele

Das Modul *Middleware und mobile Cloud Computing* zielt darauf ab, den Studierenden 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 tiefere theoretische Kenntnisse über Architektur, Aufbau und Anwendung aktueller Middlewarekonzepte. Im Übungsteil lernen die Teilnehmer parallel zur Vorlesung den praktischen Umgang mit Middleware-Technologien und Cloud-basierten, mobilen Anwendungen. 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.
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.
Leistungsnachweis
Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer.
Verwendbarkeit
Die im Modul erworbenen Kenntnisse sind elementar für die IT-technische Gestaltung von verteilten Informatik-Systemen und stellen somit eine Grundlage für Masterstudiengänge im Bereich Informatik/ Wirtschaftsinformatik/ Ingenieurinformatik dar.
Dauer und Häufigkeit
Das Modul dauert 1 Trimester. Das Modul beginnt jedes Studienjahr jeweils im Wintertrimester.

Modulname	Modulnummer
Ökonomie und Recht der Informationsgesellschaft	2461

Konto	Wahlpflicht Vertiefungsfeld Public Security

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.

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.

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.

Verwendbarkeit

Das Modul kann als eines der zwei Wahlpflichtmodule der Vertiefung "Management marktorientierter Wertschöpfungsketten" oder als eines der drei Wahlpflichtmodule "Ökonomie und Recht der globalen Wirtschaft" oder als eines der sechs Interessensfelder belegt werden. Bei Belegung im Rahmen der Vertiefung „Management marktorientierter Wertschöpfungsketten" bildet diese Modul zusammen mit dem Modul "Innovation und dynamischer Wettbewerb" oder dem Modul Information, Organisation und Management die Spezialisierung "Märkte für Informationen und Wissen". Es vertieft und verbreitert die Kenntnisse aus den Pflichtmodulen und liefert so die Voraussetzung für das Seminarmodul der Vertiefung oder eine Masterarbeit im Themenfeld. Bei Belegung im Rahmen der Vertiefung „Ökonomie und Recht der globalen Wirtschaft“ vertieft und verbreitert dieses Modul zusammen mit den beiden anderen Wahlpflichtmodule die Kenntnisse aus den Pflichtmodulen und liefert damit die Voraussetzung für das Seminarmodul oder eine Masterarbeit im Themenfeld globale Wirtschaft.

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
Benutzbare Sicherheit	3665

Konto	Wahlpflicht Vertiefungsfeld Public Security

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 und Privatsphäre	Pflicht	4
36652	SE	Seminar Empirische Forschungsmethoden in der IT-Sicherheit	Pflicht	2
36653	P	Praktikum Design sicherer und benutzbarer Systeme	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 die Grundlagen benutzbarer Sicherheit (Grundbegriffe, Sicherheitsmechanismen, Bedrohungsmodelle) vermittelt. Sie erarbeiten sich tiefgehende, methodische Kenntnisse, welche es ihnen ermöglichen, Konzepte und Systeme hinsichtlich Sicherheit und Benutzbarkeit zu evaluieren. Basierend auf dem theoretischen Grundlage- und Methodenwissen wird im praktischen Teil des Moduls die

Fähigkeit zur Konzeption und praktischen Umsetzung sicherer und benutzbarer Systeme erworben.

Inhalt

Technologie kann nicht die alleinige Lösung für Herausforderungen im Bereich IT-Sicherheit und Privatsphäre 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 Sicherheit. Daher ist es wichtig, dass Sicherheits- und Datenschutzexperten 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 den Datenschutz sicherer Systeme ein.

Dieses Modul vermittelt die theoretischen, methodischen und praktischen Grundlagen für das Design sicherer und benutzbarer Systeme. Hierfür dienen drei Lehrveranstaltungen:

Benutzbare Sicherheit und Privatsphäre – Diese Vorlesung gibt einen Überblick über Herausforderungen hinsichtlich Benutzbarkeit und User Interfaces sicherer und benutzbarer Systeme. Die Studierenden erhalten einen Überblick über Sicherheits-Mechanismen, mentale Modelle der Benutzer, eine Einführung in die Modellierung von Bedrohungen und einen Überblick über Forschungsmethoden. Die Lehrveranstaltung richtet sich sowohl an Studierende, die an Sicherheit und Datenschutz interessiert sind und mehr über Benutzbarkeit erfahren möchten, als auch an Studierende, die an Benutzbarkeit interessiert sind, aber mehr über Sicherheit und Datenschutz erfahren möchten.

Empirische Forschungsmethoden in der IT-Sicherheit – Die Evaluation und die Bewertung von sicheren und die Privatsphäre schützenden Systemen und Mechanismen ist unerlässlich, um ihre Stärken und Schwächen zu verstehen. Dies erfordert ein breites Wissen in der Forschungsmethodik. In diesem Seminar werden die Studierenden mit verschiedenen Studientypen (z.B. deskriptive Studien, relationale Studien, experimentelle Studien) und verschiedenen Studienparadigmen (u.a. Ethnographie, Laborstudien, Feldstudien, Deployments) vertraut gemacht. Ergänzt wird die Lehrveranstaltung durch einen Überblick über gängige Forschungsmethoden, wie Fragebögen, Interviews, Beobachtungen, Experience Sampling und Crowdsourcing. Die Studierenden arbeiten an ausgewählten Themen: Insbesondere werden sie eine detaillierte Einführung in eine der Methoden geben und ausgewählte Forschungsbeispiele vorstellen, welche diese Methoden anwenden. Stärken, Schwächen und Anwendungsbereiche der verschiedenen Methoden werden im Rahmen der Lehrveranstaltung diskutiert.

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 erhalten eine detaillierte Einführung in den benutzer-zentrierten Designprozess. In kleinen 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
Mobile Security	5513

Konto	Wahlpflicht Vertiefungsfeld Public Security

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).

Aufbauend auf diesen Grundlagen behandelt die Veranstaltung Sichere mobile Systeme spezifische Sicherheitsaspekte von mobilen Kommunikationssystemen: Modellierung der Bedrohungen, Vorstellung und Klassifizierung von Angriffen und Sicherheitsmechanismen. Speziell werden die Sicherheitsmechanismen in den Protokollen der mobilen Kommunikationssysteme vorgestellt und ein Übergang zwischen mobiler und nicht-mobiler Infrastruktur geschaffen (z.B. für WLAN: WEP, WPA, 802.1x, 802.11i). Ein weiteres Thema ist die Absicherung mobiler Betriebssysteme im Rahmen von drahtlosen Sensornetzen.

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

Modulname	Modulnummer
Staatliche IT-Sicherheit	5514

Konto	Wahlpflicht Vertiefungsfeld Public Security

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

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
55142	VÜ	IT-Security in der zivilen Sicherheit	Wahlpflicht	3
55143	VÜ	Security- und Krisenmanagement im internationalen Kontext	Wahlpflicht	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.
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.

