fhwedel
UNIVERSITY OF APPLIED SCIENCES

Staatlich anerkannte Fachhochschule
PTL Wedel, Prof. Dr. D. Harms, Prof. Dr. H. Harms
Gemeinnützige Schulgesellschaft mbH

Modulhandbuch

Master-Studiengang
IT-Sicherheit

M_ITS14.0

Wedel, den 30. Juni 2016

Inhaltsverzeichnis

1 Erläuterungen zu den Modulbeschreibungen

Im Folgenden wird jedes Modul in tabellarischer Form beschrieben. Die Reihenfolge der Beschreibungen richtet sich nach den Modulkürzeln.
Vor den Modulbeschreibungen sind zwei Verzeichnisse aufgeführt, die den direkten Zugriff auf einzelne Modulbeschreibungen unterstützen sollen. Ein Verzeichnis listet die Modulbeschreibungen nach Kürzel sortiert auf, das zweite Verzeichnis ist nach Modulbezeichnung alphabetisch sortiert.
Die folgenden Erläuterungen sollen die Interpretation der Angaben in einzelnen Tabellenfeldern erleichtern, indem sie die Annahmen darstellen, die beim Ausfüllen der Felder zugrunde gelegt wurden.

Angaben zum Modul

`Modulkürzel:`	FH-internes, bezogen auf den Studiengang eindeutiges Kürzel des Moduls
`Modulbezeichnung:`	Textuelle Kennzeichnung des Moduls
`Lehrveranstaltungen:`	Lehrveranstaltungen, die im Modul zusammen gefasst sind, mit dem FH-internen Kürzel der jeweiligen Leistung und ihrer Bezeichnung
`Prüfung im Semester:`	Auflistung der Semester, in denen nach Studienordnung erstmals Modulleistungen erbracht werden können
`Modulverantwortliche(r):`	Die strategischen Aufgaben des Modulverantwortlichen umfassen insbesondere: • Synergetische Verwendung des Moduls auch in weiteren Studiengängen • Entwicklung von Anstößen zur Weiterentwicklung der Moduls und seiner Bestandteile • Qualitätsmanagement im Rahmen des Moduls (z. B. Relevanz, ECTS-Angemessenheit) • Inhaltsübergreifende Prüfungstechnik. Die operativen Aufgaben des Modulverantwortlichen umfassen insbesondere: • Koordination von Terminen in Vorlesungs- und Klausurplan • Aufbau und Aktualisierung der Modul- und Vorlesungsbeschreibungen • Zusammenführung der Klausurbestandteile, die Abwicklung der Klausur (inkl. Korrekturüberwachung bis hin zum Noteneintrag) in enger Zusammenarbeit mit den Lehrenden der Modulbestandteile • Funktion als Ansprechpartner für Studierende des Moduls bei sämtlichen modulbezogenen Fragestellungen.
`Zuordnung zum Curriculum:`	Auflistung aller Studiengänge, in denen das Modul auftritt

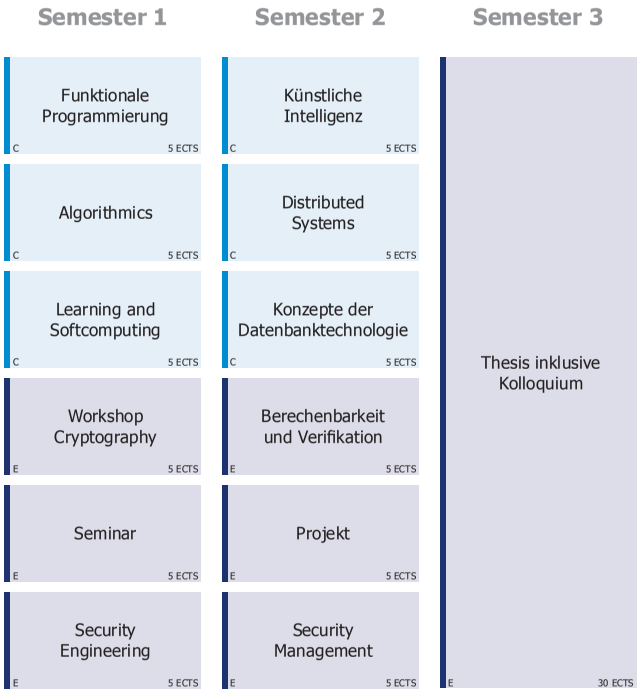
`Querweise:`	Angabe, in welchem Zusammenhang das Modul zu anderen Modulen steht
`SWS des Moduls:`	Summe der SWS, die in allen Lehrveranstaltungen des Moduls anfallen
`ECTS des Moduls:`	Summe der ECTS-Punkte, die in allen Lehrveranstaltungen des Moduls erzielt werden können
`Arbeitsaufwand:`	Der Gesamtarbeitsaufwand in Stunden ergibt sich aus den ECTS-Punkten multipliziert mit 30 (Stunden). Der Zeitaufwand für das Eigenstudium ergibt sich, wenn vom Gesamtaufwand die Präsenzzeiten abgezogen werden. Diese ergeben sich wiederum aus den Semesterwochenstunden (SWS), die multipliziert mit 45 (Minuten) geteilt durch 60 die Präsenzzeit ergeben.
`Voraussetzungen:`	Module und Lehrveranstaltungen, die eine inhaltliche Grundlage für das jeweilige Modul darstellen. Bei Lehrveranstaltungen ist der Hinweis auf das jeweilige Modul enthalten, in dem die Lehrveranstaltung als Bestandteil auftritt.
`Dauer:`	Anzahl der Semester die benötigt werden, um das Modul abzuschließen
`Häufigkeit:`	Angabe, wie häufig ein Modul pro Studienjahr angeboten wird (jedes Semester bzw. jährlich)
`Studien-/Prüfungsleistungen:`	Auflistung aller Formen von Leistungsermittlung, die in den Veranstaltungen des Moduls auftreten
`Prozentualer Anteil an der Gesamtnote:`	Prozentualer Anteil des Moduls an der Gesamtnote
`Sprache:`	In der Regel werden die Lehrveranstaltungen aller Module auf Deutsch angeboten. Um Gaststudierenden unserer Partnerhochschulen, die nicht der deutschen Sprache mächtig sind, die Teilnahme an ausgewählten Lehrveranstaltungen zu ermöglichen, ist die Sprache in einigen Modulen als „deutsch/englisch“ deklariert. Dieses wird den Partnerhochschulen mitgeteilt, damit sich die Interessenten für ihr Gastsemester entsprechende Veranstaltungen heraussuchen können.
`Lernziele des Moduls:`	Übergeordnete Zielsetzungen hinsichtlich der durch das Modul zu vermittelnden Kompetenzen und Fähigkeiten aggregierter Form

Angaben zu den Lehrveranstaltungen

`Lehrveranstaltung:`	Bezeichnung der Lehrveranstaltung, die im Modul enthalten ist
`Dozent(en):`	Namen der Dozenten, die die Lehrveranstaltung durchführen
`Hörtermin:`	Angabe des Semesters, in dem die Veranstaltung nach Studienordnung gehört werden sollte
`Art der Lehrveranstaltung:`	Angabe, ob es sich um eine Pflicht- oder Wahlveranstaltung handelt
`Lehrform / SWS:`	Die SWS der im Modul zusammen gefassten Lehrveranstaltungen werden nach Lehrform summiert angegeben
`ECTS:`	Angabe der ECTS-Punkte, die in dieser Lehrveranstaltung des Moduls erzielt werden können
`Medienformen:`	Auflistung der Medienform(en), die in der Veranstaltung eingesetzt werden
`Lernziele/Kompetenzen:`	Stichwortartige Nennung die zentralen Lernziele der Lehrveranstaltung
`Inhalt:`	Gliederungsartige Auflistung der wesentlichen Inhalte der Lehrveranstaltung
`Literatur:`	Auflistung der wesentlichen Quellen, die den Studierenden zur Vertiefung zu den Veranstaltungsinhalten empfohlen werden. Es wird keine vollständige Auflistung aller Quellen gegeben, die als Grundlage für die Veranstaltung dienen.

