

RUHR-UNIVERSITÄT BOCHUM

FACULTY OF COMPUTER SCIENCE

RUB

Modulhandbuch

für den Masterstudiengang

IT-Sicherheit | Netze und Systeme

STAND 09.06.2023 | PO 22

<https://informatik.rub.de/studium/studiengaenge/its/mnds/>



Faculty of
Computer
Science

www.informatik.rub.de



MODULHANDBUCH

Übersicht der Module

IT-Sicherheit / Informationstechnik - Master (1-Fach, PO 2022)

Wahlpflichtbereich

Aufbau eines Managementsystems für Informationssicherheit nach DIN ISO / 27001

Blockchain Security and Privacy

Developer Centered Security

Human Aspects of Cryptography Adoption

Menschliches Verhalten in der IT-Sicherheit

Message Level Security

Physical Attacks and Countermeasures

Processor Security

Programmanalyse

Software Protection

Software Security

Software-Implementierung kryptographischer Verfahren

Authentische Schlüsselvereinbarung: Formale Modelle und Anwendungen

Deep Learning

Fundamentals of Data Science

Komplexitätstheorie

Kryptographische Protokolle

Proofs are programs

Public Key Kryptanalyse 1

Public Key Verschlüsselung

Quantum Cryptography

Quantum Information and Computation

Symmetrische Kryptanalyse

Ze-ro-Know-ledge Proof Sys-tems

Autonomous Vehicles and Artificial Intelligence

Deterministic Network Caluculus

Effiziente Algorithmen

Embedded Multimedia

Fundamentals of GPU Programming

Information Theory

Knowledge Graphs

Künstliche Neuronale Netze

Machine Learning: Supervised Methods

Nebenläufige Programmierung

Web-Engineering

Praktikum/Projektarbeit

Vertiefungsseminar (M.Sc. IT-Sicherheit)

Wahlbereich

Freie Wahlfächer

Abschlussarbeit

Masterarbeit und Kolloquium (ITS)

Titel des Moduls: Aufbau eines Managementsystems für Informationssicherheit nach DIN ISO / 27001

Modul-Nr./Code	Credits 4 CP	Workload 120 h	Semester	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen 211021: Aufbau eines Managementsystems für Informationssicherheit nach DIN ISO / IEC 27001			Kontaktzeit 45 h	Selbststudium 75 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen Keine		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Professur für Systemsicherheit Lehrende: Dr.-Ing. Sebastian Uellenbeck					
Verwendung des Moduls B.Sc. IT-Sicherheit / Informationstechnik Master IT-Sicherheit Informationstechnik Master IT-Sicherheit Netze und Systeme					
Lernziele (learning outcomes) Die Studierenden haben ein fundiertes Verständnis über den Aufbau eines ISMS nach ISO 27001 und kennen die notwendigen Schritte, um ein Unternehmen zur Zertifizierungsreife zu begleiten. Studierenden können eigenständig neue Probleme analysieren und neue Lösungsmöglichkeiten entwickeln. Sie können mit diesem Verständnis mit ihren Kollegen über ISO/IEC 27001 diskutieren und auftretende Probleme im Gespräch korrekt klassifizieren.					
Inhalt Die Lehrveranstaltung vermittelt fokussiert Inhalte aus der ISO/IEC 27001 Auditorensicht. Dazu ist folgende Gliederung geplant: <ul style="list-style-type: none"> • Zielsetzung • Prinzipien und Terminologien • Auditprinzipien gemäß ISO 19011:2011 Richtlinien • ISO 19011 • ISO 27001:2013 Dokumentation • Auditvorbereitung: Pre-Audit Meeting und Auditpläne • Vorbereitung von Checklisten • Audittechniken • Auditorenpräsentationen • Auditergebnisse und Abschlusstreffen • Abweichungen, Bericht der Beobachtungen und Folgemaßnahmen • Folgemaßnahmen <p>Weitergehend werden technische Lösungsmittel besprochen, die auf dem Weg zur ISO 27001 Zertifizierung hilfreich sein können. Hierzu zählen unter anderem Security Information and Event Management Systeme (SIEM) und Identity Management Systeme (IdM).</p>					
Lehrformen Vorlesung mit Übung (Blockveranstaltung in den Semesterferien Anmeldung über sysec@rub.de)					
Prüfungsformen schriftliche Modulabschlussprüfung (90 Minuten)					
Voraussetzungen für die Vergabe von Credits bestandene schriftliche Modulabschlussprüfung					

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)

4/150: B.Sc. IT-Sicherheit / Informationstechnik [PO 22]

4/149: B.Sc. IT-Sicherheit / Informationstechnik [PO 20]

4/91 Master IT-Sicherheit | Informationstechnik [PO 22]

5/99 Master IT-Sicherheit | Netze und Systeme [PO 20]

Titel des Moduls: Au-then-ti-sche Schlüs-sel-ver-ein-ba-rung: For-ma-le Mo-del-le und An-wen-dun-gen

Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen 211038 - Au-then-ti-sche Schlüs-sel-ver-ein-ba-rung: For-ma-le Mo-del-le und An-wen-dun-gen			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen Keine		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Jörg Schwenk Lehrende: Prof. Dr. Jörg Schwenk					
Verwendung des Moduls M.Sc. IT-Sicherheit Informationstechnik M.Sc. IT-Sicherheit Netze und Systeme					
Lernziele (learning outcomes) Die Studierenden verstehen die Besonderheit kryptographischer Protokolle, bei denen nicht mehr ein Algorithmus im Vordergrund steht, sondern die Interaktion verschiedener Einheiten. Sie kennen die wichtigsten Konzepte bzgl. der beweisbaren Sicherheit von Protokollen. Die wichtigsten Bausteine kryptographischer Protokolle werden behandelt, so dass die Studierenden in der Lage sind, direkt in die wissenschaftliche Literatur zu diesem Thema einzusteigen.					
Inhalt Diese Vorlesung bietet eine Einführung in das Gebiet der kryptographischen Protokolle, die den Einsatz bekannter und neuer Verfahren der Kryptographie in der Kommunikation zwischen mehreren Instanzen beschreibt. Hierbei wird sowohl Wert auf die Beschreibungen als auch auf die Sicherheit gelegt. Die Vorlesung umfasst folgende Themen: • Kryptographische Grundlagen (Kurze Wiederholung der Wahrscheinlichkeitstheorie, Informationstheorie, etc.) • Beweisbare Sicherheit • Analyse von Schlüsselaustauschprotokollen, mit besonderem Fokus auf praktische Beispielprotokolle (wie TLS oder SSH) Die Zusammenstellung ist nicht fest und kann nach Absprache mit den Hörern auch geändert werden.					
Lehrformen Vorlesung mit Übung					
Prüfungsformen schriftlich, 120 Minuten					
Voraussetzungen für die Vergabe von Credits Bestandene Modulabschlussprüfung					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) M.Sc. IT-Sicherheit Informationstechnik (5/91) M.Sc. IT-Sicherheit Netze und Systeme (5/99)					

Titel des Moduls: Autonomous Vehicles and Artificial Intelligence					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Autonomous Vehicles and Artificial Intelligence			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße 25 Studierende
Unterrichtssprache Englisch			Teilnahmevoraussetzungen keine		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Thorsten Berger Lehrende: Prof. Dr. Thorsten Berger, Dr. Sven Peldszus					
Verwendung des Moduls B.Sc. Informatik B.Sc. IT-Sicherheit B.Sc. Angewandte Informatik M.Sc. Informatik M.Sc. Angewandte Informatik M.Sc. IT-Sicherheit/Informationstechnik					
Lernziele (learning outcomes) <ul style="list-style-type: none"> • Understanding requirements on autonomous vehicles • Understanding the architecture of autonomous vehicles • Ability to build a self-driving car with ROS2 • Understanding and applying quality assurance for autonomous vehicles 					
Inhalt Autonomous driving is the future of individual mobility and all major manufacturers are working on fully autonomous vehicles. While there are robust and good solutions for the individual problems in autonomous driving, the main challenge lies in their integration. Altogether, an autonomous vehicle's software is the biggest problem. Therefore, the key in self-driving vehicles is about getting the software right. In this course, we will investigate the different aspects of self-driving vehicles as well as the importance and application of artificial intelligence in this domain. The course will primarily focus on the following topics: <ul style="list-style-type: none"> • Requirements on autonomous vehicles • Architecture of autonomous vehicles • Operation systems and frameworks for robotic systems • Specification and Implementation of autonomous vehicles based on ROS2 • Artificial intelligence for autonomous vehicles • Simulation of autonomous vehicles &#8729; Localization and perception • Mission planning • Quality assurance for autonomous vehicles In the course's lecture, we provide the required theoretical background and practically apply the course's content in exercises by building a self-driving robot. 					
Lehrformen Vorlesung mit Übungen					
Prüfungsformen Mündliche Prüfung					
Voraussetzungen für die Vergabe von Credits Bestandene Modulabschlussprüfung und erfolgreiche Teilnahme an den Übungen					

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)

5/158: B.Sc. Informatik [PO 22]

5/165: B.Sc. Informatik [PO 22]

5/150: B.Sc. IT-Sicherheit/Informationstechnik [PO 22]

5/149: B.Sc. IT-Sicherheit/Informationstechnik [PO 20]

5/168: B.Sc. Angewandte Informatik [PO 22]

5/170: B.Sc. Angewandte Informatik [PO 20]

5/ 97: M.Sc. Informatik

5/105: M.Sc. Angewandte Informatik

5/91: M.Sc. IT-Sicherheit/Informationstechnik [PO 22]

5/84: M.Sc. IT-Sicherheit/Informationstechnik [PO 20]

Titel des Moduls: Blockchain Security and Privacy					
Modul-Nr./Code	Credits 5 CP	Workload 150 Stunden	Semester	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Blockchain security and privacy			Kontaktzeit 4 SWS	Selbststudium	Gruppengröße Studierende
Unterrichtssprache Englisch			Teilnahmevoraussetzungen keine		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Ghassan Karame Lehrende: Prof. Dr. Ghassan Karame					
Verwendung des Moduls Master IT-Sicherheit Informationstechnik Master IT-Sicherheit Netze und Systeme Master Informatik					
Lernziele (learning outcomes) Upon completion of this course, students are expected to be able to: <ol style="list-style-type: none"> 1. Reason about the security and privacy definitions of open payment systems. 2. Explain the security of PoW blockchains in light of the state of the art reported attacks. 3. Reason about possible network security and cryptographic countermeasures to deter attacks on blockchains. 4. Explain best security/privacy practices to strengthen the security of existing blockchains, and extract relevant lessons for the design of next-generation blockchain technologies. 					
Inhalt The main objective of the course is to provide a comprehensive overview of the security and privacy of blockchain technologies. Course participants will be also introduced to the basic security and privacy provisions of existing popular currencies, and will be exposed to the state-of-the-art attacks and threats reported against existing systems/deployments. The participants will also reason on the effectiveness of combining network-level security primitives, with novel cryptographic primitives to deter attacks on payment systems.					
Lehrformen Übung mit Vorlesung					
Prüfungsformen Schriftliche Modulabschlussprüfung (120 Minuten)					
Voraussetzungen für die Vergabe von Credits Erfolgreiches Bestehen der Modulklausur.					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) Master IT-Sicherheit Informationstechnik (5/91) Master IT-Sicherheit Netze und Systeme (5/99) Master Informatik					