Modulname	Modulnummer
Rechtliche und ethische Aspekte der IT-Sicherheit	5515

Konto	Wahlpflicht Vertiefungsfeld Public Security

Modulverantwortliche/r	Modultyp	Empf. Trimester
	Wahlpflicht	3

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
11651	VL	Rechtsfragen der Informatik	Pflicht	2
55151	VÜ	Ethical Hacking and Defense	Wahlpflicht	2
55152	VÜ	Kriminalpsychologie	Wahlpflicht	2
55153	VÜ	Gesellschaftliche Implikationen der Informationssicherheit	Wahlpflicht	2
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 Grundzüge von Privatrecht, öffentlichem Recht und Strafrecht, und können diese Rahmenbedingungen in das Gefüge von Compliance und Corporate Governance einordnen;
- Studierende kennen IT-Recht mit Anwendungsbeispielen im Recht der Kritischen Infrastrukturen, IT-Vertragsrecht, zivilen Haftungsrecht, Datensicherheitsrecht, Patentrecht, Urheberrechtsschutz, gewerblichem Rechtsschutz, zu völkerrechtlichen Aspekten der IT-Sicherheit und im Cyber-Strafrecht;
- Studierende kennen Grundzüge der Ethik mit Bezug zu Maschinenethik und ethischen Fragestellungen in der Informatik und in internationaler Beziehungen;
- Studierende kennen wichtige Grundzüge von Rechtspsychologie und forensischer Psychologie, Methoden der Analyse, sowie Theorien und Fallbeispiele mit besonderem Bezug zu IT-Sicherheitsvorfällen;
- Studierende kennen wesentliche Themen und Methoden der soziologischen Theorie und der Politischen Theorie, insbesondere Methoden und Fallbeispiele der Risikoanalyse und Technikfolgenabschätzung sowie der Zukunftsanalyse und Methoden des öffentlichen Diskurses.

Inhalt

Die gesellschaftliche Dimension der IT-Sicherheit ist Thema des Moduls „Rechtliche und Ethische Aspekte der IT-Sicherheit“. Ist die Gesellschaft bereit für Themen und Technologien der IT-Sicherheit? Wer haftet bei IT-Sicherheitsvorfällen oder für autonome

IT-Systeme? Dies sind Beispiele für Fragestellungen, die in diesem Modul betrachtet werden. IT-Sicherheit soll die Gesellschaft schützen und deshalb sollen Studierende die rechtlichen und ethischen Themen der IT-Sicherheit kennen. Studierende setzen sich mit den rechtlichen, normativen Fragestellungen auseinander, kennen Modelle und Theorien aus der Rechtspsychologie nicht nur, um IT-Sicherheitsvorfälle analysieren zu können, sondern auch, um IT-Sicherheitstechnologie für Menschen entwickeln zu können und können die Gestaltung von neuen Technologien aus ethischer Sicht beurteilen.

Das Modul behandelt Grundzüge des Rechts, der Kriminalpsychologie, sowie von Ethik, Politikwissenschaften und Soziologie und verschiedene Fälle aus dem Themenfeld der Cyber-Sicherheit.

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.

Modulname	Modulnummer
Security Engineering	5520

Konto	Wahlpflicht Vertiefungsfeld Public Security

Modulverantwortliche/r	Modultyp	Empf. Trimester
	Wahlpflicht	3

Workload in (h)	Präsenzzeit in (h)	Selbststudium in (h)	ECTS-Punkte
180	162	108	9

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55201	VÜ	Formale Methoden der Informationssicherheit	Wahlpflicht	3
55202	P	Sichere Softwareentwicklung	Wahlpflicht	3
55203	VÜ	User-Centric Security and Privacy-by-Design	Wahlpflicht	3
55204	VÜ	Schutz digitaler Identitäten	Wahlpflicht	3
55205	VÜ	Cloud Computing Security	Wahlpflicht	3
55206	P	Datenschutz und Privacy	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				9

Empfohlene Voraussetzungen

Es werden Kenntnisse in der Programmierung und im Software Engineering vorausgesetzt, wie sie u.a. in den Bachelor-Veranstaltungen "Einführung in die Informatik I und II", "Objektorientierte Programmierung" und "Einführung in Software Engineering" vermittelt werden.

Qualifikationsziele

Die Studierenden kennen verschiedene Konzepte, Techniken und Werkzeuge aus dem Bereich des systematischen Entwurfs und der Implementierung sicherer Systeme mit dem Schwerpunkt auf IT-Sicherheit. Die Studierenden vertiefen - in Abhängigkeit von den gewählten Wahlveranstaltungen - diese Kenntnisse im formalen Entwurf bzw. der Überprüfung von IT-Sicherheit, im Entwurf und der Implementierung sicherer Software und von Cloud-Systemen und/oder im Datenschutz sowie dem Schutz digitaler Identitäten.

Inhalt

Das zuverlässige Funktionieren komplexer Software-Systeme ist gerade für die Sicherheit von technischen Systemen besonders relevant. Bei modernen Industrieanlagen und im Verkehrsbereich drohen als Folge des Versagens Gefahren für Menschen und Umwelt. Bei der Kommunikation und Verwaltung von Daten sowie beim Zahlungsverkehr drohen, aufgrund fehlerhaften Verhaltens entsprechender informationstechnischer Systeme (IT-Systeme), Bruch der Vertraulichkeit, Verlust oder Verfälschung von Daten und, in fast

allen Fällen, erhebliche wirtschaftliche Nachteile. Letztere entstehen nicht nur aus den Schäden, die durch schlecht konzipierte bzw. fehlerhaft realisierte Systeme verursacht werden, sondern auch durch den zusätzlichen Aufwand für die Behebung von Mängeln. Daher wurden national und international verbindliche Kriterien und Standards für die Beurteilung der Betriebssicherheit (Safety) und der Informationssicherheit (Security) von informationsverarbeitenden Systemen definiert. Bei der Beurteilung der Korrektheit eines Systems nach diesen Kriterien kommt dem Entwicklungsprozess eine zentrale Rolle zu. In unterschiedlicher Ausprägung erfordern die hohen Evaluationsstufen dieser Kriterien den Einsatz formaler Methoden zur Erstellung mathematisch nachweisbar korrekter IT-Systeme. In der Vorlesung "Formale Methoden der Informationssicherheit" werden u.a. die folgenden Ansätze besprochen:

- formale Modellierung von sicherheitskritischen Systemen,
- formale Spezifikation von Sicherheitsanforderungen
- mathematisch fundierte Sicherheitsanalysen
- theoretische Grundlagen der schrittweisen Softwareentwicklung.