MSc IT-Sicherheit
Start zum Sommersemester

fhwedel
UNIVERSITY OF APPLIED SCIENCES



C INFORMATIK
E KERNFACH

Alle Angaben ohne Gewähr
Stand 22.02.2016

MSc IT-Sicherheit
Start zum Wintersemester

fhwedel
UNIVERSITY OF APPLIED SCIENCES

C INFORMATIK
E KERNFACH

Alle Angaben ohne Gewähr
Stand 22.02.2016

3 Modulbeschreibungen

3.1 Algorithmics

M003 Algorithmics	
Studiengang	Master-Studiengang IT-Sicherheit
Modulkürzel	M003
Modulbezeichnung	Algorithmics
Lehrveranstaltung(en)	`M003a` Algorithmics
Modulverantwortliche(r)	Prof. Dr. Sebastian Iwanowski
Zuordnung zum Curriculum	Informatik (Master) IT Engineering (Master) IT-Sicherheit (Master)
Verwendbarkeit des Moduls	The module is a starting module. It sets the theoretical fundamentals for a scientific IT oriented study. It covers the knowledge about fundamental algorithms that are necessary for the solution of various application problems.
SWS des Moduls	4
ECTS des Moduls	5
Arbeitsaufwand	attendance study: 38 hours self study: 112 hours
Voraussetzungen	Understanding basic mathematical concepts such as definitions, theorems and proofs. ability of logically sound formulation The students must be able to follow proofs from the beginning of this course. Required is excellent knowledge of the basics of discrete mathematics, specially in number theory and graph theory. The students must have good programming knowledge and experience in implementing basic algorithms.
Dauer	1 semester
Häufigkeit	every year
Prüfungsformen	written or oral examination
Anteil an Gesamtnote	5,88
Sprache	english

Lernziele des Moduls

The students know how to evaluate the efficiency of algorithms with theoretically sound methods. For selected application domains, they know how to describe algorithms in detail, show examples and implement them. They are able to solve basic proofs for efficiency and

correctness on their own. They can understand even complicated proofs and explain them to other people.

3.1.1 Algorithmics

Lehrveranstaltung	Algorithmics
Dozent(en)	Sebastian Iwanowski
Hörtermin	2
Art der Lehrveranstaltung	Pflicht (M_Inf14.0, M_ITS14.0) Wahl (M_ITE15.0)
Lehrform / SWS	lecture with tutorial, workshop, assignment
ECTS	5.0
Lehr- und Medienform(en)	-

Lernziele

The students ...

- know the fundamental problems of algorithmics and the classical solving methods.
- are able to analyse the correctness and efficiency of algorithms.
- have detailed knowledge of advanced algorithms for miscellaneous problems in selected application domains.
- know how to implement theoretical results in practical applications.

Inhalt

- Introduction into formal algorithmics
  - Comparing basic sorting techniques
  - Complexity measures for the analysis of algorithms
  - Lower bound for algorithms using comparisons only
- Advanced searching and sorting
  - Order statistics
  - Searching in sorted arrays
  - Sorting in finite domains
- Solutions for the dictionary problem
  - Hashing and other methods for optimising the average case behaviour
  - (2,3)-trees as example for an optimal worst case behaviour tree
  - Other optimal worst case methods for search trees
  - Optimal binary search trees (Bellman)
- Graph algorithms
  - Minimum spanning trees as motivation for basic algorithms
  - Shortest paths (Dijkstra, Floyd-Warshall, Strassen)
  - Computation of maximum flows in s/t-networks (Ford-Fulkerson, Edmonds-Karp, Dinic)
  - Computation of graph matchings (bipartite, Edmonds)
- String matching

- Fundamentals of algorithmic geometry
  - Basic problems and the use of Voronoi diagrams for solving them
  - Sweep techniques (including computation of Voronoi diagrams)

Literatur

- deBerg, M., Cheong, O., van Krefeld, M., Overmars, M.:
  Computational Geometry, Algorithms and Applications.
  Springer 2008 (3. edition), ISBN 978-3540779735
- Cormen, T.; Leiserson C.; Rivest, R.; Stein, C.:
  Introduction to Algorithms,
  MIT Press 2001 (2nd ed.)
- Levitin, A.:
  Introduction to the Design and Analysis of Algorithms.
  Addison-Wesley 2006, ISBN 0-321-36413-9
- Mehlhorn, K. / Sanders, P.:
  Algorithms and Data Structures The Basic Toolbox.
  Springer 2008, ISBN 978-3-540-77977-3
- Papadimitriou, C. / Steiglitz, K.:
  Combinatorial Optimization Algorithms and Complexity.
  Dover 1998, ISBN 0-486-40258-4

3.2 Funktionale Programmierung

M005 Funktionale Programmierung

Studiengang	Master-Studiengang IT-Sicherheit
Modulkürzel	M005
Modulbezeichnung	Funktionale Programmierung
Lehrveranstaltung(en)	`M005a` Funktionale Programmierung `M005b` Übg. Funktionale Programmierung
Modulverantwortliche(r)	Prof. Dr. Uwe Schmidt
Zuordnung zum Curriculum	Informatik (Master) IT-Sicherheit (Master)
Verwendbarkeit des Moduls	Das Modul kann sinnvoll im Modul „Künstliche Intelligenz“, in Projekten und der Master-Thesis genutzt werden.
SWS des Moduls	4
ECTS des Moduls	5
Arbeitsaufwand	Präsenzstudium: 38 Stunden Eigenstudium: 112 Stunden
Voraussetzungen	Voraussetzungen sind Kenntnisse und praktische Erfahrungen in höheren Programmiersprachen, insbesondere mit getypten Sprachen. Außerdem werden Kenntnisse über Diskrete Mathematik und algebraische Strukturen erwartet. Elementares Wissen über Komplexitätstheorie wird ebenfalls vorausgesetzt.
Dauer	1 Semester
Häufigkeit	jährlich
Prüfungsformen	Klausur / Mündliche Prüfung (Teil M005a), Abnahme (Teil M005b)
Anteil an Gesamtnote	5,88
Sprache	deutsch

Lernziele des Moduls

In diesem Modul werden fortgeschrittenen Techniken der funktionalen Programmierung am Beispiel der Sprache Haskell behandelt. Hierzu gehören der Umgang mit Funktionen höherer Ordnung, das Arbeiten mit generischen Datentypen und mit Typklassen, und mit Monaden und Arrows. Es werden beispielhaft eingebettete problemspezifische Sprachen (EDSL) vorgestellt. Dieses Modul soll außerdem die Abstraktion, die Modellbildung stärken und das aus der Mathematik bekannte präzise Arbeiten auf die Software-Entwicklung übertragen. Die Studierenden lernen, warum Kernelemente funktionaler Programmierung, insbesondere die Seiteneffektfreiheit und die starke Typisierung, besonders geeignet sind, Sicherheitsaspekte von Software zu gewährleisten undnachzuweisen.

3.2.1 Funktionale Programmierung

Lehrveranstaltung	Funktionale Programmierung
Dozent(en)	Uwe Schmidt
Hörtermin	2
Art der Lehrveranstaltung	Pflicht
Lehrform / SWS	Vorlesung
ECTS	2.0
Lehr- und Medienform(en)	Tafel, Beamerpräsentation, Handout, Softwaredemonstration

Lernziele

Die Studierenden ...

- lernen fortgeschrittene Techniken der funktionalen Programmierung am Beispiel der Sprache Haskell kennen.
- können mit Funktionen höherer Ordnung, mit generischen Datentypen und Typklassen, mit Funktoren, Monaden, Monoiden und weiteren mathematischen Strukturen umgehen.
- lernen die Software-Realisierung mit eingebetteten problemspezifischen Sprachen kennen.
- stärken die Fähigkeiten in der Modellbildung und Abstraktion.
- lernen die Bezüge zwischen Mathematik und funktionaler Programmierung kennen.
- kennen die Vor- und Nachteile des funktionalen Paradigmas für Anwendungen der IT-Sicherheit.

Inhalt

- Einleitung
  - Grundlegende Konzepte
  - Syntax von Haskell
- Datentypen
  - Einfache Datentypen
  - Produkt- und Summen-Datentypen
  - Listen
  - Funktionen höherer Ordnung für Listen
- Typcheck
- Korrektheitsargumentationen
- Rekursive Datenstrukturen
  - Bäume
- Bedarfsauswertung
  - Unendliche Strukturen
- Funktoren und Monaden
  - Maybe- und Listen-Monade

  - Zustands-Monade und Ein- und Ausgabe
  - weitere Varianten von Monaden
- Fallstudien
  - Eingebettete problemspezifische Sprachen
  - Monadische Parser
- Parallele und nebenläufige Programmierung
- Testen

Literatur

- Uwe Schmidt:
  Funktionale Programmierung,
  Vorlesungsunterlagen im Web: `http://www.fh-wedel.de/si/vorlesungen/fp/fp.html`
- Bird, Richard:
  Introduction to Functional Programming using Haskell,
  2nd Edition Prentice Hall, New Jersey, 1998, ISBN: 0-13-484346-0
- Graham Hutton: Programming in Haskell, Cambridge University Press, 2007, ISBN: 978-0-521-69269-4

3.2.2 Übg. Funktionale Programmierung

Lehrveranstaltung	Übg. Funktionale Programmierung
Dozent(en)	Uwe Schmidt
Hörtermin	2
Art der Lehrveranstaltung	Pflicht
Lehrform / SWS	Übung/Praktikum/Planspiel
ECTS	3.0
Lehr- und Medienform(en)	Tafel, Beamerpräsentation, Handout, studentische Arbeit am Rechner

Lernziele

Ziel der Übung ist das Erlernen des praktischen Anwenden der Methoden und Konzepte aus der Vorlesung.

Inhalt

Praktische Übungen über die Themen

- Rekursion,
- Typisierung,
- Listen und Tuple,
- Funktionen als Daten,
- Funktoren und Monaden,
- Ein-und Ausgabe.