Titel des Moduls: Deep Learning					
Modul-Nr./Code	Credits 5 CP	Workload 150 Stunden	Semester	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Deep Learning			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Asja Fischer Lehrende: Prof. Dr. Asja Fischer					
Verwendung des Moduls M.Sc. IT-Sicherheit / Informationstechnik M.Sc. IT-Sicherheit / Netze und Systeme M.Sc. Angewandte Informatik M.Sc. Informatik					
Lernziele (learning outcomes) Die Vorlesung hat das Ziel, einen Einblick in dieses Gebiet zu vermitteln. Zu Beginn werden die grundlegenden Begriffe und Konzepte des maschinellen Lernens eingeführt. Im weiteren Verlauf wird auf verschiedene neuronale Netze, Gradienten-basierte Optimierungsverfahren und generative Modelle eingegangen.					
Inhalt Deep Learning ist ein Untergebiet des maschinellen Lernens, welches in den letzten Jahren zu Durchbrüchen in zahlreichen Anwendungsgebieten (wie z.B. in der Objekt- und Spracherkennung und der maschinellen Übersetzung) geführt hat. Deep Learning Methoden finden unter anderem Anwendung im Bereich IT Security					
Lehrformen Vorlesung und Übung					
Prüfungsformen Schriftliche Modulabschlussprüfung (120 Minuten)					
Voraussetzungen für die Vergabe von Credits Bestandene schriftliche Modulabschlussprüfung.					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) 5/91: M.Sc. IT-Sicherheit / Informationstechnik [PO 22] 5/84: M.Sc. IT-Sicherheit / Informationstechnik [PO 20] 5/99: M.Sc. IT-Sicherheit / Netze und Systeme [PO 22] 5/96: M.Sc. IT-Sicherheit / Netze und Systeme [PO 20] 5/105: M.Sc. Angewandte Informatik 5/ 97: M.Sc. Informatik					

Titel des Moduls: Deterministic Network Caluculus					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Deterministic Network Caluculus (211054)			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Englisch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Steffen Bondorf Lehrende: Prof. Dr. Steffen Bondorf					
Verwendung des Moduls M.Sc. Informatik M.Sc. IT-Sicherheit/Informationstechnik M.Sc. Angewandte Informatik					
Lernziele (learning outcomes) Nach erfolgreichem Abschluss des Moduls werden die Studierenden in der Lage sein, <ul style="list-style-type: none"> • komplexe, vernetzte Systeme als deterministische Warteschlangensysteme zu modellieren, • worst-case Leistungsanalysen von bestehenden Systemen bzw. Modellen durchzuführen, • die Herausforderungen bei der Leistungsdimensionierung von geplanten Systemen zu verstehen, &#8729; dabei die Wirkungsweise zentraler Mechanismen in Computernetzen anhand des Network Calculus zu erklären, • die vorgestellten Verfahren gegeneinander abzugrenzen und auf wissenschaftliche Fragestellungen anzuwenden. 					
Inhalt Verteilte Systeme sind heutzutage allgegenwärtig, und ihre Vernetzung ist von grundlegender Bedeutung für die kontinuierliche Verbreitung und damit Verfügbarkeit von Daten. Die Bereitstellung von Daten in Echtzeit ist einer der wichtigsten nichtfunktionalen Aspekte, den sicherheitskritische Netze gewährleisten müssen. Die formale Verifizierung der Datenkommunikation im Hinblick auf die worst-case Deadlines ist grundlegend für die Zertifizierung von neu entwickelten x-by-Wire-Systemen. Diese Verifizierung erlaubt den Start von Flugzeugen, das Lenken von Autos ohne mechanische Verbindung und den Betrieb sicherheitskritischer Industrieanlagen. Daher wurden verschiedene Methoden für die worst-case Modellierung und Analyse von Echtzeitsystemen entwickelt. Eine davon ist der Deterministische Network Calculus (DNC), eine vielseitige Technik, die in verschiedenen Bereichen wie Paketvermittlung, Task Scheduling, System on Chip, softwaredefinierte Netzwerke, Netzwerke in Rechenzentren und Netzwerkvirtualisierung eingesetzt werden kann. DNC ist eine Methode zur Ableitung deterministischer Schranken für zwei der vorrangigsten Leistungsmetriken in Kommunikationssystemen: <ul style="list-style-type: none"> • die Ende-zu-Ende-Verzögerung von Datenflüssen und • der Speicherplatz, den ein Server benötigt, um alle eingehenden Daten in einer Warteschlange zu puffern. 					
Lehrformen Vorlesung mit Übung					
Prüfungsformen Mündliche Modulabschlussprüfung über 30 Minuten					
Voraussetzungen für die Vergabe von Credits Bestandene mündliche Modulabschlussprüfung.					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) 5/97: M.Sc. Informatik 5/91: M.Sc. IT-Sicherheit/Informationstechnik [PO 22]					

5/84: M.Sc. IT-Sicherheit/Informationstechnik [PO 20]

5/105: M.Sc. Angewandte Informatik

Titel des Moduls: Developer Centered Security					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Developer Centered Security			Kontaktzeit 45 h	Selbststudium 105 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen keine		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Jun.-Prof. Dr. Alena Naiakshina Lehrende: Jun.-Prof. Dr. Alena Naiakshina					
Verwendung des Moduls Master IT-Sicherheit Informationstechnik Master IT-Sicherheit Netze und Systeme					
Lernziele (learning outcomes) Benutzbarkeitsprobleme, Sicherheitsanforderungen und Schwachstellen aktueller Systeme kennen. Methodik zur Untersuchung der Benutzbarkeit von Sicherheitsfunktionalitäten verstehen. Verhaltensstudien mit Softwareentwicklern und Administratoren unter Beachtung der vorgestellten Guidelines durchführen können. Sichere und benutzerfreundliche Systeme für Softwareentwickler und Administratoren entwickeln und beurteilen können.					
Inhalt Softwareentwickler und Administratoren sind häufig keine Sicherheitsexperten. Die von ihnen gebauten Systeme weisen daher oft Sicherheitslücken auf, durch die Millionen Nutzer und vertrauliche Daten gefährdet werden. Wie genau kommt es aber dazu, dass Softwareentwickler und Administratoren solche gravierenden Sicherheitsfehler machen, obwohl es fertige Anwendungsschnittstellen (application programming interface (API)), Programmbibliotheken und Tools gibt, die das Entwickeln und Verwenden von Sicherheitskonzepten erleichtern sollen? Es wird ein Einblick in die Grundlagen der benutzbaren Sicherheit und Privatsphäre sowie aktuelle, sicherheitsrelevante Studien mit Softwareentwicklern und Administratoren gegeben. Die daraus gewonnenen Erkenntnisse werden systematisch aufgearbeitet und dargelegt. Es wird ferner aufgezeigt, was Sicherheitssystemdesigner, Toolentwickler, und Kryptographen beim Entwurf ihrer Systeme beachten sollten, um Softwareentwickler und Administratoren dabei zu unterstützen sicherheitskritische Fehler zu vermeiden. Zudem werden Guidelines zum Durchführen von Studien mit Softwareentwicklern und Administratoren vorgestellt. Dabei wird eine Abgrenzung zu Studien mit Endbenutzern gezogen.					
Lehrformen Vorlesung mit Übung					
Prüfungsformen Schriftliche Modulabschlussprüfung					
Voraussetzungen für die Vergabe von Credits Bestandene Modulabschlussprüfung					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) Master IT-Sicherheit Informationstechnik (5/91) Master IT-Sicherheit Netze und Systeme (5/99)					

Titel des Moduls: Effiziente Algorithmen					
Modul-Nr./Code	Credits 9 CP	Workload 270 h	Semester	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Effiziente Algorithmen (150320 + 150321)			Kontaktzeit 90 h	Selbststudium 180 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: PD Dr. Daniela Kacso Lehrende: PD Dr. Daniela Kacso					
Verwendung des Moduls M.Sc. Angewandte Informatik M.Sc. IT-Sicherheit/Informationstechnik					
Lernziele (learning outcomes) Nach dem erfolgreichen Abschluss des Moduls: Die Studierenden <ul style="list-style-type: none"> • kennen, wählen aus und nutzen grundlegende Datenstrukturen und Graphenalgorithmen • sind in der Lage Analysetechniken (Korrektheitsbeweise und Laufzeitanalyse) zu erläutern und zu beurteilen • können auch bei praktischen Problemen entscheiden, welche der vermittelten Methoden/Algorithmen/Datenstrukturen anwendbar sind und diese nach Effizienz (insb. Laufzeit der Algorithmen) bewerten • können konkrete Anwendungsprobleme modellieren und bei Bedarf diese Algorithmen weiter entwickeln 					
Inhalt Die Lehrveranstaltung kann sowohl in das Gebiet der praktischen als auch in das Gebiet der theoretischen Informatik eingeordnet werden. Die zentralen Themen sind die Folgenden: <ul style="list-style-type: none"> • Berechnung kürzester Pfade in Digraphen • Berechnung eines maximalen Flusses in einem Transportnetzwerk • Berechnung einer optimalen Lösung bei einem Zuordnungsproblem (auch Matching-Problem genannt) Darüberhinaus beschäftigen wir uns mit Anwendungen dieser grundlegenden Probleme.					
Lehrformen Vortrag der Lehrenden in der Vorlesung, Gruppenarbeit in den Übungen					
Prüfungsformen Schriftliche Modulabschlussprüfung (120 Minuten)					
Voraussetzungen für die Vergabe von Credits Bestandene schriftliche Modulabschlussprüfung					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) 9/105: M.Sc. Angewandte Informatik 9/91: M.Sc. IT-Sicherheit/Informationstechnik [PO 22] 9/84: M.Sc. IT-Sicherheit/Informationstechnik [PO 22]					