Unter anderem werden folgende Themen behandelt und in den Übungen eingeübt:

- Grundlagen von formalen Methoden für IT-Sicherheit
- Erstellung und Prüfung formaler Sicherheitsmodelle im Rahmen von ITSEC/CC
- Mechanismen und formale Modelle der Zugriffskontrolle
- Ansätze zur Informationsflusskontrolle
- formale Modellierung und Analyse von Sicherheitsprotokollen
- Modellierung von Vertrauensbeziehungen in verteilten Systemen

Im Praktikum "Sichere Softwareentwicklung" befassen sich die Studierenden mit grundlegenden Angriffsvektoren von Hackern, Crackern und Schadsoftware-Autoren. Am Beispiel unsicherer Programmierung ("Buffer- und Integer-Overflows", "Script Injection", "Cross-Site-Scripting" etc.) wird die Verwundbarkeit von Software demonstriert und an praktischen Beispielen verdeutlicht. In Einzelprojekten werden die Prinzipien des sicheren Software-Entwurfs und der sichereren Programmierung praktisch erprobt. Dabei werden der "Security Development Cycle" von Microsoft und Methoden eingesetzt, die die Güte solcher Prozesse zu messen und zu verbessern gestatten. In vielen Fällen wird Eigenrecherche und Autodidaktik zur Lösung der Aufgaben notwendig sein.

Inzwischen gibt es eine Vielzahl fortschrittlicher Security-Techniken und -Methoden, um Daten, Systeme und Netzwerke abzusichern. Allerdings setzen sie meist ein tiefes Systemverständnis und detaillierte Kenntnisse voraus, über die durchschnittliche Nutzer aber im Allgemeinen nicht verfügen. Die Vorlesung mit Übungen "User-Centric Security and Privacy-by-Design" erörtert dieses Problem und stellt Ansätze und Lösungen vor, die Benutzerfreundlichkeit von Security-Techniken und -Methoden zu steigern und so häufige Nutzerfehler zu vermeiden. Im Rahmen der Vorlesung werden u.a. die folgenden Themen behandelt und in den Übungen eingeübt:

- Privacy-by-Default und Privacy-by-Design (Grundeinstellungen müssen datenschutzfreundlich sein)
- Richtlinien für User-Centric Security
- Analyse praktischer Beispiele hinsichtlich User-Centric Security

Die Vorlesung mit Übungen "Schutz digitaler Identitäten" behandelt das Problem, dass digitale Identitäten vermehrt für Betrugsdelikte missbraucht werden und der Identitätsdiebstahl zu den häufigsten Bedrohungen im Internet zählt. Aufgrund der steigenden Zahl von Transaktionen und der gleichzeitig steigenden Komplexität der digitalen Vorgänge, die mit digitalen Identitäten verknüpft sind, den steigenden Erwartungen und Anforderungen der Nutzer an digitale Identitäten sowie wachsenden gesetzlichen und vertraglichen Anforderungen wird der Schutz digitaler Identitäten immer wichtiger. Im Rahmen der Vorlesung und der Übungen werden grundlegende und fortgeschrittene Techniken zum Schutz digitaler Identitäten vorgestellt, u.a. die folgenden Themen:

- Schutz durch und für biometrische Daten
- Identity-Protection-Ansätze (z.B. mobile Endgeräte als Security-Tokens, Vereinheitlichung digitaler Identitäten, behavioral biometrics)
- Identity and Access Management (IAM) und "IAM as a Service" (IAMaaS)

Unter Cloud Computing versteht man die Bereitstellung von IT-Infrastruktur wie beispielsweise Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung über das Internet. Die Vorlesung mit Übungen "Cloud Computing Security" setzt sich mit Security-Risiken im Umfeld von Cloud Computing auseinander, u.a.:

- Verletzung der Vertraulichkeit und Integrität der Daten
- Löschung von Daten (z.B. aufgrund gesetzlicher Regelungen)
- Ungenügende Mandantentrennung
- Verletzung der Compliance
- Verletzung von Datenschutzgesetzen

In der Vorlesung werden dazu u.a. die folgenden Lösungen und Gegenmaßnahmen vorgestellt und in den Übungen an praktischen Beispielen eingeübt:

- Kontrollmechanismen für Cloud Computing Security (abschreckende, präventive, erkennende und korrigierende)
- Identitätsmanagement
- Datenschutz
- Zugriffskontrolle
- Schutz gegen Seitenkanalangriffe
- Verschlüsselung (u.a. homomorphe Verschlüsselung)

Datenschutz ist angesichts technologischer Entwicklungen, informationeller Globalisierung und eines komplexen rechtlichen Rahmens ein zentraler Compliance-Aspekt und betrifft Unternehmen ebenso wie die öffentliche Verwaltung sowie die Bundeswehr. Der inhaltliche Fokus des Praktikums "Datenschutz und Privacy" liegt auf der EU-Datenschutz-Grundverordnung und dem nationalen Datenschutzrecht. Ergänzend werden komplementäre Rechtsbereiche mit relevanten Querbezügen (u.a. Arbeitsrecht, Persönlichkeitsschutz und Telekommunikationsrecht) behandelt. In praktischen Übungen werden technischen Aspekte der Datensicherheit sowie zum Datenschutzmanagement umgesetzt. In vielen Fällen wird Eigenrecherche und Autodidaktik zur Lösung der Aufgaben notwendig sein.

Leistungsnachweis
Notenschein, der sich aus Teilprüfungen der belegten Veranstaltungen zusammensetzt.
Dauer und Häufigkeit
Das Modul dauert 1-2 Trimester.
Sonstige Bemerkungen
Es müssen drei der genannten Veranstaltungen belegt werden.

Modulname	Modulnummer
Industrial Security	5521

Konto	Wahlpflicht Vertiefungsfeld Public Security

Modulverantwortliche/r	Modultyp	Empf. Trimester
	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
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
Human Factors in Cyber Security	5522

Konto	Wahlpflicht Vertiefungsfeld Public Security

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr.-Ing. Verena Nitsch	Wahlpflicht	3

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55221	VÜ	Risikomanagement und Fehlerprävention	Wahlpflicht	3
55222	VÜ	Cyberpsychologie	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen
Es sind keine besonderen Vorkenntnisse notwendig.

Qualifikationsziele
Die Studierenden lernen Mechanismen der menschlichen Informationsverarbeitung und Handlungsmotivation kennen. Sie können Methoden des Risikomanagements und der Human Error Analyse fachgerecht einsetzen sowie systematisch Maßnahmen zur Erhöhung der Handlungssicherheit entwickeln und in Unternehmen einführen. Weiterhin sind die Studierenden vertraut mit den psychologischen Grundlagen der Cyberkriminalität und in der Lage, diese in der Entwicklung gezielter Gegenmaßnahmen zu berücksichtigen.

Inhalt
Der Mensch kann sowohl eine Sicherheitslücke als auch eine wirksame Barriere gegen Cyberattacken darstellen. In den Lehrveranstaltungen Risikomanagement und Fehlerprävention sowie Cyberpsychologie wird der Faktor Mensch in der Cybersicherheit näher beleuchtet. Die beiden Veranstaltungen behandeln entsprechend cybersicherheitsrelevante Aspekte des Risikomanagements sowie der angewandten Psychologie. In der Veranstaltung Risikomanagement und Fehlerprävention werden u.a. wahrnehmungs-, sozial- und organisationspsychologische Prozesse auf der Ebene des Individuums (z.B. Attributionsfehler), sowie der Gruppe (z.B. Gruppendenken) und der Organisation (z.B. Sicherheitskultur) beleuchtet, die Fehlerentstehung fördern und die Wirksamkeit von technischen Schutzmaßnahmen in Unternehmen einschränken. Etablierte Methoden der Risiko- bzw. Fehleranalyse (FMEA, SWOT, bzw. RCA, HFACS) werden behandelt und mittels Fallstudien vertieft. Fehlerpräventionsmaßnahmen, die

speziell die Risikowahrnehmung und –einschätzung betreffen, wie Security Awareness Training und Verhaltensmodifikationen, werden diskutiert.