Literatur

- Uwe Schmidt:

Funktionale Programmierung,
Vorlesungsunterlagen im Web: `http://www.fh-wedel.de/si/vorlesungen/fp/fp.html`

- Bird, Richard:
  Introduction to Functional Programming using Haskell,
  2nd Edition Prentice Hall, New Jersey, 1998, ISBN: 0-13-484346-0
- Graham Hutton: Programming in Haskell, Cambridge University Press, 2007, ISBN: 978-0-521-69269-4

3.3 Learning & Softcomputing

M006 Learning & Softcomputing

Studiengang	Master-Studiengang IT-Sicherheit
Modulkürzel	M006
Modulbezeichnung	Learning & Softcomputing
Lehrveranstaltung(en)	`M006a` Learning & Softcomputing
Modulverantwortliche(r)	Prof. Dr. Ulrich Hoffmann
Zuordnung zum Curriculum	Informatik (Master) IT-Sicherheit (Master)
Verwendbarkeit des Moduls	Das Modul ist sinnvoll mit dem Modul „Robotics“ und den grundlegenden Modulen „Einführung in die Robotik“ und „Bildbearbeitung und -analyse“ kombinierbar. Zudem bietet sich ein Zusammenspiel in Richtung Data Sciences an, wenn es mit den grundlegenden Modulen „Grundlagen der Mathematik 2“, „Statistik“ und im Master mit den Modulen „Business Intelligence“, „Multivariate Statistik“ und „Entscheidungsunterstützung“ kombiniert wird.
SWS des Moduls	4
ECTS des Moduls	5
Arbeitsaufwand	Präsenzstudium: 38 Stunden Eigenstudium: 112 Stunden
Voraussetzungen	Voraussetzungen dieses Moduls sind Kenntnisse und praktische Erfahrungen in höheren Programmiersprachen. Außerdem werden mathematische Grundkenntnisse und Kenntnisse der Stochastik erwartet.
Dauer	1 Semester
Häufigkeit	jährlich
Prüfungsformen	Assessment
Anteil an Gesamtnote	5,88
Sprache	deutsch

Lernziele des Moduls

Studierende erwerben Kenntnisse im Bereich des maschinellen Lernens. Sie beherrschen die wesentlichen Techniken, mit deren Hilfe Computersysteme Klassifizierungen und Bewertungen durchführen, und sie können sie nach Einsatzgebiet und Güte bewerten und beurteilen. Sie kennen die Herausforderungen die beim Parametrieren von überwachtem Lernenverfahren bedeutsam sind und können sie praktisch anwenden. Sie sind mit wesentlichen Funktionalitäten gängiger Machine-Learning-Bibliotheken vertraut. Sie sind in der Lage eigenständig Aufgaben des maschinenen Lernens zu analysieren, geeignete Methoden auszuwählen und umzusetzen. Im praktischen Teil erwerben sie zusätzlich die Kompetenz arbeitsteilig in einer kleinen Arbeitsgruppe wissenschaftlich, selbständig an einer umfangreichen Aufgabe Kenntnisse zusammenzutragen und Lösungen zu erarbeiten sowie diese verständlich und strukturiert zu präsentieren.

3.3.1 Learning & Softcomputing

Lehrveranstaltung	Learning & Softcomputing
Dozent(en)	Ulrich Hoffmann
Hörtermin	2
Art der Lehrveranstaltung	Pflicht
Lehrform / SWS	mehrere Veranstaltungsarten
ECTS	5.0
Lehr- und Medienform(en)	Handout

Lernziele

Die Studierenden ...

- besitzen grundlegende Kompetenz zum Verständnis für lernfähige, fehlertolerante Problemlösungsansätze.
- haben die Fähigkeit zur Erkennung und Unterscheidung verschiedener maschineller Lernverfahren und Verarbeitungskonzepte.
- haben grundlegendes Verständnis der Themenkomplex Künstlicher Neuronaler Netze (KNN) sowie der Support Vector Machines (SVM)
- besitzen die Fähigkeit unterschiedlichen Ansätze überwachter und unüberwachter Klassifikationsverfahren und ihre mathematischen Hintergründe zu durchdringen.
- haben die Fähigkeit, eine beispielhafte Implementierung dargestellten theoretischen Konzepten im Rahmen selbständiger, gruppenorientierter Projektarbeit gezielt und strukturiert umzusetzen.
- besitzen die Fähigkeit die von ihnen im Rahmen der Projektarbeit erarbeiteten Sachverhalte zu kondensieren und in angemessenen Vortragsstil und geeigneter Präsentationstechniken nachvollziehbar dazustellen. In freier Diskussion können sie sich über komplexe wissenschaftlichen Sachverhalts auseinandersetzen.

Inhalt

- Einführung, Motivation
- Maschinelles Lernen
- Das Konzept der Neuronalen Netze
  - Grundprinzip
  - Arten von Neuronalen Netzen
  - Einlagige Neuronale Netze
  - Mehrlagige Netze
  - Ein Lernverfahren: Backpropagation
- Das Konzept der Support Vector Machines
  - Grundlagen und Eigenschaften
  - Klassifikation durch Hyperebenen
  - Der Kernel-Trick

  - Aspekte der Implementierung von SVM

- Praktische Projektarbeit in Gruppen zur eigenständigen Implementierung und Untersuchung eines ausgewählten Themenkomplexes.

- Regelmäßige Diskussion der Ergebnisse der Projektarbeit und gruppenweise Abschlusspräsentation.

Literatur

- Kecman: Learning and Softcomputing,
  MIT Press, 2001
- Nauck, Klawonn: Neuronale Netze und Fuzzy-Systeme, R. Kruse,
  Vieweg 1996
- Bishop: Neural Networks for Pattern Recognition,
  Oxford Press 1995
- Sutton, Barto: Reinforcement Learning: An Introduction,
  MIT Press, Cambridge, MA, 1998
- Christianini, Shawe-Taylor: Support Vector Machines, N.,
  Cambridge Press, 2000
- Brause: Neuronale Netze,
  Teubner, 1991

3.4 Workshop Cryptography

M009 Workshop Cryptography

Studiengang	Master-Studiengang IT-Sicherheit
Modulkürzel	M009
Modulbezeichnung	Workshop Cryptography
Lehrveranstaltung(en)	`M009a` Workshop Cryptography
Modulverantwortliche(r)	Prof. Dr. Gerd Beuster
Zuordnung zum Curriculum	Informatik (Master) IT Engineering (Master) IT-Sicherheit (Master)
Verwendbarkeit des Moduls	For this module, basic knowledge of discrete mathematics is required. The students acquire advanced knowledge about the mathematical basis of cryptography and its practical application. This knowledge can be utilized in all fields where cryptography methods are used.
SWS des Moduls	4
ECTS des Moduls	5
Arbeitsaufwand	attendance study: 38 hours self study: 112 hours
Voraussetzungen	Students need the knowledge about discrete mathematics typically acquired in an undergraduate study programme in computer science or a similar field. Students must be familiar with the common Internet protocols. Students must have some basic knowledge in programming.
Dauer	1 semester
Häufigkeit	every year
Prüfungsformen	acceptance test
Anteil an Gesamtnote	0
Sprache	english

Lernziele des Moduls

In the cryptography workshop, students gain knowledge about the mathematical base of cryptography and its practical application. After completing the course, students are able to use cryptographic methods in the context of secure IT systems, and to evaluate the use of cryptographic methods in existing systems.
This covers both software- and hardware-based cryptography. A focus is put on cryptography used on the Internet and for E-Commerce. The students know how to ensure the confidentiality and integrity of personal data and business data by cryptographic means. Based on real world cryptographic systems, students learned that many side conditions have to be taken into account when implementing and using cryptographic methods.

3.4.1 Workshop Cryptography

Lehrveranstaltung	Workshop Cryptography
Dozent(en)	Gerd Beuster
Hörtermin	2
Art der Lehrveranstaltung	Pflicht (M_ITS14.0, M_ITS16.0) Wahl (M_Inf14.0, M_ITE15.0)
Lehrform / SWS	workshop
ECTS	5.0
Lehr- und Medienform(en)	Blackboard, projector presentation, overhead slide presentation, handout, software presentation, student computer exercises, E-Learning

Lernziele

After completing the module, students are able to ...

- use security tools as an essential building block of modern information and communication systems.
- apply their knowledge of all relevant aspects of data, network and web security.
- asses the application of cryptographic methods, especially for authentication, encryption and integrity preservation.
- assess they algorithmic strengths and weaknesses of cryptographic methods.
- assess and implement cryptographic protocols, especially for authentication in e-commerce.
- consider all side conditions relevant for implementation and application of cryptographic methods.
- assess the quality of random number generators.
- assess the suitability of software and hardware cryptography for a given task.