Titel des Moduls: Embedded Multimedia					
Modul-Nr./Code	Credits 6 CP	Workload 180 h	Semester	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Embedded Multimedia			Kontaktzeit 60 h	Selbststudium 120 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen Keine		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr.-Ing. Rainer Martin Lehrende: Dr. Wolfgang Theimer					
Verwendung des Moduls Master IT-Sicherheit Informationstechnik					
Lernziele (learning outcomes) Die Studierenden erwerben grundlegende Fertigkeiten für das Systemdesign, die Implementierung, sowie die Integrations- und Testphase von Multimedialösungen im Bereich Embedded Systems. Sie sind befähigt, Hardware- und Softwarearchitekturen von eingebetteten Multimediasystemen zu bewerten. Sie sammeln anhand einer Linux-basierten Plattform Programmiererfahrungen und lösen in einem Projektteam eine Aufgabe aus dem Bereich der Multimediakommunikation.					
Inhalt Die Lehrveranstaltung vermittelt die Grundlagen zur Durchführung von Entwicklungsarbeiten im Bereich der eingebetteten Systeme, und hat den Fokus Multimediatechnologien. Zu Beginn der Vorlesung wird eine kurze Einführung in die Entwicklungsprozesse wie System-Engineering, Softwareentwicklung und Testvorgehen gegeben, um die Projektteams methodisch vorzubereiten. Anschließend werden grundlegende Hardware- und Softwarearchitekturen von Embedded Systems präsentiert, um sie zu befähigen, Lösungskonzepte einordnen zu können. Der Fokus der Lehrveranstaltung liegt danach in der detaillierten Analyse einer eingebetteten Plattform am Beispiel des Raspberry Pi. Die Nutzung der Prozessorplattform und der Peripheriekomponenten wird anhand der plattformübergreifenden Entwicklungsumgebung Qt Creator unter C/C++ vertieft. Im Rahmen der praktischen Umsetzung in einem Projektteam erwerben die Studierenden die Fähigkeiten, gemeinsam ein Entwicklungsproblem zu strukturieren, ein Lösungskonzept zu entwickeln, und unter Zuhilfenahme von existierenden Softwaremodulen zu einer Gesamtlösung zu integrieren. Die Herangehensweise an die Problemstellung und die Lösung sind vom Projektteam zu dokumentieren und abschließend allen Teilnehmern zu präsentieren.					
Lehrformen Vorlesung mit integrierten Übungen					
Prüfungsformen schriftlich, 120 Minuten					
Voraussetzungen für die Vergabe von Credits Praxisprojekt - Mündliche Prüfung					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) Master IT-Sicherheit Informationstechnik (6/91)					

Titel des Moduls: Fundamentals of Data Science					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen 141213 - Fundamentals of Data Science			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr.-Ing. Aydin Sezgin Lehrende: Prof. Dr.-Ing. Aydin Sezgin					
Verwendung des Moduls M.Sc. IT-Sicherheit Informationstechnik M.Sc. Informatik					
Lernziele (learning outcomes)					
Inhalt Die Modulnote setzt sich aus zwei Anteilen zusammen: 1. Note der mündlichen Pruefung (36 %) 2. Note der Ausarbeitung eines wissenschaftlichen Artikels und des dazugehoerigen Vortrags (64 %) Ausarbeitung: Für die Ausarbeitung sollte eine LaTeX-Vorlage (z.B. IEEEtran mit DIN A4, zweispaltiger Text) benutzt werden und 2 Seiten nicht überschreiten. Vortrag: Die Dauer des Vortrags ist 20 Minuten mit einer anschließenden Fragen- und Diskussionsrunde von 5-10 Minuten. Es ist empfehlenswert, den Vortrag allgemein verständlich zu halten. Backup-Folien werden empfohlen. Sprache: Der Vortrag kann wahlweise in Deutsch oder Englisch sein.					
Lehrformen Vorlesung mit Übung					
Prüfungsformen mündlich (30 min), Anmeldung: FlexNow Termin und Raum nach Absprache mit dem Dozenten					
Voraussetzungen für die Vergabe von Credits Bestandene Modulabschlussprüfung					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) 5/91 M.Sc. IT-Sicherheit Informationstechnik [PO22] M.Sc. Informatik [PO23]					

Titel des Moduls: Fundamentals of GPU Programming Fundamentals of GPU Programming					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Fundamentals of GPU Programming (141374)			Kontaktzeit 45 h	Selbststudium 105 h	Gruppengröße Studierende
Unterrichtssprache Englisch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Dr. Denis Eremin Lehrende: Dr. Denis Eremin					
Verwendung des Moduls M.Sc. Angewandte Informatik M.Sc. IT-Sicherheit/Informationstechnik					
Lernziele (learning outcomes) Die Studierenden erlernen das Programmieren auf Grafikprozessoren (GPUs)					
Inhalt Zu einem bestimmten Zeitpunkt um 2003 stieg die Rechenleistung nicht auf Kosten der Taktfrequenz des Prozessors, sondern durch Erhöhung der Anzahl der auf dem Prozessorchip zugewiesenen Rechenkern. Grafikprozessoren (GPUs) sind die Meister dieser Computer-Hardware-Entwicklung und bieten bis zu Zehntausende einzelner Kerneinheiten. Gleichzeitig wird das GPU-Speichersystem nicht so sehr durch die Kompatibilitätsanforderungen mit älteren Generationen eingeschränkt wie CPU-Speichersysteme. Deswegen zeigen GPUs im Vergleich zu ihren älteren "Bruder" -Zentraleinheiten (CPUs) eine deutlich bessere Rohleistung der Recheneinheiten und des Speichersystems. Ursprünglich für Videobearbeitungsaufgaben entwickelt, wird die enorme Rechenleistung moderner GPUs üblicherweise zur Unterstützung von CPUs oder zur Lösung einer Vielzahl von Rechenproblemen mit (massiv) parallelisierbaren Teilen verwendet, wodurch Teraflops-hohe Rechenleistung kann schon auf Laptop- / Desktop-Computers erzielt werden. Der vorliegende Kurs zeigt, wie CUDA C (Erweiterung der C-Sprache für die GPU-Programmierung) und das entsprechende (sehr flexible!) CUDA-Laufzeit-API-Framework verwendet werden kann, um die Ausführung einiger typischer Programmiermuster um einen Faktor von 10 oder mehr zu beschleunigen das der CPU. Ausgehend vom CUDA-Programmiermodell geht man zum CUDA-Ausführungsmodell über und betrachtet grundlegende konzeptionelle, Software- und Hardwareprobleme, die zum Verständnis der Funktionsweise von GPUs beitragen. Fallstudien zu mehreren Problemen mit massiv parallelen Algorithmen, die in GPUs implementiert sind, werden ebenfalls weiter ausgeführt. Das theoretische Wissen, das in den Vorlesungen vermittelt wird, wird durch eine Vielzahl von praktischen Beispielen untermauert, an denen die SchülerInnen zu Hause arbeiten können.					
Lehrformen Vorlesung mit Übung					
Prüfungsformen Semesterbegleitend: Projektarbeit und schriftliche Prüfung					
Voraussetzungen für die Vergabe von Credits Bestehen der Projektarbeit und der schriftlichen Prüfung					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) 5/105: M.Sc. Angewandte Informatik 5/91: M.Sc. IT-Sicherheit/Informationstechnik [PO 22] 5/84: M.Sc. IT-Sicherheit/Informationstechnik [PO 20]					

Titel des Moduls: Human Aspects of Cryptography Adoption					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Human Aspects of Cryptography Adoption			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße 30 Studierende
Unterrichtssprache Englisch			Teilnahmevoraussetzungen Keine		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Martina Angela Sasse Lehrende: Prof. Dr. Martina Angela Sasse					
Verwendung des Moduls Master IT-Sicherheit Informationstechnik Master IT-Sicherheit Netze und Systeme					
Lernziele (learning outcomes) The aim of the lecture is to examine the reasons why <ol style="list-style-type: none"> 1. cryptographic solutions – which experts agree offer good protection against most of the common attacks today – are not adopted by most individuals and organisations, and 2. end-users, developers and system administrators who do use cryptographic solutions in some form frequently make mistakes that undermine the security protection. 					
Inhalt In 1999, Whitten & Tygar's seminal USENIX paper "Why Johnny Can't Encrypt" established that people cannot use PGP encryption correctly, even with a graphical user interface and instruction. Over the past 20 years, there has been a string of Johnny papers on studies trying to encourage adoption or correct usage. The aim of this CASA lecture is to systematically examine the results of these studies and identify effective ways of promoting adoption and enable correct use of cryptography. <ul style="list-style-type: none"> • Usability, utility and technology adoption • Security threat models and people's mental models • Complexity or simplicity – who needs to know what? • Designing frictionless user journeys • Methods for testing and tweaking 					
Lehrformen Vorlesung mit Übung					
Prüfungsformen Mündliche Prüfung					
Voraussetzungen für die Vergabe von Credits Bestandene Modulabschlussprüfung					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) Master IT-Sicherheit Informationstechnik (5/91) Master IT-Sicherheit Netze und Systeme (5/99)					

Titel des Moduls: Information Theory					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Information Theory			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Englisch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Michael Walter Lehrende: Prof. Dr. Michael Walter					
Verwendung des Moduls B.Sc. Informatik B.Sc. IT-Sicherheit M.Sc. Informatik M.Sc. IT-Sicherheit / Informationstechnik M.Sc. IT-Sicherheit / Netze und Systeme M.Sc. Angewandte Informatik					
Lernziele (learning outcomes) You will learn fundamental concepts, algorithms, and results in information theory. After successful completion of this course, you will know the mathematical model of information theory, how to design and analyze algorithms for a variety of information processing tasks, and how to implement them in Python. You will have independently read about a topic in information theory and presented it to your peers. You will be prepared for an advanced course or a research or thesis project in this area. Please see the course homepage for a precise list of learning objectives.					
Inhalt This course will give an introduction to information theory – the mathematical theory of information. Ever since its inception, information theory has had a profound impact on society. It underpins important technological developments, from reliable memories to mobile phone standards, and its versatile mathematical toolbox has found use in computer science, machine learning, physics, electrical engineering, mathematics, and many other disciplines. Starting from probability theory, we will discuss how to mathematically model information sources and communication channels, how to optimally compress information, and how to design error-correcting codes that allow us to reliably communicate over noisy communication channels. We will also see how techniques used in information theory can be applied more generally to make predictions from noisy data.					
Tentative syllabus: - Welcome, Introduction to Information Theory - Probability Theory Refresher - Numerical Random Variables, Convexity and Concavity, Entropy - Symbol Codes: Lossless Compression, Huffman Algorithm - Block Codes: Shannon's Source Coding Theorem, its Proof, and Variations - Stream Codes: Lempel-Ziv Algorithm					

- Stream Codes: Arithmetic Coding
- Joint Entropies & Communication over Noisy Channels
- Shannon's Noisy Coding Theorem
- Proof of the Noisy Coding Theorem
- Proof of the Converse, Shannon's Theory vs Practice
- Reed-Solomon Codes
- Message Passing for Decoding and Inference, Outlook
- Student Presentations

Please see the course homepage https://qi.rub.de/it_ss23 for more information.