Cyberkriminelle nutzen nicht nur technische, sondern vor allem auch menschliche Schwächen aus. Die Veranstaltung Cyberpsychologie bietet dementsprechend einen Überblick über relevante psychologische Aspekte der Cyberkriminalität. Techniken des Social Engineering werden vorgestellt und diskutiert mit einem Fokus auf zugrundeliegenden psychologischen Mechanismen, u.a. Hilfsbereitschaft, Zugehörigkeitsgefühl, Disinhibition, Technikvertrauen und digitale Kompetenz. Handlungsmotivationen und Verhaltensmuster von Cyberkriminellen, sowie situationale Einflüsse auf cyberkriminelles Verhalten werden näher beleuchtet.

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

Modulname	Modulnummer
Analytische Modelle	1032

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence

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
Operations Research	1036

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Stefan Pickl	Pflicht	5

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
10361	VL	Operations Research	Pflicht	3
10362	UE	Operations Research	Pflicht	2
Summe (Pflicht und Wahlpflicht)				5

Empfohlene Voraussetzungen
Kenntnisse in Analysis und Linearer Algebra, wie sie beispielsweise in den Modulen Analysis und Lineare Algebra vermittelt werden.

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 zughörige Probleme zu identifizieren und mit geeigneten Modellen und Lösungsverfahren zu behandeln. Es ist das Ziel des Moduls, dass die Studierenden sicher mit den Standardverfahren des Operations Research umgehen können. Im Rahmen des heutigen unterstützenden Rechnereinsatzes sollen sie in der Lage sein, zukünftige Potentiale zu erkennen und damit verbundene Komplexitätsaspekte kompetent zu behandeln.

Inhalt
Die Veranstaltung führt in das weite fachliche Gebiet des Operations Research ein. Der quantitativen Beschreibung und Lösung von komplexen Entscheidungsproblemen 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). 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. Eine inhaltliche Auswahl besteht aus folgenden Elementen: Einführung in die Problemstellung und Lösungsmethoden der allgemeinen Unternehmensforschung, 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.

Leistungsnachweis
Schriftliche Prüfung von 60 Minuten Dauer.
Dauer und Häufigkeit
Das Modul dauert 1 Trimester.Das Modul beginnt jedes Studienjahr im Wintertrimester.

Modulname	Modulnummer
Informations- und Codierungstheorie	1037

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. 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. Das Modul wird jedes zweite Studienjahr angeboten und beginnt jeweils im Wintertrimester.

Modulname	Modulnummer
Visual Computing (erweitert)	1152

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence

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	Pflicht	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 Übung Bildverarbeitung für Computer Vision werden die Studierenden mit Techniken der Bildverarbeitung vertraut gemacht, die in Computer Vision verwendet werden. Sie lernen deren Einsatzmöglichkeiten kennen und abzuschätzen, welche Technik sich in Abhängigkeit von Faktoren wie Genauigkeit, Robustheit und Geschwindigkeit besonders gut für welches Einsatzgebiet eignet. Neben dem Einsatz in Computer Vision, die durch Dreidimensionalität (3D) und Objekterkennung, d.h. Bestimmung von Objektbedeutung, geprägt ist, werden praktische Einsatzmöglichkeiten der Techniken in der industriellen Bildverarbeitung aufgezeigt.

Der Schwerpunkt der Vorlesung und Übung Computer Vision liegt auf der Rekonstruktion der 3D Geometrie aus perspektiven Bildern inkl. der Bestimmung dichter Tiefendaten, mittels derer realistische 3D Visualisierungen erzeugt werden können. Es werden verschiedene Techniken vorgestellt, die eine Orientierung mit und ohne Wissen über den Aufbau der Kamera (Kalibrierung) ermöglichen. Weiterhin wird gezeigt, wie weit auseinander liegende Aufnahmen (wide-baseline) orientiert werden können und wie bei sehr nah beieinander liegenden Aufnahmen, z.B. aus Videosequenzen, eine Echtzeitauswertung, mit der z.B. in Gebäuden navigiert werden kann, erfolgen kann.

In der Vorlesung und Seminarübung Computer Vision und Graphik werden die Studierenden in Techniken zur automatischen Extraktion von Objekten aus Bildern eingeführt. Neben der aussehensbasierten Extraktion auf Grundlage von ähnlichem Aussehen und ähnlicher Anordnung von kleinen Bildausschnitten, wird insbesondere auf die Möglichkeiten eingegangen, die sich durch eine Kopplung von Computer Vision und

Graphik in Form von generativen Modellen ergeben. Hierbei werden Objekte modelliert und dann visualisiert. Unterschiede zwischen Visualisierungsergebnissen und Bildern motivieren eine Modifikation der Objektmodellierung mit dem Ziel, die Unterschiede zu minimieren.

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

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

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

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

Modulverantwortliche/r	Modultyp	Empf. Trimester
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

Modulverantwortliche/r	Modultyp	Empf. Trimester
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	Wahlpflicht	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

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)				5

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

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr.-Ing. Andreas Karcher	Wahlpflicht	4

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

Qualifikationsziele

Das Modul *Middleware und mobile Cloud Computing* zielt darauf ab, den Studierenden 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 tiefere theoretische Kenntnisse über Architektur, Aufbau und Anwendung aktueller Middlewarekonzepte. Im Übungsteil lernen die Teilnehmer parallel zur Vorlesung den praktischen Umgang mit Middleware-Technologien und Cloud-basierten, mobilen Anwendungen. 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.
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.
Leistungsnachweis
Schriftliche Prüfung von 60 Minuten Dauer oder mündliche Prüfung von 30 Minuten Dauer.
Verwendbarkeit
Die im Modul erworbenen Kenntnisse sind elementar für die IT-technische Gestaltung von verteilten Informatik-Systemen und stellen somit eine Grundlage für Masterstudiengänge im Bereich Informatik/ Wirtschaftsinformatik/ Ingenieurinformatik 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

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 Übung Bildverarbeitung für Computer Vision werden die Studierenden mit Techniken der Bildverarbeitung vertraut gemacht, die in Computer Vision verwendet werden. Sie lernen deren Einsatzmöglichkeiten kennen und abzuschätzen, welche Technik sich in Abhängigkeit von Faktoren wie Genauigkeit, Robustheit und Geschwindigkeit besonders gut für welches Einsatzgebiet eignet. Neben dem Einsatz in Computer Vision, die durch Dreidimensionalität (3D) und Objekterkennung, d.h. Bestimmung von Objektbedeutung, geprägt ist, werden praktische Einsatzmöglichkeiten der Techniken in der industriellen Bildverarbeitung aufgezeigt.