Inhalt

- Theory of Cryptography
  - Semantic Security
  - Unbreakable Encryption and One Time Pad
  - Diffusion and Confusion
- Classic Cryptography
  - Substitution and Transposition
  - Affine Encryption
  - Rotor Machines
- Modern Cryptography
  - Stream and Block Ciphers
  - DES and GOST
  - AES

- Block Cipher Modes of Operation
  - ECB, CBC, CTR, AES-GCM
- Random number generators
  - TRNG and PRNG
  - Requirements for CSPRNG
  - PRNG based on mathematical problems
    - Blum-Blum-Shub
- Hashing
  - Hashing Algorithms
    - SHA 2
    - Keccak
  - Message authentication
    - CMAC and HMAC
- Asymmetric Cryptography
  - Diffie-Hellman
  - RSA
  - Elliptic Curves
  - Asymmetric Encryption and Digital Signatures
- Practical Cryptography: PGP and SSL
- Hardware Cryptography
  - Trusted Computing
  - Smartcards
  - Differential Power Analysis

Literatur

- Stallings, William: Cryptography and Network Security : Principles and Practice. 6. Edition. Harlow, UK: Pearson, 2013.
- Ferguson, Niels; Schneier, Bruce; Kohno, Tadayoshi: Cryptography Engineering : Design Principles and Practical Applications. Indianapolis (IN), USA: Wiley Publishing, 2010.
- Menezes, Alfred J.;van Oorschot, Paul C.; Vanstone, Scott A.: Handbook of Applied Cryptography. Boca Raton (FL), USA: CRC Press, 1996.
- Douglas R. Stinson: Cryptography : Theory and Practice. 3. Edition. Boca Raton (FL), USA: CRC Press, 2005.
- Lawrence C. Washington: Elliptic Curves : Number Theory and Cryptography. 2. Edition. Boca Raton (FL), USA: CRC Press, 2008.
- Joshua Davies: Implementing SSL/TLS Using Cryptography and PKI. Indianapolis (IN), USA: Wiley Publishing, 2011.
- Katz, Jonathan; Lindell, Yehuda: Introduction to Modern Cryptography. Boca Raton (FL), USA: CRC Press, 2007.
- Swenson, Christopher: Modern Cryptanalysis : Techniques for Advanced Code Breaking. Indianapolis (IN), USA: Wiley Publishing, 2008.
- Mao, Wenbo: Modern Cryptography: Theory and Practice, Upper Saddle River (NJ), USA: Prentice Hall, 2003.

3.5 Security Engineering

M019 Security Engineering

Studiengang	Master-Studiengang IT-Sicherheit
Modulkürzel	M019
Modulbezeichnung	Security Engineering
Lehrveranstaltung(en)	`M019a` Security Engineering
Modulverantwortliche(r)	Prof. Dr. Gerd Beuster
Zuordnung zum Curriculum	IT Engineering (Master) IT-Sicherheit (Master)
Verwendbarkeit des Moduls	The module requires basic knowledge in the fields of computer architecture, operating systems, computer networks, and programming. The skills acquired in this module are applicable to all tasks involving software and security engineering.
SWS des Moduls	4
ECTS des Moduls	5
Arbeitsaufwand	attendance study: 38 hours self study: 112 hours
Voraussetzungen	Students must be able to think analytically and to build formal methods. These abilities are typically acquired in an undergraduate study programme in computer science or a similar field. In addition, students must know the general principals of modern computers and operating systems, network technology, and programming.
Dauer	1 semester
Häufigkeit	every year
Prüfungsformen	written or oral examination
Anteil an Gesamtnote	5,88
Sprache	english

Lernziele des Moduls

After completing the module, the students are able to evaluate the security of existing IT systems and to design and implement new, secure IT systems. This module focuses on the engineering aspects of IT security. When the module is completed, the students know the state of the art in secure software, secure hardware, network security and physical security. The students are able to design systems providing adequate security both for personal and business data.

3.5.1 Security Engineering

Lehrveranstaltung	Security Engineering
Dozent(en)	Gerd Beuster
Hörtermin	2
Art der Lehrveranstaltung	Pflicht (M_ITS14.0, M_ITS16.0) Wahl (M_ITE15.0)
Lehrform / SWS	lecture with tutorial, workshop, assignment
ECTS	5.0
Lehr- und Medienform(en)	Blackboard, projector presentation, overhead slide presentation, handout, software presentation, student computer exercises, guest speakers, E-Learning

Lernziele

After completing the module, students are able to ...

- apply the basic concepts of IT Security.
- define and check security requirements for software.
- develop and evaluate secure software.
- assess and evaluate the security of hardware components
- evaluate the security of computer networks
- design secure computer networks.

Inhalt

- Basic Concepts of IT Security
- Threat Modeling
- Threats in Practice
- Security Modeling
- Security Administration and Physical Security
- Operating System Security and Access Rights
- Security Protocols
- Methods for Developing Secure Software
- Typical Attacks on Software Systems
- Distributed Systems / Network Security
- Secure Hardware

Literatur

- Allen, Julia H.; Barnum, Sean; Ellison, Robert J.; McGraw, Gary; Mead, Nancy R.: Software Security Engineering : A Guide for Project Managers. Bosten (MA), USA: Addison Wesley, 2008.
- Anderson, Ross J.: Security Engineering : A Guide to Building Dependable Distributed

Systems. 2. Edition. Hoboken (NJ), USA: Wiley & Sons, 2008.
- Graves, Michael W.: Digital Archaeology : The Art and Science of Digital Forensics. Bosten (MA), USA: Addison Wesley, 2013.
- Pfleeger, Charls P.;Pfleeger, Shari Lawrence: Security in Computing. 4. Edition. München: Prentice Hall, 2012.
- Shimeall, Timothy J.; Spring, Jonathan M.: Introduction to Information Security : A Strategic-based Approach. Amsterdam, NL: Elsevier Syngress, 2013.
- Stallings, William: Computer Security : Principles and Practice. 2. Edition. München: Pearson, 2012.
- Watson, David; Jones, Andrew: Digital Forensics Processing and Procedures. Amsterdam, NL: Elsevier Syngress, 2013.
- Wilhelm, Thomas: Professional Penetration Testing : Creating and Operating a Formal Hacking Lab. 2. Edition. Amsterdam, NL: Elsevier, 2013.

3.6 Seminar (Master)

M023 Seminar (Master)

Studiengang	Master-Studiengang IT-Sicherheit
Modulkürzel	M023
Modulbezeichnung	Seminar (Master)
Lehrveranstaltung(en)	`M023a` Seminar (Master)
Modulverantwortliche(r)	Prof. Dr. Ulrich Raubach
Zuordnung zum Curriculum	Betriebswirtschaftslehre (Master) E-Commerce (Master) Informatik (Master) IT-Sicherheit (Master)
Verwendbarkeit des Moduls	Die Fähigkeit, theoriegestützt zu arbeiten, wird in der Master-Thesis benötigt.
SWS des Moduls	2
ECTS des Moduls	5
Arbeitsaufwand	Präsenzstudium: 20 Stunden Eigenstudium: 130 Stunden
Voraussetzungen	Keine
Dauer	1 Semester
Häufigkeit	jedes Semester
Prüfungsformen	Schriftl. Ausarbeitung (ggf. mit Präsentation)
Anteil an Gesamtnote	5,88
Sprache	deutsch

Lernziele des Moduls

Nach dem Seminar sind die Studierenden in der Lage, anspruchsvolle Themen eigenständig stärker theorieorientiert zu strukturieren und ihre Ausarbeitungen nach wissenschaftlichen Standards zu konzipieren. Im obligatorischen Vortrag können sie ihre Arbeitsergebnisse fundiert darlegen und im Diskurs kristisch diskutieren.

3.6.1 Seminar (Master)

Lehrveranstaltung	Seminar (Master)
Dozent(en)	jeweiliger Dozent
Hörtermin	1
Art der Lehrveranstaltung	Pflicht
Lehrform / SWS	Seminar
ECTS	5.0
Lehr- und Medienform(en)	Tafel, Beamerpräsentation, Handout

Lernziele

Das Seminar dient der Vorbereitung auf die spätere Master-Thesis.
Die Studierenden sind in der Lage, ...

- anspruchsvollere Themen eigenständig stärker theorieorientiert zu strukturieren.
- ihre Ausarbeitungen nach wissenschaftlichen Standards zu konzipieren.
- im obligatorischen Vortrag ihre Arbeitsergebnisse fundiert darzulegen und dabei im Diskurs kristisch zu diskutieren.

Inhalt

Gegenstand dieser Veranstaltung stellen wechselnde Themen aus Forschung und Praxis dar. Die Ergebnisse der Seminararbeiten werden von den Studierenden präsentiert und im Rahmen der abschließenden Diskussion verteidigt.

Literatur

- Zum Einstieg: Grundlagenliteratur der Fachrichtung
- Spezialliteratur: in Abhängigkeit vom gewählten Thema durch eigenständige Recherche.