Lehrformen

Lecture with Exercise

Prüfungsformen

Wird noch nachgeliefert

Voraussetzungen für die Vergabe von Credits

Passed Exam.

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)

5/158: B.Sc. Informatik [PO 22]

5/170: B.Sc. Informatik [PO 20]

5/150: B.Sc. IT-Sicherheit [PO 22]

5/149: B.Sc. IT-Sicherheit [PO 20]

5/97: M.Sc. Informatik

5/91: M.Sc. IT-Sicherheit / Informationstechnik [PO 22]

5/84: M.Sc. IT-Sicherheit / Informationstechnik [PO 20]

5/99: M.Sc. IT-Sicherheit / Netze und Systeme [PO 22]

5/105: M.Sc. Angewandte Informatik

Titel des Moduls: Knowledge Graphs

Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Knowledge Graphs			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Englisch			Teilnahmevoraussetzungen		

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Jun.-Prof. Maribel Acosta Deibe
Lehrende: Jun.-Prof. Maribel Acosta Deibe

Verwendung des Moduls

M.Sc. Informatik

M.Sc. Angewandte Informatik

M.Sc. IT-Sicherheit | Informationstechnik

Lernziele (learning outcomes)

In this lecture, students will learn about the foundations of modelling, querying, publishing, and reasoning over KGs. The topics will be complemented with exercises and Jupyter Notebooks (<https://jupyter.org/>) to show how KG technologies work in practice.

Inhalt

Knowledge Graphs (KG) allow for representing inter-connected facts or statements annotated with semantics. In KGs, concepts and entities are typically modeled as nodes while their connections are modeled as directed and labeled edges, creating a graph. In recent years, KGs have become core components of modern data ecosystems. KGs, as building blocks of many Artificial Intelligence approaches, allow for harnessing and uncovering patterns from the data. Currently, KGs are used in the data-driven business processes of multinational companies like Google, Microsoft, IBM, eBay, and Facebook. Furthermore, thousands of KGs are openly available on the web following the Linked Data (<https://lod-cloud.net/>) principles. The specific topics covered in the lecture are as follows:

1. Introduction to Knowledge Graphs
2. The Resource Description Framework (RDF)
3. RDF Schema (RDFS)
4. The SPARQL Query Language
5. Semantics of SPARQL
6. Linked Data: Knowledge Graphs and Ontologies on the Web
7. The Web Ontology Language (OWL)
8. Entailment Regimes
9. Reasoning over Knowledge Graphs
10. Property Graphs
11. Knowledge Graph Applications

Lehrformen

Lecture with Exercise

Prüfungsformen

Written Exam (120 minutes)

Voraussetzungen für die Vergabe von Credits

Passed written Exam.

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)

5/97: M.Sc. Informatik

5/105: M.Sc. Angewandte Informatik

5 /91 M.Sc. IT-Sicherheit | Informationstechnik

Titel des Moduls: Komplexitätstheorie Complexity Theory					
Modul-Nr./Code	Credits 9 CP	Workload 270 h	Semester	Turnus Unregelmäßig (i.d.R Sommersemester)	Dauer 1 Semester
Lehrveranstaltungen Komplexitätstheorie			Kontaktzeit 90 h	Selbststudium 180 h	Gruppengröße Studierende
Unterrichtssprache Englisch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Thomas Zeume Lehrende: Prof. Thomas Zeume					
Verwendung des Moduls M.Sc. Informatik M.Sc. Angewandte Informatik					
Lernziele (learning outcomes) Die Studierenden lernen, algorithmische Probleme bezüglich ihrer Komplexität einzuordnen und so geeignete algorithmische Techniken zu ihrer Lösung zu identifizieren. Sie können insbesondere algorithmische Methoden für NP-vollständige Probleme anwenden. Sie können mit unterschiedlichen Berechnungsmodellen umgehen und sind in der Lage, einfache Aussagen über sie zu beweisen. Sie lernen im Diskurs eigene und fremde Lösungsansätze zu bewerten.					
Inhalt Die Komplexitätstheorie untersucht und klassifiziert Berechnungsprobleme bezüglich ihrer algorithmischen Schwierigkeit. Ziel ist es, den inhärenten Ressourcenverbrauch bezüglich verschiedener Ressourcen wie Rechenzeit oder Speicherplatz zu bestimmen, und Probleme mit ähnlichem Ressourcenverbrauch in Komplexitätsklassen zusammenzufassen. Die bekanntesten Komplexitätsklassen sind sicherlich P und NP, die die in polynomieller Zeit lösbaren bzw. verifizierbaren Probleme umfassen. Die Frage, ob P und NP verschieden sind, wird als eine der bedeutendsten offenen Fragen der theoretischen Informatik, ja sogar der Mathematik, angesehen. P und NP sind jedoch nur zwei Beispiele von Komplexitätsklassen. Andere Klassen ergeben sich unter anderem bei der Untersuchung der des benötigten Speicherplatzes, der effizienten Parallelisierbarkeit von Problemen, der Lösbarkeit durch zufallsgesteuerte Algorithmen, und der approximativen Lösbarkeit von Problemen. Die Vorlesung hat das Ziel, einen breiten Überblick über die grundlegenden Konzepte und Resultate der Komplexitätstheorie zu geben: <ul style="list-style-type: none"> • Klassische Resultate für Platz- und Zeitkomplexitätsklassen: z.B. die Korrespondenz zwischen Spielen und Speicherplatz-Beschränkungen, der Nachweis, dass sich mit mehr Platz oder Zeit auch mehr Probleme lösen lassen, weitere grundlegende Beziehungen zwischen Zeit- und Platzbasierten Klassen, und die Komplexitätswelt zwischen NP und PSPACE • Grundzüge der Komplexitätstheorie paralleler, zufallsbasierter und approximativer Algorithmen • Einführung in ausgewählte neuere Themen: Komplexitätstheorie des interaktiven Rechnens, des probabilistischen Beweisens und Fine-grained Complexity. 					
Lehrformen Vorlesung mit Übungen					
Prüfungsformen Abschlussprüfung; mündlich, 20-30min					
Voraussetzungen für die Vergabe von Credits Bestandene mündliche Modulabschlussprüfung					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) 9/105: M.Sc. Angewandte Informatik [PO22]					

9/97: M.Sc. Informatik [PO 23]

9/91: M.Sc. IT-Sicherheit | Informationstechnik [PO 22]

9/99: M.Sc. IT-Sicherheit | Netze und Systeme [PO22]

Titel des Moduls: Kryptographische Protokolle					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Kryptographische Protokolle			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Englisch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Eike Kiltz Lehrende: Prof. Dr. Eike Kiltz					
Verwendung des Moduls M.Sc. IT-Sicherheit / Informationstechnik M.Sc. IT-Sicherheit / Netze und Systeme M.Sc. Angewandte Informatik					
Lernziele (learning outcomes) - Vertiefung des Verständnisses für beweisbare Sicherheit - Schreiben von fehlerfreien Sicherheitsreduktionen - Neue Techniken für Sicherheitsbeweise - Erlernen fortgeschrittener kryptographischer Konstruktionen					
Inhalt Die Vorlesung beschäftigt sich mit erweiterten kryptographischen Protokollen und deren Anwendungen. Themenübersicht: <ul style="list-style-type: none"> • Game-based security definitions and proofs • Bilinear maps • Digital Signatures • Identification Protocols • Zero-Knowledge Proofs • Identity-based Encryption • CCA-secure encryption 					
Lehrformen Vorlesung mit Übung					
Prüfungsformen Mündliche (30 Minuten) oder schriftliche Modulabschlussprüfung (120 Minuten)					
Voraussetzungen für die Vergabe von Credits Bestandene Modulabschlussprüfung.					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) 5/91: M.Sc. IT-Sicherheit / Informationstechnik [PO 22] 5/84: M.Sc. IT-Sicherheit / Informationstechnik [PO 20] 5/99: M.Sc. IT-Sicherheit / Netze und Systeme [PO 22] 5/96: M.Sc. IT-Sicherheit / Netze und Systeme [PO 20] 5/105: M.Sc. Angewandte Informatik					

Titel des Moduls: Künstliche Neuronale Netze Artificial Neural Networks					
Modul-Nr./Code	Credits 6 CP	Workload 180 h	Semester siehe Prüfungsordnung	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Artificial Neural Networks (212006)			Kontaktzeit 60 h	Selbststudium 120 h	Gruppengröße 150 Studierende
Unterrichtssprache Englisch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Sen Cheng Lehrende: Prof. Dr. Sen Cheng					
Verwendung des Moduls B.Sc. Angewandte Informatik B.Sc. Informatik M.Sc. IT-Sicherheit / Informationstechnik					
Lernziele (learning outcomes) Die mathematischen Grundlagen, Möglichkeiten und Beschränkungen überwachter Lernverfahren für Regression und Klassifikation mit künstlichen neuronalen Netzen (KNN), sowie für deren Anwendung erforderliche praktische Kenntnisse werden vermittelt. Nach dem erfolgreichen Abschluss des Moduls <ul style="list-style-type: none"> • verstehen Studierende die theoretisch-mathematischen Grundlagen von KNN im Kontext des überwachten Lernens. • können Studierende selbstständig zwischen verschiedenen KNN unterscheiden und in einer Anwendungssituation das geeignete Verfahren auswählen. • können Studierende grundlegende Verfahren selbstständig in einer höheren Programmiersprache implementieren, sowie ihre eigene Implementierung und Standard- Implementierung anderer auf Daten anwenden. • können Studierende Ergebnis der KNN selbstständig interpretieren, insbesondere erkennen, wann sie unrealistisch sind. 					
Inhalt Verfahren: Struktur von Optimierungsproblemen, Regression, logistische Regression, biologische neuronal Netze, Modellselektion, universelle Approximationstheorem, Perzeptron, mehr-schichtiges Perzeptron, Backpropagation, tiefe neuronale Netze, rekurrente neuronale Netze, Long-Short Term Memory, Hopfield Netze, Botzmann-Machine Software: python, numpy, matplotlib, scikit-learn, tensorflow					
Lehrformen Vorlesung, Hausaufgaben, angeleitete Übungen am Computer					
Prüfungsformen Schriftliche Modulabschlussprüfung (120 Minuten)					
Voraussetzungen für die Vergabe von Credits Bestandene schriftliche Modulabschlussprüfung					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) 6/168: B.Sc. Angewandte Informatik [PO 22] 6/170: B.Sc. Angewandte Informatik [PO 20]					

6/158: B.Sc. Informatik [PO 22]

6/170: B.Sc. Informatik [PO 20]

6/91: M.Sc. IT-Sicherheit / Informationstechnik [PO 22]

6/84: M.Sc. IT-Sicherheit / Informationstechnik [PO 20]