Der Schwerpunkt der Vorlesung und Übung Computer Vision liegt auf der Rekonstruktion der 3D Geometrie aus perspektiven Bildern inkl. der Bestimmung dichter Tiefendaten, mittels derer realistische 3D Visualisierungen erzeugt werden können. Es werden verschiedene Techniken vorgestellt, die eine Orientierung mit und ohne Wissen über den Aufbau der Kamera (Kalibrierung) ermöglichen. Weiterhin wird gezeigt, wie weit auseinander liegende Aufnahmen (wide-baseline) orientiert werden können und wie bei sehr nah beieinander liegenden Aufnahmen, z.B. aus Videosequenzen, eine Echtzeitauswertung, mit der z.B. in Gebäuden navigiert werden kann, erfolgen kann.

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
Formale Entwicklung korrekter Software	1518

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence

Modulverantwortliche/r	Modultyp	Empf. Trimester
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
Algorithmen und Komplexität	3491

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. 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
Security-Lagebilder	5516

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence

Modulverantwortliche/r	Modultyp	Empf. Trimester
	Wahlpflicht	4

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55161	VÜ	Cyber-Lagebilderstellung	Pflicht	3
55162	VÜ	Visuelle Datenauswertung	Wahlpflicht	3
55163	P	Cyber-Lagebilderstellung	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Grundlegende Kenntnisse in Themen und Verfahren der IT-Sicherheit und Grundlagen der Informatik, wie sie in einem Bachelor Informatik oder Wirtschaftsinformatik vermittelt werden.

Qualifikationsziele

- Studierende kennen Gestaltungsprinzipien und Fallbeispiele von Sicherheitslagebildern und speziell von Lagebildern der IT-Sicherheit
- Studierende kennen Methoden und Verfahren der Gestaltung, der Entwicklung und der Evaluation von Lagebildern
- Studierende kennen Verfahren der Auswertung von Informationen für Lagebilder und Visualisierung von Lagebildern

Inhalt

Ein Lagebild soll Informationen zusammenführen, darstellen und damit Entscheidungen und zielgerichtetes Handeln vorbereiten. Frühe Erkennung von Anomalien oder von neuartigen Bedrohungen sowie Trends und Muster in der Entwicklung von Bedrohungslagen sind Themen in der Erstellung von Sicherheitslagebildern. Informationen und Darstellung in Sicherheitslagebildern sind spezifisch für Rollen und auch Ebenen. Lagebilder der IT-Sicherheit müssen dabei selbst hohe Anforderungen hinsichtlich Informationssicherheit in allen Prozessen der Informationsgewinnung, Informationsverarbeitung und Informationspräsentation erfüllen. Usability des IT-Systems und Transparenz aller Prozesse und Verfahren sind zentrale Aspekte in der Gestaltung von Lagebildern.

In der Veranstaltung „Cyber-Lagebilderstellung“ werden zentrale Themen für die Gestaltung von Security Lagebildern und speziell IT-Sicherheitslagebildern behandelt. Dazu gehören die Verfahren der Informationsgewinnung, der Analyse

von Informationen, der Aggregation von Informationen und der Visualisierung von Informationen, der ebenen- und rollengerechten Aufbereitung von Informationen, der Gestaltung von Prozessen und Organisation der Informationsanalyse und der Entscheidungsvorbereitung. Die Akzeptanz von Lagebildtechnologien und die Usability von Lagebildern sind zentrale Themen in der Lagebilderstellung und so sind kreative Methoden in der Gestaltung von IT-Anwendungen und Einbeziehung von Anwendern in die Gestaltung von Lagebildtechnologie ein wichtiges Thema dieser Veranstaltung. „Visuelle Datenauswertung“ legt als Veranstaltung den Fokus auf Verfahren und Werkzeuge der Auswertung und Darstellung von Informationen in Lagebildern. Erkennung und Darstellung von Trends und Mustern und Abweichungen oder Anomalien sind hier wichtige Themen in der Anwendung genau wie die rollen- und ebenengerechte Aufbereitung und Visualisierung von Informationen und Aggregation von geopolitischen, geographischen und IT-Sicherheitsinformationen. Im Praktikum „Cyber-Lagebilderstellung“ wenden Studierende Methoden und Verfahren praktisch an und entwickeln für ausgewählte Fragestellungen Technologie für Sicherheitslagebilder.
Leistungsnachweis
Der Leistungsnachweis erfolgt als Notenschein mit Präsentationen, schriftlichen Ausarbeitungen und Design Studien. Die Prüfungsform wird zu Beginn des Moduls festgelegt.
Dauer und Häufigkeit
1-2 Trimester

Modulname	Modulnummer
Security Data und Intelligence Analysis	5517

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence

Modulverantwortliche/r	Modultyp	Empf. Trimester
	Wahlpflicht	2

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55171	VÜ	Security Data Analytics	Pflicht	3
55172	VÜ	Social Media Analysis	Wahlpflicht	3
55173	VÜ	Text Mining	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Grundkenntnisse zur Verarbeitung IT-sicherheitsrelevanter Informationen, wie sie z.B. im Modul Netzsicherheit vermittelt werden. Gute Kenntnisse imperativer und objektorientierter Programmierung, wie sie u.a. zur Nutzung der APIs sozialer Netzwerke benötigt werden.

Qualifikationsziele

Studierende beherrschen ausgewählte Big-Data-Analysemethoden, die sich speziell für IT-sicherheitsrelevante Daten eignen. Sie kennen die Architektur von Security Information & Event Management Systemen und die zur Datenaggregation, -korrelation und -auswertung eingesetzten Protokolle und Algorithmen. Sie können die Güte prädiktiver und retrospektiver Ansätze in Abhängigkeit von den verwendeten Datenquellen und Randbedingungen wie dem Echtzeit-Einsatz bewerten. Studierende kennen Methoden zur Vorverarbeitung und Aufbereitung unstrukturierter Daten, die z.B. aus sozialen Netzwerken abgerufen werden, um daraus Rückschlüsse auf sicherheitsrelevante Abläufe zu ziehen. Sie kennen Algorithmen z.B. zur Text- und Sentimentanalyse und können deren Güte und Grenzen beurteilen.

Inhalt

Die Vorlesung Security Data Analytics führt u.a. anhand der Anwendungsgebiete Security-Monitoring und IT-Forensik in die Auswertung so großer Mengen an sicherheitsrelevanten Daten ein, dass eine manuelle Analyse nicht zielführend wäre. Auf Basis von Security Information und Event Management Systemen, die Protokolldaten und Security-Meldungen von typischerweise Hunderten von Systemen aggregieren und korrelieren müssen, wird der gesamte Auswertungszyklus zunächst konzeptionell aufbereitet und durch ausgewählte Algorithmen, z.B. für regelbasierte Computer-assisted Audit Techniques, und Werkzeuge veranschaulicht. Für verschiedene Anwendungsdomänen werden anschließend Data-Mining- und Outlier-Detection-

Verfahren behandelt. In den Übungen werden regelbasierte, statistikbasierte und visuelle Werkzeuge zur Datenauswertung erprobt und ausgewählte Knowledge-Discovery-Algorithmen implementiert.