3.7 Datenbanken 3

M027 Datenbanken 3

Studiengang	Master-Studiengang IT-Sicherheit
Modulkürzel	M027
Modulbezeichnung	Datenbanken 3
Lehrveranstaltung(en)	`M027a` Konzepte der Datenbanktechnologie `M027b` Übg. Konzepte der Datenbanktechnologie
Modulverantwortliche(r)	Prof. Dr. Ulrich Hoffmann
Zuordnung zum Curriculum	E-Commerce (Master) Informatik (Master) IT-Sicherheit (Master)
Verwendbarkeit des Moduls	Das Modul ist sinnvoll im Datenbanken-Curriculum zusammen mit den grundlegenden Modulen „Datenbanken 1“ und „Datenbanken 2“ aber auch den Programmiereinführungsmodulen („Einführung in die Programmierung“, „Programmstrukturen 1“) zu kombinieren. Auch eine Kombination mit dem grundlegenden Modul „Systemmodellierung“ ist ratsam.
SWS des Moduls	4
ECTS des Moduls	5
Arbeitsaufwand	Präsenzstudium: 38 Stunden Eigenstudium: 112 Stunden
Voraussetzungen	Das Modul setzt solide Kenntnisse der Funktionsweise und des Aufbaus relationaler Datenbankmanagementsysteme voraus. Der praktische Anteil erfordert fortgeschrittene Fähigkeiten der objektorientierten Programmierung.
Dauer	1 Semester
Häufigkeit	jährlich
Prüfungsformen	Klausur / Mündliche Prüfung (Teil M027a), Abnahme (Teil M027b)
Anteil an Gesamtnote	5,88
Sprache	deutsch

Lernziele des Moduls

Nach Abschluss des Moduls besitzen die Studierenden fortgeschrittene Kenntnisse über Datenbanksysteme. Sie verfügen dabei über Wissen über relationaler Datenbanksysteme und über Datenbanksysteme, die auf alternativen Ansätzen (objekt-orientiert, objekt-relational, XML, NoSQL, u., a.) basieren. Sie können deren Vor- und Nachteile abwägen. Die Studierenden sind in der Lage, sich kritisch mit den Möglichkeiten moderner Datenbanksysteme auseinanderzusetzen, diese geeignet einzuschätzen und praxisgerecht anzuwenden.

3.7.1 Konzepte der Datenbanktechnologie

Lehrveranstaltung	Konzepte der Datenbanktechnologie
Dozent(en)	Ulrich Hoffmann
Hörtermin	1
Art der Lehrveranstaltung	Pflicht
Lehrform / SWS	Vorlesung
ECTS	3.0
Lehr- und Medienform(en)	Handout

Lernziele

Die Studierenden erlangen die ...

- Kenntnis, der für die Implementierung von Datenbanksystemen wichtigen Architekturprinzipien, Datenstrukturen und Algorithmen und damit Kenntnis des Aufbaus und der internen Arbeit eines großen komplexen Softwaresystems.
- Fähigkeit, die Arbeitsweise von Datenbanksystemen zu optimieren bzw. selbst Architekturen für große komplexe Softwaresysteme zu entwerfen.
- Fähigkeiten eines Datenbankadministrators für Datenbanksysteme.

Inhalt

- Grundlagen objektorientierter Datenbanksysteme
  - Persistenz
  - Transaktionen
  - Anfragen
- Objekt-relationales Mapping
  - Java Persistence API (JPA)
- NoSQL-Datenbanksysteme
  - Verteilte Wert/Schlüssel-Speicher
  - Dokumentendatenbanken
- Konkrete Systeme:
  - Persistente Objekte mit Versant jd4objects
  - Objekt-relationales Mapping mit Hibernate bzw. EclipseLink
  - Dokumentenbasierte Datenhaltung mit CouchDB

Literatur

- GEPPERT, Andreas:
  Objektrelationale und objektorientierte Datenbankkonzepte und -systeme,
  dpunkt.verlag, Heidelberg, 2002
- KEMPER, Alfons; EICKLER, Andre:
  Datenbanksysteme - Eine Einführung.
  Oldenbourg Verlag, 2004
- MEIER, Andreas; WÜST, Thomas:
  Objektorientierte und objektrelationale Datenbanken.
  dpunkt.verlag, Heidelberg, 2000

- JORDAN, David; RUSSEL, Craig:
  Java Data Objects,
  OReilly, Sebastopol, 2003
- KEITH, Mike; SCHINCARIOL, Merrik:
  Pro JPA 2 - Mastering the Java Persistence API.
  APress, 2009
- PATERSON, Jim, et., al.:
  The Definitive Guide to db4o,
  APress, Berkeley, 2006
- BAUER, Christian; KING, Gavin:
  Java Persistence with Hibernate,
  Manning, Greenwich, 2007
- div. Konferenzbeiträge und Forschungsarbeiten zu moderneren Entwicklungen der Datenbanktechnologie

3.7.2 Übg. Konzepte der Datenbanktechnologie

Lehrveranstaltung	Übg. Konzepte der Datenbanktechnologie
Dozent(en)	Ulrich Hoffmann
Hörtermin	1
Art der Lehrveranstaltung	Pflicht
Lehrform / SWS	Übung/Praktikum/Planspiel
ECTS	2.0
Lehr- und Medienform(en)	-

Lernziele

Studierende ...

- beherrschen die Fähigkeit einschlägige Softwaresysteme im Bereich objektorientierter Datenbanken sowie objektrelationaler Datenbanken-Abbildungs-Werkzeuge in Betrieb zu nehmen und sie zur Lösung von Problemen einzusetzen.
- sind mit den praktisch auftretenden Schwierigkeiten vertraut und können sie systematisch überwinden.
- besitzen durch praktischen Einsatz vertieftes Wissen über die spezifischen Eigenschaften objektorientierter Datenbanken sowie objektrelationaler Datenbanken-Abbildungs-Werkzeuge und können sie bewerten und einordnen.

Inhalt

Vorlesungsbegleitende praktische Übungen in der Programmierung von objektorientierten Datenbanksystemen, von objektrelationalen Datenbanken-Abbildungs-Werkzeugen und anderen alternativen Persistenzansätzen.

Literatur

- siehe Vorlesung
- diverse Online-Quellen

3.8 Berechenbarkeit und Verifikation

M029 Berechenbarkeit und Verifikation

Studiengang	Master-Studiengang IT-Sicherheit
Modulkürzel	M029
Modulbezeichnung	Berechenbarkeit und Verifikation
Lehrveranstaltung(en)	`M029a` Berechenbarkeit und Komplexität `M029a` Formale Spezifikation und Verifikation
Modulverantwortliche(r)	Prof. Dr. Sebastian Iwanowski
Zuordnung zum Curriculum	Informatik (Master) IT-Sicherheit (Master)
Verwendbarkeit des Moduls	Das Modul gibt eine Vertiefung der wissenschaftlichen Grundlagen des Informatikstudiums. Es ergänzt auf diese Weise das grundlegendere und anwendungsbezogenere Modul „Algorithmics“, setzt dieses aber nicht voraus.
SWS des Moduls	6
ECTS des Moduls	5
Arbeitsaufwand	Präsenzstudium: 56 Stunden Eigenstudium: 94 Stunden
Voraussetzungen	Vorausgesetzt wird ein sehr gutes mathematisches Grundwissen, insbesondere der Logik und Mengenlehre. Die Teilnehmer sollten mit der Verwendung einer formalen Sprache vertraut sein und entsprechende Formeln verstehen.
Dauer	1 Semester
Häufigkeit	jährlich
Prüfungsformen	Klausur / Mündliche Prüfung
Anteil an Gesamtnote	5,88
Sprache	deutsch/englisch

Lernziele des Moduls

Nach Abschluss des Moduls verfügen die Studierenden über einen theoretisch fundierten und umfassenden Überblick über die Möglichkeiten der Spezifikation von Lösung und Problemen. Sie kennen ferner die Grundlagen der klassischen Spezifikations- und Lösungsmethoden. Außerdem verfügen sie über eine theoretisch fundierte Beurteilungsfähigkeit bezüglich der Grenzen von Berechenbarkeit und effizienter Lösbarkeit.

3.8.1 Berechenbarkeit und Komplexität

Lehrveranstaltung	Berechenbarkeit und Komplexität
Dozent(en)	Sebastian Iwanowski
Hörtermin	1
Art der Lehrveranstaltung	Pflicht
Lehrform / SWS	Vorlesung
ECTS	2.5
Lehr- und Medienform(en)	Handout

Lernziele

Nach Abschluss der Veranstaltung besitzen die Studierenden folgende Kompetenzen:

- Fundierter theoretischer Überblick über die Möglichkeiten des Problemlösens.
- Theoretisch fundierte Kenntnis der Grenzen der Berechenbarkeit und der effizienten Lösbarkeit.
- Kenntnis der Alternativen für die Praxis bei theoretisch unbefriedigenden Resultaten.