Titel des Moduls: Machine Learning: Supervised Methods

Modul-Nr./Code	Credits 6 CP	Workload 180 Stunden	Semester	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Machine Learning: Supervised Methods			Kontaktzeit 60 h	Selbststudium 120 h	Gruppengröße 80 Studierende
Unterrichtssprache Englisch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Tobias Glasmachers Lehrende: Prof. Dr. Tobias Glasmachers					
Verwendung des Moduls Master Informatik Master Angewandte Informatik Master IT-Sicherheit/ Informationstechnik					
Lernziele (learning outcomes) Internationalisierung: Die Veranstaltung wird auf Englisch durchgeführt. Digitalisierung: Inhalte werden durch Videos und Lesematerial vermittelt. Übungsaufgaben mit Programmieranteilen werden in Form von Jupyter-Notebooks bereitgestellt. Nach dem erfolgreichen Abschluss des Moduls <ul style="list-style-type: none">• verstehen die Teilnehmer die Grundlagen der statistischen Lerntheorie• kennen die Teilnehmer die wichtigsten Algorithmen des überwachten statistischen Lernens und können diese auf Lernprobleme anwenden,• kennen die Teilnehmer Stärken und Beschränkungen verschiedenen Lernverfahren,• können die Teilnehmer Standardsoftware zum maschinellen Lernen zur Lösung neuer Probleme einsetzen.					
Inhalt Grundlagen der statistischen Lerntheorie, Querschnitt der wichtigsten Algorithmen des maschinellen Lernens, konkrete Problemlösung mit Standardsoftware					
Lehrformen flipped classroom					
Prüfungsformen Abschlussprüfung; Klausur 90 Minuten,					
Voraussetzungen für die Vergabe von Credits Bestandene schriftliche Modulabschlussprüfung					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) 6/105: M.Sc. Angewandte Informatik 6/97: M.Sc. Informatik 6/91: M.Sc IT-Sicherheit Informationstechnik					

Titel des Moduls: Menschliches Verhalten in der IT-Sicherheit					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen 211033: Menschliches Verhalten in der IT-Sicherheit			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen Keine		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Martina Angela Sasse Lehrende: Prof. Dr. Martina Angela Sasse M. Sc. Jonas Hielscher					
Verwendung des Moduls Master ITS Netze und Systeme Master ITS Informationstechnik					
Lernziele (learning outcomes) Die Veranstaltung vermittelt theoretische und praktische Kenntnisse über Forschungs- und Methoden im Bereich usable Security mit einem besonderen Schwerpunkt auf Laborstudien. Es werden theoretische Kenntnisse vermittelt, auf deren Grundlage die Studierenden selbstständig eine Laborstudie planen und umsetzen und auf diese Weise praktische Kenntnisse erwerben sollen.					
Inhalt In <i>Menschliches Verhalten in der IT-Sicherheit</i> lernt ihr, welche Faktoren Einfluss auf das Sicherheitsverhalten von Angestellten in Unternehmen und Nutzenden im Alltag nehmen, und welche Möglichkeiten bestehen, dieses zu beeinflussen und verändern. Außerdem wird vermittelt, warum bestehende Ansätze des Information Security Management (auch nach ISO 27000) in der Praxis oft nicht funktionieren und wie wir sie erweitern bzw. anpassen sollten. Studierende werden befähigt IT-Sicherheit in Organisationen aus einem ganzheitlichen Ansatz heraus zu betrachten, was unter anderem zwingend erforderlich ist um später Sicherheitsführungsaufgaben wahrzunehmen. Die Vorlesungsinhalte sind dabei umfangreich mit Erfahrungen aus der Praxis angereichert.					
Lehrformen Vorlesung und Übung					
Prüfungsformen Schriftliche Modulabschlussprüfung (120 Minuten)					
Voraussetzungen für die Vergabe von Credits Bestandene Modulabschlussprüfung					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) 5/99: Master ITS Netze und Systeme [PO 22] 5/96: Master ITS Netze und Systeme [PO 20] 5/91: Master ITS Informationstechnik [PO 22] 5/84: Master ITS Informationstechnik [PO 20]					

Titel des Moduls: Message Level Security					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen 212060: Message-Level Security			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Dr.-Ing. Christan Mainka Lehrende: Dr.-Ing. Christan Mainka Dr.-Ing. Vladislav Mladenov					
Verwendung des Moduls B.Sc. IT-Sicherheit/Informationstechnik M.Sc. IT-Sicherheit/Informationstechnik M.Sc. IT-Sicherheit / Netze und Systeme					
Lernziele (learning outcomes) Studierende verfügen nach erfolgreichem Abschluss der Vorlesung über ein umfassendes Verständnis der Sicherheit der folgenden Technologien: Datenformate im Web, REST APIs, Authentifizierungs- und Autorisierungsprotokollen und Dokumentenformaten. Durch die praxisnahe Arbeit im Rahmen der Übungen bauen die Studierenden ihre Recherche-Fähigkeiten aus und erlernen weiterhin den sicheren Umgang mit verschiedenen Penetrationswerkzeugen. Am Ende der Vorlesung sind die Studierenden in der Lage, systematisch umfassende Sicherheitsanalysen sowie praktische Angriffe auf die behandelten Technologien selbstständig durchzuführen. Weiterhin sind die Studierenden in der Lage, das erlernte Wissen auf andere Technologien zu übertragen und komplexere Angriffsmöglichkeiten selbst durch kreatives Denken zu finden und auszunutzen.					
Inhalt Die Vorlesung behandelt das Thema Message-Level Security. Anders als bei SSL/TLS, welches einen sicheren Transportkanal aufbaut, geht es bei Message-Level Security darum, Nachrichten – wie HTTP Requests – auf Nachrichtenebene zu schützen. Hierbei kommt es auf die korrekte Verwendung von kryptografischen Verfahren als auch eine sichere Bereitstellung von API-Schnittstellen an. Im Rahmen der Vorlesung werden verschiedene Verfahren von Message-Level Security beleuchtet:					
<ul style="list-style-type: none"> • JSON ist eine universelle Datenbeschreibungssprache, die unter anderem von jedem modernen Browser unterstützt wird. Mithilfe von JSON-Signature und JSON-Encryption können JSON Nachrichten direkt geschützt werden. Doch reicht das aus oder können diese Sicherheitsmechanismen umgangen werden? • OAuth ist eine sehr weitverbreitete Technologie zum Delegieren von Berechtigungen und wird heutzutage von allen großen Webseiten wie Facebook, Google, Twitter, Github usw. eingesetzt. Die Vorlesung erklärt tiefgehende Details und gängige Fehler/Angriffe, die bei der Verwendung von OAuth entstehen können. • OpenID Connect ist eine Erweiterung für OAuth, um Benutzer:innen auf Webseiten mithilfe eines Drittanbieters zu authentifizieren (z. B. mittels Single Sign-On Verfahren wie „Sign in with Google“). OpenID Connect hat sich in den letzten Jahren zum de facto Standard für Web-Logins über Drittanbieter etabliert. In der Vorlesung wird detailliert erklärt, was die Unterschiede zu OAuth sind und welche Angriffe auf OpenID Connect möglich sind. In den praktischen Übungen können Sie Ihre Exploit-Fähigkeiten unter Beweis stellen. Schaffen wir es, den Account des Opfers übernehmen? • SAML steht für Security Assertion Markup Language und ist ein Single Sign-On Standard, der eine weitgehende Verbreitung in Business-Szenarien findet. Allerdings existieren zahlreiche Angriffe von Identitätsdiebstahl bis hin zu Remote Code Execution. • PDF ist das vermutlich am weitesten verbreitetste universelle Dokumentenaustauschformat. In der Vorlesung werden die Sicherheitseigenschaften von PDFs beleuchtet. Insbesondere werden hierbei digitale Signaturen untersucht, welche z. B. bei Verträgen zum Einsatz kommen. Wird es uns gelingen, signierte Dokumente zu fälschen? 					

Den Studierenden wird ein tiefgehendes Verständnis der Systeme vermittelt. Zu allen untersuchten Systemen werden Angriffe vorgestellt, die sowohl aus der akademischen Welt als auch aus der Pentesting-Community stammen. Die Übungen bieten die Möglichkeit, das erlernte Wissen praktisch auszuprobieren. Hierzu erhalten die Studierenden eine virtuelle Maschine.

Lehrformen

Vorlesung mit Übung

Prüfungsformen

Schriftliche Modulabschlussprüfung (120 Minuten)

Voraussetzungen für die Vergabe von Credits

Bestandene schriftliche Modulabschlussprüfung

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)

5/150: B.Sc. IT-Sicherheit/Informationstechnik [PO 22]

5/149: B.Sc. IT-Sicherheit/Informationstechnik [PO 20]

5/91: M.Sc. IT-Sicherheit/Informationstechnik [PO 22]

5/84: M.Sc. IT-Sicherheit/Informationstechnik [PO 20]

5/99: M.Sc. IT-Sicherheit / Netze und Systeme [PO 22]

5/96: M.Sc. IT-Sicherheit / Netze und Systeme [PO 20]

Titel des Moduls: Nebenläufige Programmierung

Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Nebenläufige Programmierung (211012)			Kontaktzeit 45 h	Selbststudium 105 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen keine		

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Dr.-Ing. Doga Arinir (Lehrauftrag)
Lehrende: Dr.-Ing. Doga Arinir

Verwendung des Moduls

B.Sc. Informatik

B.Sc. Angewandte Informatik

Master IT-Sicherheit | Informationstechnik

Lernziele (learning outcomes)

Nach dem erfolgreichen Abschluss des Moduls

- haben die Studierenden grundlegende Fähigkeiten und Techniken erworben, um nebenläufige Programme sicher entwickeln zu können
- kennen die Studierenden softwaretechnische Entwurfsmuster, welche bekannte Probleme bei nebenläufigen Programmen, wie zum Beispiel die Verklemmung, vermeiden lassen
- können die Studierenden die Performanz von Programmen durch den Einsatz der nebenläufigen Programmierung verbessern
- sind die Studierenden in der Lage, bestehende Programme zu analysieren und mögliche Fehler zu erkennen
- können die Studierenden die Sprachmerkmale und Schnittstellen von JAVA für die nebenläufige Programmierung sicher anwenden

Inhalt

Moderne Hardware-Architekturen lassen sich nur durch den Einsatz nebenläufiger Programme richtig ausnutzen. Die nebenläufige Programmierung garantiert bei richtiger Anwendung eine optimale Auslastung der Hardware. Jedoch sind mit einem sorglosen Einsatz dieser Technik auch viele Risiken verbunden. Die Veranstaltung stellt Vorteile und auch Probleme nebenläufiger Programme dar und zeigt, wie sich die Performanz von Programmen verbessern lässt.