In der Vorlesung Social Media Analysis werden technische und algorithmische Ansätze zur Auswertung von frei verfügbaren Daten aus sozialen Netzwerken behandelt. Während eine Auswertung sozialer Netzwerke kommerziell überwiegend im Kontext der Public Relations von Unternehmen erfolgt, findet eine Fokussierung auf sicherheitsrelevante Informationen statt, die eine andere Form der Auswertung und Verknüpfung mit spezielleren Bestandsdaten und anderen Echtzeit-Informationsquellen erfordert. Anhand aktueller Forschungsansätze und Studien wird auf Problembereiche wie die Zuverlässigkeit bzw. Beeinflussbarkeit öffentlicher Datenquellen durch manipulierte Meldungen und entsprechende Gegenmaßnahmen durch Plausibilitäts- und Konsistenzprüfungen eingegangen.

Die Vorlesung Text Mining behandelt Data-Mining-Verfahren zur Auswertung natürlichsprachlicher Texte mit ihren Anwendungsgebieten von der Autorenidentifikation bis zum Question Answering. Neben den grundlegenden Verfahren zum Preprocessing, um den unstrukturierten Text analysierbar zu machen, werden Ansätze zur Informations- und Relationsextraktion sowie zur Indexierung und Klassifikation von Texten behandelt. Neben automatenbasierten Ansätzen kommen dabei auch Verfahren des maschinellen Lernens zum Einsatz. Zur Datenauswertung, die anhand von Fallbeispielen zur IT-Sicherheit erarbeitet wird, werden ausgewählte Visualisierungsverfahren eingeführt.

Leistungsnachweis
Schriftliche Prüfung mit 60 Minuten Dauer oder mündliche Prüfung mit 30 Minuten Dauer. Die Prüfungsform wird zu Beginn des Moduls festgelegt.
Dauer und Häufigkeit
Das Modul dauert 1-2 Trimester.

Modulname	Modulnummer
Automatisierung in der Sicherheitsdatenauswertung	5518

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence

Modulverantwortliche/r	Modultyp	Empf. Trimester
	Wahlpflicht	3

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55181	VÜ	Machine Learning and Artificial Intelligence	Pflicht	3
55182	VÜ	Biometrische Systeme	Pflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Kenntnisse der Auswertung von Sicherheitsdaten, wie z.B. im Modul Security Data and Intelligence Analysis vermittelt. Gute Kenntnisse in linearer Algebra und imperativer Programmierung.

Qualifikationsziele

Die Studierenden beherrschen die technischen und mathematischen Grundlagen des maschinellen Lernens. Sie kennen Methoden und Algorithmen in den Bereichen Supervised, Unsupervised und Reinforcement Learning und können Probleme wie Overfitting vermeiden. Die Studierenden kennen biometrische Merkmale von Menschen und deren Anwendungsgebiete wie Identifikation und Authentifizierung. Für verschiedene biometrische Merkmale kennen sie die mit dem Stand der Technik verbundenen Fehlerraten und Randbedingungen für den praktischen Einsatz.

Inhalt

Die Vorlesung Machine Learning and Artificial Intelligence vermittelt Methoden zur Implementierung lernfähiger Systeme. Anhand von neuronalen Netzen und Support Vector Machines wird der Bereich des Supervised Learning eingeführt und gezeigt, wie die Performanz neuronaler Netze mit Deep-Learning-Ansätzen verbessert werden kann. U.a. auf Basis der Clusteranalyse werden die Methoden des Unsupervised Learning vermittelt, das beispielsweise zur automatisierten Erkennung von Strukturen in Daten eingesetzt werden kann, und zum optimierenden Lernen weiterentwickelt. Besonderer Fokus wird auf die Qualität von Trainingsdaten durch Vorverarbeitung, Dimensionsreduktion und Auswahl relevanter Merkmale gelegt. Abschließend werden Ansätze zur Kombination verschiedener Modelle z.B. bei Klassifizierer-Ensembles vertieft. In Übungsaufgaben werden ausgewählte Ansätze implementiert und zur Auswertung von Sicherheitsdaten angewandt und bewertet.

In der Vorlesung Biometrische Systeme werden die technische Erfassung und algorithmische Verarbeitung ausgewählter biometrischer Merkmale von Menschen behandelt, u.a. Fingerabdruck, Handvenenmuster, Irismuster, Gesicht, Sprache, Tastaturtippverhalten und Gangart. Je nach Anwendungsgebiet, z.B. Identifizierung von Personen auf Basis von Bild-/Filmmaterial oder Authentifizierung von Personen u.a. beim Zutritt zu Sicherheitsbereichen, und Größe des relevanten Personenkreises müssen Erkennungsleistungsaspekte wie Fehlerraten bei der Erfassung und Kooperationsbereitschaft der Subjekte systematisch berücksichtigt werden. Neben Aspekten des Datenschutzes und ethischen Fragestellungen spielen auch Komfort und Usability eine wichtige Rolle für die praktische Akzeptanz der Verfahren. Zu allen Verfahren werden mögliche Angriffe und Gegenmaßnahmen wie die Verifikation der Lebendigkeit betrachtet.

Leistungsnachweis

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

Dauer und Häufigkeit

Das Modul dauert 1 Trimester.

Modulname	Modulnummer
Cryptography Engineering	5519

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Cornelius Greither	Wahlpflicht	4

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	Wahlpflicht	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.

Modulname	Modulnummer
Industrial Security	5521

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence

Modulverantwortliche/r	Modultyp	Empf. Trimester
	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
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
Human Factors in Cyber Security	5522

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence

Modulverantwortliche/r	Modultyp	Empf. Trimester
Prof. Dr.-Ing. Verena Nitsch	Wahlpflicht	3

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

Zugehörige Lehrveranstaltungen:

Nr.	Art	Veranstaltungsname	Teilnahme	TWS
55221	VÜ	Risikomanagement und Fehlerprävention	Wahlpflicht	3
55222	VÜ	Cyberpsychologie	Wahlpflicht	3
Summe (Pflicht und Wahlpflicht)				6

Empfohlene Voraussetzungen

Es sind keine besonderen Vorkenntnisse notwendig.

Qualifikationsziele

Die Studierenden lernen Mechanismen der menschlichen Informationsverarbeitung und Handlungsmotivation kennen. Sie können Methoden des Risikomanagements und der Human Error Analyse fachgerecht einsetzen sowie systematisch Maßnahmen zur Erhöhung der Handlungssicherheit entwickeln und in Unternehmen einführen. Weiterhin sind die Studierenden vertraut mit den psychologischen Grundlagen der Cyberkriminalität und in der Lage, diese in der Entwicklung gezielter Gegenmaßnahmen zu berücksichtigen.