Inhalt

- Berechenbarkeit und Nichtberechenbarkeit
  - Präzisierung der Begriffe Problem und Algorithmen für die Theorie der Berechenbarkeit
  - Turingmaschinen im Detail
  - Komplexitätsklassen für Turingmaschinen
  - Beispiele für unentscheidbare Probleme
  - Beweise der Unentscheidbarkeit für ausgewählte Probleme
- NP-vollständige Probleme
  - Historie des P-NP-Problems
  - Beweis der NP-Vollständigkeit von SATISFIABILITY
  - Übersicht über NP-vollständige Probleme
  - Reduktionsmethode zum Beweis von NP-Vollständigkeit mit Beispielen
- Optimierungsaufgaben für NP-vollständige Probleme
  - Lösungstechniken für NP-vollständige Probleme
  - Übersicht über wichtige Anwendungen - Vergleich zu Verfahren der Künstlichen Intelligenz

Literatur

- Hopcroft, John E.; Motwani, Rajeev; Ullman, Jeffrey D.:
  Einführung in die Automatentheorie, Formale Sprachen und Komplexitätstheorie.
  2. überarb. Aufl. München: Addison-Wesley Longman Verlag, 2002.
- Vossen,Gottfried; Witt, Kurt-Ulrich:
  Theoretische Informatik.
  Braunschweig: Verlag Vieweg & Teubner 2004 (3. Auflage), ISBN 978-3528231477
- Wagenknecht, C.:
  Algorithmen und Komplexität,

Fachbuchverlag Leipzig 2003
- Winter, R.:
  Theoretische Informatik,
  Oldenbourg-Verlag München 2002

3.8.2 Formale Spezifikation und Verifikation

Lehrveranstaltung	Formale Spezifikation und Verifikation
Dozent(en)	Ulrich Hoffmann
Hörtermin	1
Art der Lehrveranstaltung	Pflicht
Lehrform / SWS	Vorlesung mit integrierter Übung/Workshop/Assigm.
ECTS	2.5
Lehr- und Medienform(en)	Handout

Lernziele

Die Studierenden ...

- erlangen fundierte Kenntnisse der mathematischen Grundlagen der formalen Spezifikation und Verifikation.
- beherrschen verschiedene Spezifikationsstile.
- bekommen einen Einblick in verschiedene formale Spezifikationssprachen.
- erlangen die Fähigkeit, Spezifikationen systematisch zu konstruieren.
- können mathematische Beweise von Eigenschaften spezifizierte Software-Systeme führen.
- erlangen grundlegende Kenntnisse der Verifikation mit automatischen Beweissystemen.

Inhalt

- Mathematische und logische Grundlagen der Spezifikation und Verifikation; Mengen, Multimengen, Verbände, partielle und totale Funktionen, algebraische Strukturen, Aussagen- und Prädikatenlogik, Modallogik, temporale Logik
- Algebraische Spezifikation; Terme, Gleichungen; Fallbeispiel einer algebraischen Spezifikation; Datenstrukturen, Operationen, Nachweis von Eigenschaften; maschinenunterstütztes Beweisen von Eigenschaften
- Modellorientierte Spezifikation; Fallbeispiel einer modellorientierten Spezifikation
- Konstruktion korrekter Programme aus Spezifikationen
- Aktuelle Spezifikationssprachen im Überblick

Literatur

- BJØRNER, Dines:
  Software Engineering 1.
  Heidelberg: Springer Verlag, 2006
- DILLER, Antoni:
  Z An Introduction to Formal Methods.
  New York: Wiley & Sons, 1994
- EHRICH/GOGOLLA/LIPECK:

Algebraische Spezifikation abstrakter Datentypen.
Stuttgart: Teubner Verlag, 1989

- GOOS, Gerhard:
  Vorlesungen über Informatik Band 1 - Grundlagen und funktionales Programmieren.
  Heidelberg: Springer Verlag, 2005
- LAMPORT, Leslie:
  Specifying Systems.
  Amsterdam: Addison-Wesley, 2002
- SCHÖNING, Uwe:
  Logik für Informatiker.
  Heidelberg: Spektrum Akademischer Verlag, 2000
- WORDSWORTH, J., B.:
  Software Development with Z.
  New York: Addison-Wesley, 1992

3.9 Künstliche Intelligenz

M033 Künstliche Intelligenz

Studiengang	Master-Studiengang IT-Sicherheit
Modulkürzel	M033
Modulbezeichnung	Künstliche Intelligenz
Lehrveranstaltung(en)	`M033a` Methoden der Künstlichen Intelligenz
Modulverantwortliche(r)	Prof. Dr. Gerd Beuster
Zuordnung zum Curriculum	Informatik (Master) IT-Sicherheit (Master)
Verwendbarkeit des Moduls	Das Modul setzt voraus, dass die Studierenden die grundlegenden Algorithmen der Informatik und Grundlagen diskreter algebraischer Strukturen kennen. Die im Modul erworbenen Fähigkeiten können überall dort verwendet werden, wo autonom handelnde Agenten benötigt werden.
SWS des Moduls	4
ECTS des Moduls	5
Arbeitsaufwand	Präsenzstudium: 38 Stunden Eigenstudium: 112 Stunden
Voraussetzungen	Die Studierenden benötigen die in einem Bachelor-Studium der Informatik oder einem ähnlichen Studium erworben Kenntnisse über diskrete algebraische Strukturen und grundlegende Algorithmen der Informatik. Die Studierenden verfügen über Programmierkenntnisse.
Dauer	1 Semester
Häufigkeit	jährlich
Prüfungsformen	Klausur / Mündliche Prüfung
Anteil an Gesamtnote	5,88
Sprache	deutsch/englisch

Lernziele des Moduls

Nach Abschluss des Moduls verfügen die Studierenden über das Wissen über grundsätzliche Verfahrensweisen der Künstlichen Intelligenz im weiteren Sinne. Sie verfügen über einen umfassenden Überblick der theoretischen Grundlagen sowie über ein gutes Verständnis für die Implementierung ausgewählter Verfahren. Der Schwerpunkt liegt hierbei in der symbolischen Künstlichen Intelligenz und Methoden der formalen Logik. Die Studierenden sind in der Lage, Probleme der realen Welt in die Formalismen der klassischen Logiken (Aussagen- und Prädikatenlogik) umzusetzen. Sie kennen die Syntax und Semantiken der klassischen Logiken und die Grenzen der formallogischen Beweisbarkeit. Sie sind mit Methoden des automatischen Schließens vertraut.

3.9.1 Methoden der Künstlichen Intelligenz

Lehrveranstaltung	Methoden der Künstlichen Intelligenz
Dozent(en)	Gerd Beuster
Hörtermin	1
Art der Lehrveranstaltung	Pflicht
Lehrform / SWS	Vorlesung mit integrierter Übung/Workshop/Assigm.
ECTS	5.0
Lehr- und Medienform(en)	Tafel, Beamerpräsentation, Handout, Softwaredemonstration, studentische Arbeit am Rechner, interaktive Entwicklung und Diskussion von Modellen, E-Learning

Lernziele

Die Studierenden sind in der Lage, Probleme der realen Welt in die Formalismen der klassischen Logiken (Aussagen- und Prädikatenlogik) umzusetzen. Sie kennen die Syntax und Semantiken der klassischen Logiken und die Grenzen der formallogischen Beweisbarkeit. Sie sind mit Methoden des automatischen Schließens vertraut.

Inhalt

- Einführung in die Künstliche Intelligenz
- Intelligente Agenten
- Suchverfahren
- Aussagenlogik
- Logikbasierte autonome Agenten
- Prädikatenlogik
- Grenzen der Prädikatenlogik
- Logikprogrammierung
- Prädikatenlogisches Planen

Literatur

- Harrison, John: Handbook of Practical Logic and Automated Reasoning, Cambridge: Cambridge University Press, 2009.
- Mackworth, Alan K.; Poole, David: Artificial Intelligence : Foundations of Computational Agents. Cambridge: Cambridge University Press, 2010.
- Norvig, Peter; Russell, Stuart: Artificial Intelligence : A Modern Approach. 3. Auflage. Upper Saddle River (NJ), USA: Prentice Hall, 2009.
- Schöning, Uwe: Logik für Informatiker, 5. Auflage. Heidelberg: Spektrum Akademischer Verlag, 2000.
- Lipovaca, Miran: Learn You a Haskell for Great Good! San Francisco (CA), USA: No Starch Press, 2012.
- Blackburn, Patrick; Bos, Johan; Striegnitz, Kristina: Learn Prolog Now!. London, UK: College Publications, 2006.

3.10 Distributed Systems

M035 Distributed Systems

Studiengang	Master-Studiengang IT-Sicherheit
Modulkürzel	M035
Modulbezeichnung	Distributed Systems
Lehrveranstaltung(en)	`M035a` Distributed Systems `M035b` Tutorial: Distributed Systems
Modulverantwortliche(r)	Prof. Dr. Ulrich Hoffmann
Zuordnung zum Curriculum	Informatik (Master) IT Engineering (Master) IT-Sicherheit (Master)
Verwendbarkeit des Moduls	The module can well be combined with modules „Funktionale Programmierung“ and „Aktuelle Entwicklungen in der Informatik“ as well as with the „Seminar Master“.
SWS des Moduls	4
ECTS des Moduls	5
Arbeitsaufwand	attendance study: 38 hours self study: 112 hours
Voraussetzungen	The practical exercises assume advanced programming abilities. In addition the module assume solid knowledge of internet arhitecture and structure as well as basic knowledge of enterprise workflow processe organization.
Dauer	1 semester
Häufigkeit	every year
Prüfungsformen	written or oral examination (Teil M035a), acceptance test (Teil M035b)
Anteil an Gesamtnote	5,88
Sprache	english

Lernziele des Moduls

Students gain extended knowledge of technical aspects of distributed systems as well as their area of applications in commercial contexts. They experience and discuss technological inherent problems of distributed systems and thus have the ability to address the challenges of distributet system and to copy with them. They know the architecture and major algorithms in distributetd systems as well as processes in development and administration that lead to successful distributed products. They are able to program distributed systems in different programm paradigms.