1. Nebenläufigkeit: Schnelleinstieg

- Anwendungen vs. Prozesse
- Programme und ihre Ausführung
- Vorteile und Probleme von nebenläufigen Programmen (Verbesserung der Performanz, Synchronisation, Realisierung kritischer Abschnitte, Monitore, Lebendigkeit, Verklemmungen)

2. Threads in Java

3. UML-Modellierung von Nebenläufigkeit

4. Neues zur Nebenläufigkeit in Java 5 und Java 6

5. Realisierung von Nebenläufigkeit 6. Fortschritte Java-Konzepte für Nebenläufigkeit

6. Fortschritte Java-Konzepte für Nebenläufigkeit

Lehrformen

Online Vorlesung mit begleitendem eLearning Kurs

Prüfungsformen

Schriftliche Modulabschlussprüfung über 90 Minuten

Voraussetzungen für die Vergabe von Credits

Bestandene Modulabschlussprüfung

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)

5/158: B.Sc. Informatik [PO 22]

5/165: B.Sc. Informatik [PO 20]

5/168: B.Sc. Angewandte Informatik [PO 22]

5/170: B.Sc. Angewandte Informatik [PO 20]

5/91 Master IT-Sicherheit | Informationstechnik

Titel des Moduls: Physical Attacks and Countermeasures					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen 211034: Physical Attacks and Countermeasures			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Englisch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Amir Moradi Lehrende: Prof. Dr. Amir Moradi					
Verwendung des Moduls M.Sc. IT-Sicherheit/Informationstechnik M.Sc. IT-Sicherheit/Netze und Systeme M.Sc. Informatik					
Lernziele (learning outcomes) Die Studierenden <ul style="list-style-type: none"> • verstehen wie und warum physikalische Angriffe funktionieren. • sind in der Lage Messdaten anhand der erlernten Methoden auszuwerten und die Sicherheit einer Implementierung zu bewerten. • erkennen die Gefahr von physikalischen Angriffen für Implementierungen von kryptographischen Algorithmen. • kennen mögliche Gegenmaßnahmen und wissen wie diese anzuwenden sind, um ein System gegen physikalische Angriffe zu schützen. 					
Inhalt Moderne kryptographische Algorithmen bieten ausreichend Schutz gegen die bekannten mathematischen und kryptanalytischen Angriffe. In der Praxis werden diese Algorithmen für sicherheitskritische Anwendungen auf verschiedenen Plattformen implementiert. Dies geschieht sowohl als Programmcode (Software) als auch mit logischen Elementen/Schaltungen (Hardware). Der physikalische Zugang zu kryptographischen Implementierungen (z.B., eine Smartcard oder ein Smartphone, welche zum Bezahlen benutzt werden), in welchen der geheime Schlüssel eingebettet ist, hat zur Entstehung einer neuen Klasse von Angriffen, genannt physikalische Angriffe, geführt. Diese Angriffe zielen darauf ab den geheimen Schlüssel, welcher vom kryptographischen Algorithmus benutzt wird, zu extrahieren. Ein erfolgreicher physikalischer Angriff deutet nicht auf Schwächen im Algorithmus sondern auf Schwachstellen in der Implementierung hin. Daher müssen bereits in der Entwicklungsphase von kryptographischen Implementierungen physikalische Angriffe als potentielles Risiko berücksichtigt und bestmöglich verhindert werden. Das Ziel dieser Lehrveranstaltung ist es einen Überblick über bekannte physikalische Angriffe und deren Gegenmaßnahmen zu geben. Im ersten Teil der Vorlesung werden die verschiedenen Angriffstypen eingeführt, während im zweiten Teil der Fokus auf Gegenmaßnahmen liegt.					
Lehrformen Vorlesung mit Übung					
Prüfungsformen Schriftliche Prüfung (120 Minuten), Projektarbeit und Seminar					
Voraussetzungen für die Vergabe von Credits Projektbasiertes Arbeiten ist ein großer Teil der Lehrveranstaltung. Zusätzlich zu einer schriftlichen Prüfung gibt es wöchentliche Projektarbeiten (Hausaufgaben) und ein abschließendes Seminar. Alle Teile müssen individuell bearbeitet werden, sind bewertet und gehen in die Endnote ein. Für das erfolgreiche Bestehen des Kurses muss die Klausur mit mindestens 50					

Wöchentliche Projektarbeiten (Hausaufgaben): 30

Klausur: 60

Abschließendes Seminar: 20

Dies ergibt eine Summe von 110

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)

5/91: M.Sc. IT-Sicherheit/Informationstechnik [PO 22]

5/84: M.Sc. IT-Sicherheit/Informationstechnik [PO 20]

5/99: M.Sc. IT-Sicherheit/Netze und Systeme [PO 22]

5/96: M.Sc. IT-Sicherheit/Netze und Systeme [PO 20]

5/97: M.Sc. Informatik

Titel des Moduls: Praktikum/Projektarbeit					
Modul-Nr./Code	Credits 4 CP	Workload	Semester	Turnus	Dauer Semester
Lehrveranstaltungen			Kontaktzeit	Selbststudium	Gruppengröße Studierende
Unterrichtssprache			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Lehrende:					
Verwendung des Moduls					
Lernziele (learning outcomes)					
Inhalt					
Lehrformen					
Prüfungsformen					
Voraussetzungen für die Vergabe von Credits					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)					

Titel des Moduls: Processor Security Processor Security					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester	Turnus Sommersemester	Dauer Semester
Lehrveranstaltungen 211099: Processor Security			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Dr.-Ing. Pascal Sasdrich Lehrende: Dr.-Ing. Pascal Sasdrich					
Verwendung des Moduls B.Sc. IT-Sicherheit/Informationstechnik M.Sc. IT-Sicherheit/Informationstechnik M.Sc. IT-Sicherheit/Netze und Systeme					
Lernziele (learning outcomes) Im Rahmen dieser Veranstaltung lernen die Studierenden wichtige Sicherheitsaspekte und -konzepte moderner Prozessoren kennen. Der Fokus der Veranstaltung liegt dabei auf (a) Kenntnis gängiger Angriffsvektoren, (b) Verständnis der zugrundeliegenden Hardware- und Prozessormechanismen, (c) Diskussion möglicher Gegenmaßnahmen, sowohl in Hardware als auch Software.					
Inhalt Moderne Prozessorenarchitekturen, von eingebetteten Mikrocontrollern bis hin zu Server-CPU's, bilden das Kernstück unserer heutigen Informationsgesellschaft und werden seit Jahrzehnten immer komplizierter. Diese gesteigerte Komplexität führt aber unausweichlich zu neuen Schwachstellen und gesteigerter Anfälligkeiten gegen gezielte Angriffe. Im Rahmen dieser Veranstaltung werden daher verschiedene Sicherheitsaspekte und -konzepte moderner Prozessorarchitekturen vorgestellt und erläutert. Dazu werden sowohl wichtige Angriffsvektoren (z.B. Buffer Overflows, Privilege Escalation, Control-Flow Manipulation, Side Channel Attacks, Microarchitectural Attacks, ...), fundamentale Ursachen in der Prozessorarchitektur, als auch mögliche Abwehrstrategien diskutiert. Vorlesungsbegleitend wird ein Moodle-Kurs angeboten, der zusätzliche Inhalte sowie die praktischen Übungen bereithält.					
Lehrformen Vorlesung mit Übung					
Prüfungsformen Schriftliche Modulabschlussprüfung (120 Minuten)					
Voraussetzungen für die Vergabe von Credits					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) 5/150: B.Sc. IT-Sicherheit/Informationstechnik [PO 22] 5/149: B.Sc. IT-Sicherheit/Informationstechnik [PO 20] 5/91: M.Sc. IT-Sicherheit/Informationstechnik [PO 22] 5/84: M.Sc. IT-Sicherheit/Informationstechnik [PO 20] 5/99: M.Sc. IT-Sicherheit/Netze und Systeme [PO 22]					

Titel des Moduls: Programmanalyse					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Programmanalyse			Kontaktzeit 60 h	Selbststudium	Gruppengröße Studierende
Unterrichtssprache Englisch			Teilnahmevoraussetzungen keine		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Kevin Borgolte Lehrende: Prof. Kevin Borgolte					
Verwendung des Moduls M.Sc. IT-Sicherheit / Informationstechnik M.Sc. IT-Sicherheit / Netze und Systeme					
Lernziele (learning outcomes) Die Studierenden kennen verschiedene Konzepte, Techniken und Tools aus dem Bereich der Programmanalyse. Dies beinhaltet den Überblick über verschiedene Konzepte aus dem Bereich Reverse Engineering sowie Binäranalyse. Die Studierenden haben grundlegendes Verständnis von sowohl statischen als auch dynamischen Methoden zur Analyse eines gegebenen Programms. Sie sind in der Lage, verschiedene Aspekte der Programmanalyse zu beschreiben und auf neue Problemstellungen anzuwenden.					
Inhalt In der Vorlesung werden unter anderem die folgenden Themen und Techniken aus dem Bereich der Programmanalyse behandelt: <ul style="list-style-type: none"> • Statische und dynamische Analyse von Programmen • Analyse von Kontroll- und Datenfluss • Symbolische Ausführung • Taint Tracking • Binary Instrumentation • Program Slicing • Überblick zu existierenden Analysetools Daneben wird im ersten Teil der Vorlesung eine Einführung in x86/x64 Assembler gegeben sowie die grundlegenden Techniken aus dem Themenbereich Reverse Engineering vorgestellt. Begleitet wird die Vorlesung von Übungen, in denen die vorgestellten Konzepte und Techniken praktisch eingeübt werden.					
Lehrformen Vorlesung mit Übung					
Prüfungsformen schriftlich (120 min), Anmeldung: FlexNow					
Voraussetzungen für die Vergabe von Credits Bestandene Modulabschlussprüfung					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) 5/91: M.Sc. IT-Sicherheit / Informationstechnik [PO 22] 5/84: M.Sc. IT-Sicherheit / Informationstechnik [PO 20] 5/99: M.Sc. IT-Sicherheit / Netze und Systeme [PO 22] 5/96: M.Sc. IT-Sicherheit / Netze und Systeme [PO 20]					