Inhalt

Der Mensch kann sowohl eine Sicherheitslücke als auch eine wirksame Barriere gegen Cyberattacken darstellen. In den Lehrveranstaltungen Risikomanagement und Fehlerprävention sowie Cyberpsychologie wird der Faktor Mensch in der Cybersicherheit näher beleuchtet. Die beiden Veranstaltungen behandeln entsprechend cybersicherheitsrelevante Aspekte des Risikomanagements sowie der angewandten Psychologie.

In der Veranstaltung Risikomanagement und Fehlerprävention werden u.a. wahrnehmungs-, sozial- und organisationspsychologische Prozesse auf der Ebene des Individuums (z.B. Attributionsfehler), sowie der Gruppe (z.B. Gruppendenken) und der Organisation (z.B. Sicherheitskultur) beleuchtet, die Fehlerentstehung fördern und die Wirksamkeit von technischen Schutzmaßnahmen in Unternehmen einschränken. Etablierte Methoden der Risiko- bzw. Fehleranalyse (FMEA, SWOT, bzw. RCA, HFACS) werden behandelt und mittels Fallstudien vertieft. Fehlerpräventionsmaßnahmen, die

speziell die Risikowahrnehmung und –einschätzung betreffen, wie Security Awareness Training und Verhaltensmodifikationen, werden diskutiert.

Cyberkriminelle nutzen nicht nur technische, sondern vor allem auch menschliche Schwächen aus. Die Veranstaltung Cyberpsychologie bietet dementsprechend einen Überblick über relevante psychologische Aspekte der Cyberkriminalität. Techniken des Social Engineering werden vorgestellt und diskutiert mit einem Fokus auf zugrundeliegenden psychologischen Mechanismen, u.a. Hilfsbereitschaft, Zugehörigkeitsgefühl, Disinhibition, Technikvertrauen und digitale Kompetenz. Handlungsmotivationen und Verhaltensmuster von Cyberkriminellen, sowie situationale Einflüsse auf cyberkriminelles Verhalten werden näher beleuchtet.

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

Modulname	Modulnummer
Signalverarbeitung	6050

Konto	Wahlpflicht Vertiefungsfeld Security Intelligence

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

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
Seminarmodul CYB	5501

Konto	Seminar - CYB 2018

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. Wolfgang Hommel	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 2018

Modulverantwortliche/r	Modultyp	Empf. Trimester
Univ.-Prof. Dr. 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
Zentralinstitut Studium+	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.

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	**Plichtmodule - CYB 2018**		**44**
1	3	5502	Netzsicherheit	G. Dreo Rodosek	6
1	2	5503	Hardwaresicherheit	K. Buchenrieder	6
1	3	5504	Datenschutz und Privacy	N. N.	6
2	2	5505	Systemsicherheit	G. Teege	6
1	3	5506	Kryptologie	N. N.	6
2	2	5507	Anwendungssicherheit	W. Hommel	6
2	3	5508	Security- und IT- Management	U. Lechner	8
		8 -10	**Überkonto Wahlpflicht - CYB 2018**		**36**
1	6	3459	Grundlagen der Informationssicherheit	W. Hommel	6
		9	**Wahlpflicht Vertiefungsfeld Enterprise Security**		**30**
1	3	1008	Einführung in das Industrial Engineering	O. Rose	9
3	7	1034	Softwareentwicklungsumgebungen	M. Minas	6
3	3	1168	Integrierte Anwendungssysteme im Produkt Lifecycle Management	A. Karcher	6
1	1	1231	Data Mining und IT- basierte Entscheidungsunterstützung	S. Pickl	6
6	6	1306	Web Technologies	M. Koch	6
4	1	1398	Middleware und mobile Cloud Computing	A. Karcher	6
1	1	1507	Enterprise Architecture und IT Service Management	A. Karcher	6
1	2	1518	Formale Entwicklung korrekter Software	B. Elbl	6
3	3	3647	Compilerbau	S. Brunthaler	6
3	3	3648	Compilerbau (erweitert)	S. Brunthaler	9
4		3665	Benutzbare Sicherheit	F. Alt	9
4	5	5509	Offensive Sicherheitsüberprüfungen	N. N.	6
2	3	5510	Maschinennahe Softwareanalyse	N. N.	6
4	4	5511	Automatisierung in der Angriffserkennung	N. N.	6
3	5	5512	Softwareanalyse und -härtung	N. N.	6
4	5	5519	Cryptography Engineering	C. Greither	9
3	4	5520	Security Engineering	N. N.	9
3	4	5522	Human Factors in Cyber Security	V. Nitsch	6
		10	**Wahlpflicht Vertiefungsfeld Public Security**		**30**
1	3	1008	Einführung in das Industrial Engineering	O. Rose	9
1	3	1033	Simulationstechnik	O. Rose	9
5	5	1036	Operations Research	S. Pickl	5
0	1	1166	Formale Entwicklung korrekter Software	N. N.	12
6	6	1306	Web Technologies	M. Koch	6
3	3	1394	Aviation Management, Computational Networks and System Dynamics	S. Pickl	6