3.10.1 Distributed Systems

Lehrveranstaltung	Distributed Systems
Dozent(en)	Ulrich Hoffmann
Hörtermin	1
Art der Lehrveranstaltung	Pflicht
Lehrform / SWS	lecture
ECTS	3.0
Lehr- und Medienform(en)	Handout

Lernziele

The students gain ...

- thorough understanding of principles of distributed applications.
- knowledge in mastering base technologies and current software tools for distributes systems.
- knowledge of state of the are in different application areas such as service mediation and e-commerce.
- knowledge of basic algorithms in distributed systems.
- precise knowledge of current web service architectures.
- practical skills to realize a project.
- distributed programming skills in different paradigms.

Inhalt

- practical examples
- general requirements of distributed systems
- the client server relation and resulting questions
- communications in distributed systems
- naming services
- techniques for concurrency
- remote calls
- alternative paradigms (actor concept, . . .)
- synchronisation of data and processes
- coordination methods
- replication techniques
- WEB services with SOAP and REST
- fault tolerance concepts
- security in distributed systems

- programming with threads
- communication via sockets, structure of clients and servers
- remote procedure call / remote method invocation
- using naming services
- programming WEB services (SOAP, server / client, WSDL, data binding)
- distributed programming with alternate concepts
- programming synchronisation algorithms
- programming distributed election algorithms
- programming of REST based services and clients
- fault tolerant programming in distributed systems

Literatur

- ARMSTRONG, Joe:
  Programming Erlang.
  Pragmatic Programmers, 2007
- ODERSKY, Martin; SPOON, Lex; VENNERS, Bill:
  Programming in Scala.
  Artima Press, Mountain View, 2008
- COULOURIS, George; DOLLIMORE, Jean; KINDBERG, Tim:
  Distributed Systems, Concepts and Design.
  Addison-Wesley, 2011, ISBN 0-1321-4301-1
- TANENBAUM, Andrew; VAN STEEN, Marten:
  Distributed Systems, Priciples and Paradigms.
  Prentice Hall, 2006, ISBN 0-1323-9227-5

3.10.2 Tutorial: Distributed Systems

Lehrveranstaltung	Tutorial: Distributed Systems
Dozent(en)	Ulrich Hoffmann
Hörtermin	1
Art der Lehrveranstaltung	Pflicht
Lehrform / SWS	tutorial/lab/business game
ECTS	2.0
Lehr- und Medienform(en)	-

Lernziele

The students ...

- have the ability to operate typical software systems (middleware) in the area of distributed systems and use them to solve problems.
- are accustomed to problems that occur in reality and are able to overcome these.
- have deep knowledge of the specific properties of distributed systems by practical experience. They can categorize and evaluate these properties.

Inhalt

Lecture accompanying practical exercises in programming distributed systems and their algorithms in different programming paradigms.

Literatur

- c., f. lecture
- numerous online ressources

3.11 Projekt IT-Sicherheit

M047 Projekt IT-Sicherheit

Studiengang	Master-Studiengang IT-Sicherheit
Modulkürzel	M047
Modulbezeichnung	Projekt IT-Sicherheit
Lehrveranstaltung(en)	`M047a` Projekt IT-Sicherheit
Modulverantwortliche(r)	Prof. Dr. Gerd Beuster
Zuordnung zum Curriculum	IT-Sicherheit (Master)
Verwendbarkeit des Moduls	Die Studierenden benötigen Kenntnisse der informatischen Grundlagen, um ein Projekt im Bereich der IT-Sicherheit erfolgreich durchzuführen. Die erworbenen Kenntnisse sind konkret auf Problemstellungen der IT-Sicherheit anwendbar. Darüber hinaus erwerben die Studierenden allgemeine Projektmanagement-Kompetenzen.
SWS des Moduls	4
ECTS des Moduls	5
Arbeitsaufwand	Präsenzstudium: 38 Stunden Eigenstudium: 112 Stunden
Voraussetzungen	Die Studierenden benötigen die in einem Bachelor-Studium der Informatik oder einem ähnlichen Studium erworben Fähigkeit zum analytischen Denken und zur Modellbildung. Weiterhin benötigen die in einem Bachelor-Studium der Informatik oder einem ähnlichen Studium Kenntnisse der Funktionsweise eines modernen Computers und Betriebssystems, der Netzwerktechnik und der Programmierung.
Dauer	1 Semester
Häufigkeit	jährlich
Prüfungsformen	Schriftl. Ausarbeitung (ggf. mit Präsentation)
Anteil an Gesamtnote	5,88
Sprache	deutsch/englisch

Lernziele des Moduls

Nach Abschluss des Moduls verfügen die Studierenden über fortgeschrittene praktische Kenntnisse und Fähigkeiten in der IT-Sicherheit. Sie haben eine Sicherheitsanalyse eines praktisch genutzten IT-Produkts vorgenommen oder ein IT-System mit besonderen Anforderungen an die Sicherheit entwickelt.
Die Studierenden verfügen nach Abschluss des Moduls des Weiteren über soziale Kompetenzen im Bereich Projekt-Management. Die Studierenden sind in der Lage, sich auf die Projektdynamik und auf die kontinuierlichen Veränderungen während der Projektlaufzeit einzustellen. Sie sind in der Lage, Projekte auch im internationalen Kontext zu leiten.

3.11.1 Projekt IT-Sicherheit

Lehrveranstaltung	Projekt IT-Sicherheit
Dozent(en)	Gerd Beuster
Hörtermin	1
Art der Lehrveranstaltung	Pflicht
Lehrform / SWS	Projekt
ECTS	5.0
Lehr- und Medienform(en)	Tafel, Beamerpräsentation, Softwaredemonstration, studentische Arbeit am Rechner, interaktive Entwicklung und Diskussion von Modellen

Lernziele

Die Studierenden ...

- führen über weiterführende theoretische und praktische Kenntnisse in einem ausgewählten Bereich der IT-Sicherheit.
- verfügen über die Fähigkeit, in IT-Sicherheitsprojekten Leitungsfunktionen zu übernehmen.
- sind zur Arbeit in internationalen Teams befähigt.
- können die besonderen Anforderungen von IT-Sicherheitsprojekten im Change Management berücksichtigen.

Inhalt

Die Inhalte variieren von Veranstaltung zu Veranstaltung. Die Themensetzung orientiert sich an aktuellen Produkten und Entwicklungen in der IT-Sicherheit.

Literatur

Themenabhängig

3.12 Security Management

M049 Security Management

Studiengang	Master-Studiengang IT-Sicherheit
Modulkürzel	M049
Modulbezeichnung	Security Management
Lehrveranstaltung(en)	`M049a` Security Management
Modulverantwortliche(r)	Prof. Dr. Gerd Beuster
Zuordnung zum Curriculum	Betriebswirtschaftslehre (Master) IT-Management, -Consulting & -Auditing (Bachelor) IT-Sicherheit (Master) Wirtschaftsingenieurwesen (Master)
Verwendbarkeit des Moduls	Das Modul setzt keine speziellen Kenntnisse voraus, allgemeine Fähigkeiten zum analytischen Denken und zur Modellbildung werden jedoch benötigt. Die im Modul erworbenen Kenntnisse können sowohl im Bereich des Security-Managements als auch in anderen Managementbereichen, insbesondere im Qualitäts-Management, verwendet werden.
SWS des Moduls	4
ECTS des Moduls	5
Arbeitsaufwand	Präsenzstudium: 38 Stunden Eigenstudium: 112 Stunden
Voraussetzungen	Die Studierenden benötigen die in einem Bachelor-Studium der Informatik oder einem ähnlichen Studium erworben Fähigkeit zum analytischen Denken und zur Modellbildung.
Dauer	1 Semester
Häufigkeit	jährlich
Prüfungsformen	Klausur / Mündliche Prüfung
Anteil an Gesamtnote	5,88
Sprache	deutsch/englisch

Lernziele des Moduls

In dem Modul Security Management lernen die Studierenden, IT-Sicherheit im Kontext von Unternehmensstrategien zu bewerten und zu gestalten. Die Studierenden lernen, Sicherheit als ganzheitliches Konzept zu erfassen, das nicht nur Software, sondern auch Hardware sowie administrative und physikalische Aspekte hat. Nach Abschluss des Moduls kennen sie die gesetzlichen und privatwirtschaftlichen Standards der Sicherheitsevaluierung und -zertifizierung. Sie können Sicherheitskonzepten und -richtlinien erstellen und praktisch umsetzen. Sie sind mit den grundlegenden Konzepten des Datenschutzes im nationalen und internationalen Kontext vertraut. Den Studierenden wird die Fähigkeit vermittelt, Management-Aufgaben im Bereich der IT-Sicherheit zu übernehmen und als IT-Sicherheitsmanager zu arbeiten. Sie sind in der Lage, in einem Unternehmen schützenswerte Güter zu identifizieren und die zum Schutz notwendigen administrative Maßnahmen zu entwickeln und umzusetzen. Die Studierenden kennen die Schnittstellen zu und Überschneidungen mit anderen Bereichen des Managements, insbesondere des IT-Managements und des Change Managements.