Titel des Moduls: Proofs are programs					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen 211003: Proofs are Programms			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße 40 Studierende
Unterrichtssprache Englisch			Teilnahmevoraussetzungen keine		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Dr. Catalin Hritcu Lehrende: Dr. Catalin Hritcu Dr. Clara Schneidewind					
Verwendung des Moduls B.Sc. Informatik B.Sc. IT-Sicherheit / Informationstechnik M.Sc. IT-Sicherheit / Informationstechnik M.Sc. IT-Sicherheit / Netze und Systeme					
Lernziele (learning outcomes) After successful completion of this course, students will be able to <ul style="list-style-type: none"> • develop purely functional programs using recursive functions on numbers, lists, maps, and various kinds of trees, including the abstract syntax trees of programs; • use functional programming concepts such as type polymorphism and higher-order functions, which are increasingly becoming mainstream; • formally state and prove theorems in the Coq proof assistant; • apply different proof techniques in Coq (e.g. equational reasoning, contradiction, case analysis, induction on natural numbers, structural induction, proof automation); • define new inductive types and relations in Coq and prove statements about them; • understand the connection between constructive logics and typed functional programming that is at the heart of Coq, in which propositions are types and proofs are programs; • understand how the syntax and semantics of simple imperative programs can be formally defined in Coq and how to prove theorems about such programs and languages. 					
Inhalt Complex mathematical proofs on paper are difficult to write, check, and maintain. This holds not only for interesting proofs in mathematics, but also for complex formal proofs about interesting programs. For this reason, machine-checked proofs created with the help of interactive tools called proof assistants are gaining increased traction in academia and industry. Proof assistants have been used to prove the correctness and security of realistic compilers, operating systems, cryptographic libraries, or smart contracts, and also to construct machine-checked proofs for challenging mathematical results such as the four color theorem, the odd-order theorem (Feit–Thompson), or the construction of perfectoid spaces. This course introduces the Coq proof assistant and explains how to use it to prove properties about functional programs and inductive relations. The Coq proof assistant enables us to program formal proofs interactively and it machine-checks the correctness of the proofs along the way. The design of the Coq proof assistant itself exploits a beautiful connection between programs in typed functional programming languages and proofs in constructive logics, which is known as the Curry-Howard Correspondence. This deep connection between programs and proofs should make this course interesting to both computer scientists and mathematicians. For computer scientists the goal is to demystify proofs as just programs in an elegant programming language, for which the course provides a gentle introduction. For mathematicians this course serves as an introduction to functional programming and also to the idea that proofs are not only a way to convince a human reader, but they can					

actually be fully formalized in a proof assistant like Coq and automatically checked by a computer.

This hands-on course is based on the Logical Foundations online textbook, which is itself formalized and machine-checked in the Coq proof assistant. The many exercises in each book chapter are to be solved weekly mostly in Coq, from easy exercises allowing the students to practice concepts from the lecture, building incrementally to slightly more interesting programs and proofs and also to various optional challenges. Finally, this course serves as the base for a more advanced course on “Foundations of Programming Languages, Verification, and Security”.

Lehrformen

This course consists of lectures and weekly exercises, in which the students will solve problems using the Coq proof assistant for which they can get help from a tutor.

Prüfungsformen

Written final exam (90 minutes). We also plan to have a midterm exam that helps students practice for the final exam, but only counts for bonus points.

Voraussetzungen für die Vergabe von Credits

Passing the final exam (60% of the grade) and timely submission of solutions for the weekly Coq exercise sheets (40% of the grade).

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)

5/158: B.Sc. Informatik [PO 22]

5/170: B.Sc. Informatik [PO 20]

5/150: B.Sc. IT-Sicherheit / Informationstechnik [PO 22]

5/149: B.Sc. IT-Sicherheit / Informationstechnik [PO 20]

5/91: M.Sc. IT-Sicherheit / Informationstechnik [PO 22]

5/84: M.Sc. IT-Sicherheit / Informationstechnik [PO 20]

5/99: M.Sc. IT-Sicherheit / Netze und Systeme [PO 22]

5/96: M.Sc. IT-Sicherheit / Netze und Systeme [PO 20]

Titel des Moduls: Public Key Kryptanalyse 1
Public Key Cryptanalysis 1

Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester	Turnus Sommersemester	Dauer Semester
Lehrveranstaltungen Public Key Kryptanalyse 1 (211055)			Kontaktzeit 45 h	Selbststudium 105 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen keine		

Modulbeauftragte/r und hauptamtlich Lehrende

Modulbeauftragte/r: Prof. Alex May
 Lehrende: Prof. Alex May

Verwendung des Moduls

Lernziele (learning outcomes)

Die Studierenden sollen breite Kenntnisse zu algorithmischen Techniken der asymmetrischen Kryptanalyse, insbesondere für codierungsbasierte Kryptographie, erlangen.

Nach dem erfolgreichen Abschluss des Moduls

- kennen die Studierenden grundlegende Schlüsselfindungs-Algorithmen wie Brute-Force und Meet-in-the-Middle und können diese auf neue kryptographische Systeme anwenden,
- beherrschen sie die Grundlagen linearer Codes und ihrer Dualcodes, insbesondere als kryptographische Anwendung das McEliece-Kryptosystem,
- kennen Studierende Time-Memory Techniken wie Pollard Rho und Parallel Collision Search, und können sie auf neue Probleme anwenden,
- haben Studierende einen Überblick über alle aktuellen Dekodieralgorithmen im Bereich des Information Set Decoding, die für die Sicherheits-Evaluierung moderner codierungsbasierter Kryptosysteme relevant sind,
- sind Studierende in der Lage, Techniken der Kryptanalyse mit Hilfe der Computer-Algebra Sage zu implementieren.

Inhalt

Kryptanalyse dient dazu, kryptographische Systeme derart zu instantiiieren, dass sie einerseits ein vordefiniertes Sicherheitsniveau bieten, andererseits aber möglichst performant sind. Die Kryptanalyse bietet dazu einen ganzen Werkzeugkoffer an algorithmischen Techniken, um die Evaluation neuer kryptographischer Systeme zu realisieren. Dies beinhaltet sowohl klassische Algorithmen als auch Algorithmen für Quantenrechner, damit die verwendete Kryptographie selbst in einer Ära von Quantenrechnern sicher bleiben.

Lehrformen

Die Vorlesung wird als seminaristischer Unterricht abgehalten, die praktischen Übungen am Rechner mit der Computer-Algebra Sage werden zudem weitere Lehrformen wie Gruppen- und Projektarbeit beinhalten.

Prüfungsformen

Schriftliche Modulabschlussprüfung über 120 Minuten

Voraussetzungen für die Vergabe von Credits

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)

5/149 B.Sc. IT-Sicherheit [PO20]

5/150 B.Sc. IT-Sicherheit [PO22]

5/91 M.Sc IT-Sicherheit | Informationstechnik [PO22]

5/99 M.Sc IT-Sicherheit | Netze und Systeme [PO22]

Titel des Moduls: Public Key Verschlüsselung					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Public Key Verschlüsselung			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Jun. Prof. Dr. Nils Fleischhacker Lehrende: Jun. Prof. Dr. Nils Fleischhacker					
Verwendung des Moduls Master IT-Sicherheit Informationstechnik Master IT-Sicherheit Netze und Systeme					
Lernziele (learning outcomes) Die Studierenden haben einen Einblick in in theoretische und praktische Aspekte der Public Key Verschlüsselung erhalten					
Inhalt Die Vorlesung gibt einen Einblick in theoretische und praktische Aspekte der Public Key Verschlüsselung. Dies umfasst Grundlagen und formalen Definitionen von Sicherheit (CPA, CCA1, CCA2), die beweisbare Sicherheit verschiedener theoretischer und praktischer Konstruktionen, sowie die Verbindungen von Public Key Verschlüsselung zu anderen Aspekten der Kryptographie.					
Lehrformen Vorlesung mit Übung					
Prüfungsformen Mündlich (30 Minuten)					
Voraussetzungen für die Vergabe von Credits Bestandene Modulabschlussprüfung					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) Master IT-Sicherheit Informationstechnik (5/91) Master IT-Sicherheit Netze und Systeme (5/99)					

Titel des Moduls: Quantum Cryptography

Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen 212016 - Quantum Cryptography			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Englisch			Teilnahmevoraussetzungen keine		

Modulbeauftragte/r und hauptamtlich Lehrende

Modulbeauftragte/r: Prof. Michael Walter
Lehrende: Prof. Michael Walter
Dr. Giulio Malavolta

Verwendung des Moduls

M.Sc. IT-Sicherheit | Informationstechnik
M.Sc. IT-Sicherheit | Netze und Systeme

Lernziele (learning outcomes)

You will learn fundamental concepts, algorithms, protocols, and results in quantum (and quantum-resistant) cryptography. After successful completion of this course, you will know how to generalize cryptographic concepts to the quantum setting, how quantum algorithms can attack well-known cryptographic protocols, and how to design and analyze classical and quantum protocols for protecting classical and quantum data against quantum adversaries. You will be prepared for a research or thesis project in this area.

Inhalt

This course will give an introduction to the interplay of quantum information and cryptography, which has recently led to much excitement and insights – including by researchers at CASA right here on our very own campus. We will begin with a brief introduction to both fields and discuss in the first half of the course how quantum computers can attack classical cryptography and how to overcome this challenge – either by protecting against the power of quantum computers or by leveraging the power of quantum information. In the second half of the course, we will discuss how to generalize cryptography to protect quantum data and computation.

Topics to be covered will likely include:

- * Basic quantum computing
- * Basic cryptography
- * Quantum attacks on classical cryptography
- * Quantum random oracles and compressed oracle technique
- * Quantum-resistant cryptography in light of the NIST competition
- * Classical vs quantum information
- * Quantum money
- * Quantum key distribution
- * Quantum complexity theory
- * Quantum pseudorandomness
- * From classical to quantum fully homomorphic encryption
- * Classical verification of quantum computation

* Quantum rewinding

This course should be of interest to students of computer science, mathematics, physics, and related disciplines. Students interested in a Master's project in quantum or quantum-resistant cryptography, quantum information, quantum computing, and similar are particularly encouraged to participate.

Lehrformen

Vorlesung mit Übungen

Prüfungsformen

Modulabschlussprüfung; schriftlich oder mündlich je nach Teilnehmendenzahl.

Voraussetzungen für die Vergabe von Credits

Bestandene Modulabschlussprüfung

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)

5/91 M.Sc. IT-Sicherheit | Informationstechnik

5/99 :M.Sc. IT-Sicherheit | Netze und Systeme

Titel des Moduls: Quantum Information and Computation					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Quantum Information and Computation			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache German or Englisch (depends on audience)			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Michael Walter Lehrende: Prof. Dr. Michael Walter					
Verwendung des Moduls B.Sc. Informatik B.Sc. IT-Sicherheit/Informationstechnik M.Sc. Angewandte Informatik M.Sc. IT-Sicherheit Informationstechnik M.Sc. IT-Sicherheit Netze und Systeme					
Lernziele (learning outcomes) You will learn fundamental concepts, algorithms, and results in quantum information and computation. After successful completion of this course, you will know the theoretical model of quantum information and computation, how to generalize computer science concepts to the quantum setting, how to design and analyze quantum algorithms and protocols for a variety of computational problems, and how to prove complexity theoretic lower bounds. You will be prepared for an advanced course or a research or thesis project in this area.					
Inhalt This course will give an introduction to quantum information and quantum computation from the perspective of theoretical computer science. Topics to be covered will likely include: <ul style="list-style-type: none"> • Fundamentals of quantum computing: quantum bits, states and operations • The power of quantum entanglement: nonlocal games • Entanglement as a resource: superdense coding and teleportation • Quantum circuit model of computation • Quantum computing with oracles: Deutsch-Jozsa, Bernstein-Vazirani, Simon • Quantum Fourier transform and phase estimation • Shor's factoring algorithm • Grover's search algorithm and beyond: how to solve SAT on a quantum computer? • From no cloning to quantum money: a peek at quantum cryptography <p>The course should be of interest to students of computer science, mathematics, physics, and related disciplines. Students interested in a BSc or MSc project in quantum information, computing, cryptography, etc. are particularly encouraged to participate.</p>					
Lehrformen Lecture with Exercise					
Prüfungsformen Written Exam (120 Minutes)					
Voraussetzungen für die Vergabe von Credits Passed written Exam.					