4	1	1398	Middleware und mobile Cloud Computing	A. Karcher	6
3	3	2461	Ökonomie und Recht der Informationsgesellschaft	S. Koos	5
4		3665	Benutzbare Sicherheit	F. Alt	9
3	4	5513	Mobile Security	G. Dreo Rodosek	6
2	3	5514	Staatliche IT-Sicherheit	U. Lechner	6
3	4	5515	Rechtliche und ethische Aspekte der IT-Sicherheit	N. N.	6
3	4	5520	Security Engineering	N. N.	9
3	4	5521	Industrial Security	N. N.	6
3	4	5522	Human Factors in Cyber Security	V. Nitsch	6
		11	**Wahlpflicht Vertiefungsfeld Security Intelligence**		**30**
2	3	1032	Analytische Modelle	M. Siegle	9
5	5	1036	Operations Research	S. Pickl	5
1	0	1037	Informations- und Codierungstheorie	P. Hertling	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
4	1	1398	Middleware und mobile Cloud Computing	A. Karcher	6
2	2	1489	Visual Computing	H. Mayer	6
1	2	1518	Formale Entwicklung korrekter Software	B. Elbl	6
2	2	3491	Algorithmen und Komplexität	P. Hertling	5
4	5	5516	Security-Lagebilder	N. N.	6
2	3	5517	Security Data und Intelligence Analysis	N. N.	6
3	3	5518	Automatisierung in der Sicherheitsdatenauswertung	N. N.	6
4	5	5519	Cryptography Engineering	C. Greither	9
3	4	5521	Industrial Security	N. N.	6
3	4	5522	Human Factors in Cyber Security	V. Nitsch	6
8	0	6050	Signalverarbeitung	A. Knopp	8
		13	**Seminar - CYB 2018**		**5**
1	0	5501	Seminarmodul CYB	W. Hommel	5
		14	**Masterarbeit - CYB 2018**		**30**
5	5	5500	Masterarbeit CYB	W. Hommel	30
		99MA	**Verpflichtendes Begleitstudium plus**		**5**
	9	1008	Seminar studium plus, Training	. Zentralinstitut Studium+	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
	1037	Informations- und Codierungstheorie	Vorlesung/Übung	WPf	5
	11662	Methoden und Werkzeuge	Vorlesung/Übung	WPf	5
	11663	Modulprojekt	Vorlesung/Übung	WPf	4
	11664	Spezifikation	Vorlesung/Übung	WPf	5
	13943	Computational Networks	Vorlesung/Übung	WPf	3
	36481	Praktikum Compilerbau	Praktikum	Pf	3
	36651	Benutzbare Sicherheit und Privatsphäre	Vorlesung/Übung	Pf	4
	36652	Seminar Empirische Forschungsmethoden in der IT-Sicherheit	Seminar	Pf	2
	36653	Praktikum Design sicherer und benutzbarer Systeme	Praktikum	Pf	3
	55091	Penetration Testing	Vorlesung/Übung	Pf	3
	55092	Social Engineering	Vorlesung/Übung	WPf	3
	55093	Penetration Testing	Praktikum	WPf	3
	55101	Schwachstellenanalyse und -beseitigung	Vorlesung/Übung	Pf	3
	55102	Software Reverse Engineering und Exploitentwicklung	Vorlesung/Übung	WPf	3
	55103	Schwachstellenanalyse und Exploitentwicklung	Praktikum	WPf	3
	55104	Statische und dynamische Code-Analyse	Vorlesung/Übung	WPf	3
	55111	Autonome Sicherheitsmaßnahmen	Vorlesung/Übung	Pf	3
	55112	Frühwarnsysteme	Vorlesung/Übung	Pf	3
	55121	Malware-Analyse	Vorlesung/Übung	Pf	3
	55122	Operating System Hardening und System Intrusion Detection	Vorlesung/Übung	WPf	3
	55123	Seitenkanalangriffe gegen Software	Vorlesung/Übung	WPf	3
	55124	IT-Forensik	Praktikum	WPf	3
	55125	Malware-Analyse	Praktikum	WPf	3
	55131	Sichere mobile Systeme	Vorlesung/Übung	WPf	3
	55132	Sensorik und Manipulationsdetektion	Vorlesung/Übung	WPf	3
	55142	IT-Security in der zivilen Sicherheit	Vorlesung/Übung	WPf	3
	55151	Ethical Hacking and Defense	Vorlesung/Übung	WPf	2
	55152	Kriminalpsychologie	Vorlesung/Übung	WPf	2
	55161	Cyber-Lagebilderstellung	Vorlesung/Übung	Pf	3
	55162	Visuelle Datenauswertung	Vorlesung/Übung	WPf	3
	55163	Cyber-Lagebilderstellung	Praktikum	WPf	3
	55171	Security Data Analytics	Vorlesung/Übung	Pf	3
	55172	Social Media Analysis	Vorlesung/Übung	WPf	3
	55173	Text Mining	Vorlesung/Übung	WPf	3
	55181	Machine Learning and Artificial Intelligence	Vorlesung/Übung	Pf	3

	55182	Biometrische Systeme	Vorlesung/Übung	Pf	3
	55191	Post-Quantum Kryptographie	Vorlesung/Übung	WPf	3
	55192	Implementierung und Anwendung kryptographischer Verfahren	Praktikum	WPf	3
	55201	Formale Methoden der Informationssicherheit	Vorlesung/Übung	WPf	3
	55202	Sichere Softwareentwicklung	Praktikum	WPf	3
	55203	User-Centric Security and Privacy-by-Design	Vorlesung/Übung	WPf	3
	55204	Schutz digitaler Identitäten	Vorlesung/Übung	WPf	3
	55205	Cloud Computing Security	Vorlesung/Übung	WPf	3
	55206	Datenschutz und Privacy	Praktikum	WPf	3
	55211	Internet of Things and Industrial Internet Security	Vorlesung/Übung	WPf	3
	55212	Praktikum Sicherheit eingebetteter Systeme	Praktikum	WPf	3
	55221	Risikomanagement und Fehlerprävention	Vorlesung/Übung	WPf	3
	55222	Cyberpsychologie	Vorlesung/Übung	WPf	3
1	10102	Netzsicherheit	Vorlesung/Übung	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	11651	Rechtsfragen der Informatik	Vorlesung	Pf	2
1	11661	Entwurf Verteilter Systeme	Vorlesung/Übung	WPf	5
1	12112	Ausgewählte mathematische Methoden in Kryptographie und Codierungstheorie	Vorlesung/Übung	WPf	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	55041	Datenschutz	Vorlesung/Übung	Pf	3
1	55062	Kryptoanalyse	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	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	15172	Methoden und Werkzeuge	Vorlesung/Übung	WPf	5
2	34911	Algorithmen und Komplexität	Vorlesung/Übung	WPf	5
2	55031	Embedded Systems Security	Vorlesung/Übung	Pf	3

2	55051	Betriebssystemsicherheit	Vorlesung/Übung	Pf	3
2	55071	Language-based Security	Vorlesung/Übung	Pf	3
2	55143	Security- und Krisenmanagement im internationalen Kontext	Vorlesung/Übung	WPf	3
3	10081	Produktionsmanagement in der Fertigung	Vorlesung	Pf	3
3	10082	Ressourceneinsatzplanung für die Fertigung	Vorlesung	Pf	3
3	10103	Praktikum Netzsicherheit	Praktikum	Pf	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	11522	Computer Vision und Graphik	Vorlesung/Übung	Pf	3
3	11681	Integrierte Anwendungssysteme im Product Lifecycle Management	Vorlesung	Pf	3
3	11682	Integrierte Anwendungssysteme im Product Lifecycle Management	Übung	Pf	2
3	11972	Mobile Kommunikationssysteme	Vorlesung/Übung	Pf	3
3	12111	Algorithmische Zahlentheorie	Vorlesung/Übung	WPf	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	WPf	3
3	24611	Ökonomie und Recht der Informationsgesellschaft	Vorlesung/Seminar	WPf	2
3	36471	Compilerbau	Vorlesung	Pf	2
3	36472	Compilerbau	Übung	Pf	4
3	55042	Privacy Enhancing Technologies	Vorlesung/Übung	Pf	3
3	55061	Einführung in die Kryptographie	Vorlesung/Übung	Pf	3
3	55141	Schutz von kritischen Infrastrukturen	Vorlesung/Übung	Pf	3
3	55153	Gesellschaftliche Implikationen der Informationssicherheit	Vorlesung/Übung	WPf	2
5	10361	Operations Research	Vorlesung	Pf	3
5	10362	Operations Research	Übung	Pf	2
6	10101	Ausgewählte Kapitel der IT-Sicherheit	Vorlesung/Übung	Pf	3
6	11432	Sicherheit in der Informationstechnik	Vorlesung/Übung	Pf	3
6	11901	Web Technologies	Vorlesung/Übung	Pf	3