3.12.1 Security Management

Lehrveranstaltung	Security Management
Dozent(en)	Gerd Beuster
Hörtermin	1
Art der Lehrveranstaltung	Pflicht (B_IMCA16.0, M_ITS14.0, M_ITS16.0) Wahl (M_BWL16.1, M_BWL16.2, M_WIng14.0)
Lehrform / SWS	Vorlesung mit integrierter Übung/Workshop/Assigm.
ECTS	5.0
Lehr- und Medienform(en)	Tafel, Beamerpräsentation, Handout, Softwaredemonstration, interaktive Entwicklung und Diskussion von Modellen, Gastreferenten, E-Learning

Lernziele

In dem Modul Security Management lernen die Studierenden, IT-Sicherheit im Kontext von Unternehmensstrategien zu bewerten und zu gestalten. Den Studierenden wird die Fähigkeit vermittelt, Management-Aufgaben im Bereich der IT-Sicherheit zu übernehmen und als IT-Sicherheitsmanager zu arbeiten.
Sie erlangen die ...

- Fähigkeit, Bedrohungen zu identifizieren und zu modellieren.
- Fähigkeit, Risiken zu bewerten.
- Fähigkeit, die Angemessenheit von Sicherheitsmaßnahmen zu bewerten und angemessene Sicherheitsmaßnahmen zu konzipieren.
- Kenntnis der relevanten Standards und Zertifizierungsschemata im Bereich der IT-Sicherheit
- Fähigkeit, IT-Sicherheit im Zusammenspiel mit organisatorischen und physischen Sicherheitsanforderungen und -maßnahmen zu gewährleisten
- Kenntnisse der Zusammenhänge zwischen Sicherheits- und Qualitätsmanagement

Inhalt

- Einführung in das IT-Security-Management
- Unternehmenssicherheit als ökonomischer Faktor
- Angreifer und Angriffsziele
- Management sicherheitskritischer IT-Projekte
- IT-Grundschutz
- Evaluierungs- und Zertifizierungsschemata in der IT-Sicherheit
- Datenschutz
- Sicherheitstrainings
- Physikalische Sicherheit
- Sicherheitsaudits und Revisionskontrolle
- Sicherheitsmanagement und Qualitätsmanagement

Literatur

- BSI - Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Informationssicherheit und IT-Grundschutz : BSI-Standards 100-1, 100-2 und 100-3. 2. Auflage. Köln : Bundesanzeiger Verlag, 2008.
- Cazemier, Jacques: Information Security Management with ITIL V3. Zaltbommel, NL: Van Haren, 2010.
- Cole, Eric: Advanced Persistent Threat : Understanding the Danger and How to Protect Your Organization. Amsterdam, NL: Elsevier Syngress, 2012.
- Common Criteria for Information Technology Security Evaluation. Version 3.1 Revision 4. CCMB-2012-09-001. September 2012.
- Gantz, Stephen D.: The Basics of IT Audit : Purposes, Processes, and Practical Information. Amsterdam, NL: Elsevier Syngress, 2013.
- Kersten, Heinrich; Klett, Gerhard: Der IT Security Manager. 3. Auflage. Wiesbaden: Springer Vieweg, 2013.
- Smith, Clifton L.; Brooks, David J.: Security Science : The Theory and Practice of Security. Oxford, UK: Butterworth-Heinemann, 2013.
- Snedaker, Susan: IT Security Project Management Handbook. Amsterdam, NL: Elsevier Syngress, 2006.
- Stallings, William: Computer Security : Principles and Practice. 2. Auflage. München: Pearson, 2012.
- Vacca, John R. (Hrsg.): Computer and Information Security Handbook. 2. Auflage. Burlington (MA), USA: Morgan Kaufmann, 2013.
- Watson, David; Jones, Andrew: Digital Forensics Processing and Procedures. Amsterdam, NL: Elsevier Syngress, 2013.

3.13 Master-Thesis

M050 Master-Thesis

Studiengang	Master-Studiengang IT-Sicherheit
Modulkürzel	M050
Modulbezeichnung	Master-Thesis
Lehrveranstaltung(en)	`M050a` Master-Thesis
Modulverantwortliche(r)	jeweiliger Dozent
Zuordnung zum Curriculum	Betriebswirtschaftslehre (Master) E-Commerce (Master) Informatik (Master) IT-Sicherheit (Master) Wirtschaftsingenieurwesen (Master)
Verwendbarkeit des Moduls	Keine.
SWS des Moduls	0
ECTS des Moduls	28
Arbeitsaufwand	Präsenzstudium: 2 Stunden Eigenstudium: 838 Stunden
Voraussetzungen	Voraussetzung für die Master-Thesis ist der Stoff aus den vorangegangenen beiden Semestern, insbesondere der Veranstaltungen, die einen Bezug zur Themenstellung der Arbeit haben.
Dauer	1 Semester
Häufigkeit	jedes Semester
Prüfungsformen	Schriftl. Ausarbeitung (ggf. mit Präsentation)
Anteil an Gesamtnote	32,94
Sprache	deutsch

Lernziele des Moduls

In der Masterthesis zeigen die Studierenden, dass sie in der Lage sind, komplexe Aufgabenstellungen mit wissenschaftlich methodischer Vorgehensweise selbstständig und zielorientiert zu erarbeiten. Sie sind befähigt, Problemstellungen im größeren Kontext zu verorten, die fachlichen Zusammenhänge zu vernetzen und die gewonnenen Erkenntnisse argumentativ überzeugend darzustellen und zu präsentieren.

3.13.1 Master-Thesis

Lehrveranstaltung	Master-Thesis
Dozent(en)	jeweiliger Dozent
Hörtermin	3
Art der Lehrveranstaltung	Pflicht
Lehrform / SWS	Thesis
ECTS	28.0
Lehr- und Medienform(en)	Keine

Lernziele

Die Studierenden sind in der Lage ...

- komplexe Aufgabenstellungen selbständig zu erarbeiten.
- Problemstellungen im größeren Kontext zu verorten.
- wissenschaftliche Methoden für die Problemlösung einzusetzen.
- Ergebnisse überzeugend darzustellen und zu präsentieren.

Inhalt

themenabhängig

Literatur

themenabhängig

3.14 Master-Kolloquium

M058 Master-Kolloquium

Studiengang	Master-Studiengang IT-Sicherheit
Modulkürzel	M058
Modulbezeichnung	Master-Kolloquium
Lehrveranstaltung(en)	`M058a` Kolloquium
Modulverantwortliche(r)	jeweiliger Dozent
Zuordnung zum Curriculum	Betriebswirtschaftslehre (Master) E-Commerce (Master) Informatik (Master) IT-Sicherheit (Master) Wirtschaftsingenieurwesen (Master)
Verwendbarkeit des Moduls	Keine
SWS des Moduls	0
ECTS des Moduls	2
Arbeitsaufwand	Präsenzstudium: 2 Stunden Eigenstudium: 58 Stunden
Voraussetzungen	Zulassungsvoraussetzung zum Kolloquium ist eine mit mindestens “‘ausreichend”’ bewertete Master-Thesis.
Dauer	1 Semester
Häufigkeit	jedes Semester
Prüfungsformen	Kolloquium
Anteil an Gesamtnote	2,35
Sprache	deutsch

Lernziele des Moduls

Die Studierenden präsentieren ihre Arbeitsergebnisse überzeugend vor dem Prüfungsausschuss. Sie beherrschen das Instrument der freien Rede, argumentieren schlüssig und beweisführend. In einer anschließenden fächerübergreifenden mündlichen Prüfung verteidigen sie ihre Arbeitsergebnisse und erweisen sich in der Diskussion als problemvertraut.

3.14.1 Kolloquium

Lehrveranstaltung	Kolloquium
Dozent(en)	verschiedene Dozenten
Hörtermin	3
Art der Lehrveranstaltung	Pflicht
Lehrform / SWS	Kolloquium
ECTS	2.0
Lehr- und Medienform(en)	Tafel, Beamerpräsentation

Lernziele

Die Studierenden ...

- besitzen die Fähigkeit der konzentrierten Darstellung eines intensiv bearbeiteten Facthemas.
- verfestigen die Kompetenz, eine fachliche Diskussion über eine Problemlösung und deren Qualität zu führen.
- verfügen über ausgeprägte Kommunikations- und Präsentationsfähigkeiten.

Inhalt

- Fachvortrag über Thema der Master-Thesis sowie über die gewählte Vorgehensweise und die Ergebnisse
- Diskussion der Qualität der gewählten Lösung
- Fragen und Diskussion zum Thema der Master-Arbeit und verwandten Gebieten

Literatur

themenabhängig