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)

5/158: B.Sc. Informatik [PO 22]

5/165: B.Sc. Informatik [PO 20]

5/150: B.Sc. IT-Sicherheit/Informationstechnik [PO 22]

5/149: B.Sc. IT-Sicherheit/Informationstechnik [PO 20]

5/105: M.Sc. Angewandte Informatik

5 /91: M.Sc. IT-Sicherheit | Informationstechnik [PO 22]

5/ 99: M.Sc. IT-Sicherheit | Netze und Systeme [PO 22]

Titel des Moduls: Software Protection Software Protection					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Software Protection			Kontaktzeit 45 h	Selbststudium 105 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen keine		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Professur für Systemsicherheit Lehrende: Dr.-Ing. Tim Blazytko Philipp Koppe					
Verwendung des Moduls Bachelor IT-Sicherheit Informationstechnik Master IT-Sicherheit Informationstechnik Master IT-Sicherheit Netze und Systeme					
Lernziele (learning outcomes) Die Studierenden kennen verschiedene Konzepte, Techniken und Tools aus dem Bereich Software Protection. Dies beinhaltet sowohl Wissen über das Design und die Implementierung von Obfuskingstechniken als auch die Sicherheitsanalyse gängiger Systeme. Die Studierenden lernen erweiterte Techniken zur Programmanalyse, mit welchen sie komplexe Protection-Mechanismen angreifen können. Sie sind in der Lage, verschiedene Aspekte der Software Protection zu beschreiben und auf neue Problemstellungen anzuwenden.					
Inhalt Unter Software Protection versteht man Maßnahmen, welche die Analyse bzw. das Reverse Engineering von Software erschweren. Solche Methoden finden sowohl Anwendung in kommerzieller Software, um Piraterie zu verhindern, als auch in Malware, um deren Funktionsweise zu verschleiern. In dieser Lehrveranstaltung lernen die Studierenden gängige Methoden der Software Protection kennen sowie Methoden, um diese zu brechen. Dazu designen und implementieren sie in praxisnahen Aufgaben erst ihre eigenen Protection-Mechanismen, welche sie im Anschluss brechen werden mit dem Ziel, diese wieder zu verbessern. Parallel dazu werden Schutzmechanismen aus der echten Welt analysiert, attackiert und diskutiert. Dabei werden unter anderem die folgenden Themen und Techniken aus dem Bereich Software Protection behandelt: - Opaque Predicates - Control-flow Flattening - Mixed Boolean-Arithmetic Expressions - Virtual Machines - Anti-Tamper - Symbolische Ausführung - SMT Solving - Programmsynthese					

- Überblick zu existierenden Analysetools und Frameworks

Lehrformen

Vorlesung mit Übung

Prüfungsformen

Arbeit/Kompetenznachweis im Semester. Die Lehrveranstaltung beinhaltet mehrere benotete praktische Übungen mit einer Dauer von 2-3 Wochen pro Übung. Jeder Teilnehmer bearbeitet die Übungen selbstständig in Einzelarbeit. Die Modulabschlussnote bildet sich aus dem gewichteten arithmetischen Mittel der einzelnen Übungen.

Voraussetzungen für die Vergabe von Credits

Erfolgreiche Kompetenznachweis im Semester

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)

5/150: Bachelor IT-Sicherheit | Informationstechnik [PO 22]

5/149: Bachelor IT-Sicherheit | Informationstechnik [PO 20]

5/91: Master IT-Sicherheit | Informationstechnik [PO 22]

5/84: Master IT-Sicherheit | Informationstechnik [PO 20]

5/99: Master IT-Sicherheit | Netze und Systeme [PO 22]

5/96: Master IT-Sicherheit | Netze und Systeme [PO 20]

Titel des Moduls: Software Security					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Software Security			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Englisch			Teilnahmevoraussetzungen Keine		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Kevin Borgolte Lehrende: Prof. Kevin Borgolte					
Verwendung des Moduls Master IT-Sicherheit Informationstechnik Master IT-Sicherheit Netze und Systeme					
Lernziele (learning outcomes) At the end of this course, students will be able to: <ul style="list-style-type: none"> • classify and describe vulnerabilities and protection mechanisms of software systems • analyze and reason about protection mechanisms for modern software systems • identify vulnerabilities in software systems • develop proofs of concept exploits/verifications to show the existence of a vulnerability in a software system • understand how to write code defensively to reduce the risk of vulnerabilities 					
Inhalt The course covers the area of software security and vulnerability discovery and vulnerability verification, focusing on: <ul style="list-style-type: none"> • Assembly and Disassembly, Shellcode • Binary Reverse Engineering and Debugging • Sandboxing • Memory and Type Safety/Errors • Information Leakage • Vulnerability Exploitation/Verification, Buffer and Heap Overflows • Code Re-use Attacks, e.g., Return Oriented Programming • Race Conditions • Format String Vulnerabilities • Exploit/Verification Synthesis and Automated Exploitation/Verification • Kernel Security • Defensive Programming 					
Lehrformen Vorlesung mit Übung					
Prüfungsformen					
Voraussetzungen für die Vergabe von Credits					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) Master IT-Sicherheit Informationstechnik (5/91) Master IT-Sicherheit Netze und Systeme (5/99)					

Titel des Moduls: Software-Implementierung kryptographischer Verfahren

Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen 211035: Software-Implementierung kryptographischer Verfahren			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen keine		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr.-Ing. Tim Guneyusu Lehrende: Dr.-Ing. Max Hoffmann					
Verwendung des Moduls B.Sc. IT-Sicherheit/Informationstechnik M.Sc. IT-Sicherheit/Informationstechnik M.Sc. IT-Sicherheit/Netze und Systeme					
Lernziele (learning outcomes) Die Studierenden haben ein Verständnis für Methoden für die schnelle Software-Realisierung ausgewählter Krypto-Verfahren und diese selbst implementiert.					
Inhalt Es werden ausgewählte fortgeschrittene Implementierungstechniken der modernen Kryptographie behandelt. Inhalte: - Effiziente Implementierung von Blockchiffren - Bitslicing - Effiziente Arithmetik in $GF(2^m)$ - Effiziente Arithmetik auf elliptischen Kurven - Spezielle Primzahlen zur schnellen modularen Reduktion - Primzahltests - Post-Quantum Kryptographie - Secure Coding					
Lehrformen Vorlesung mit Übungen					
Prüfungsformen Schriftliche Modulabschlussprüfung (120 Minuten)					
Voraussetzungen für die Vergabe von Credits Es müssen mindestens 50 Prozent aller möglichen Punkte in der Klausur und den semesterbegleitenden Projekten erreicht werden.					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) 5/150: B.Sc. IT-Sicherheit/Informationstechnik [PO 22] 5/149: B.Sc. IT-Sicherheit/Informationstechnik [PO 20] 5/91: M.Sc. IT-Sicherheit/Informationstechnik [PO 22] 5/84: M.Sc. IT-Sicherheit/Informationstechnik [PO 20]					

5/99: M.Sc. IT-Sicherheit/Netze und Systeme [PO 22]

5/96: M.Sc. IT-Sicherheit/Netze und Systeme [PO 20]

Titel des Moduls: Symmetrische Kryptanalyse

Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Symmetrische Kryptanalyse			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Nils-Gregor Leander Lehrende: Prof. Dr. Nils-Gregor Leander					
Verwendung des Moduls M.Sc. IT-Sicherheit/Informationstechnik M.Sc. IT-Sicherheit/Netze und Systeme M.Sc. Angewandte Informatik					
Lernziele (learning outcomes) Die Studierenden haben ein vertieftes Verständnis für die Sicherheit symmetrischer Chiffren.					
Inhalt Wir behandeln die wichtigsten Themen in der symmetrischen Kryptanalyse. Nach einer ausführlichen Vorstellung von linearer und differentieller Kryptanalyse werden weitere Angriffe auf symmetrische Primitive, insbesondere Block-Chiffren behandelt. Hierzu zählen insbesondere Integral (auch Square) Attacks, Impossible Differentials, Boomerang-Angriffe und Slide-Attacks. Neben den Angriffen selbst werden auch immer die daraus resultierenden Design-Kriterien beschrieben, um neue Algorithmen sicher gegen die Angriffe zu machen.					
Lehrformen					
Prüfungsformen Mündliche Modulabschlussprüfung (30 Minuten)					
Voraussetzungen für die Vergabe von Credits Bestandene mündliche Modulabschlussprüfung.					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) 5/91: M.Sc. IT-Sicherheit/Informationstechnik [PO 22] 5/84: M.Sc. IT-Sicherheit/Informationstechnik [PO 20] 5/99: M.Sc. IT-Sicherheit/Netze und Systeme [PO 22] 5/96: M.Sc. IT-Sicherheit/Netze und Systeme [PO 20] 5/105: M.Sc. Angewandte Informatik					

Titel des Moduls: Vertiefungsseminar (M.Sc. IT-Sicherheit)

Modul-Nr./Code	Credits 3 CP	Workload 90 h	Semester	Turnus jedes Semester	Dauer Semester
Lehrveranstaltungen			Kontaktzeit	Selbststudium	Gruppengröße Studierende
211104 Human Centred Security and Privacy			30 h		
211110 Seminar Real-World Kryptanalyse					
211114 Master-Seminar on Security and Privacy of Mobile Operating Systems					
211117 Seminar Satisfiability (bis SoSe 23)					
211119 Quantum Algorithms (bis SoSe 23)					
211121 Fortgeschrittene Themen des Model Checking ()					
211122 Seminar über Grenzen in der theoretischen Informatik ()					
211129 Master-Seminar Developer Centered Security					
211132 Master-Seminar Digitale Souveränität					
211133 Seminar on Current Topics for Systems Security and Privacy					
212109 Information Security Seminar					
212111 Seminar Ressourceneffiziente Systemsoftware					
212112 Seminar Security Engineering					
212118 Seminar zur symmetrischen Kryptographie					
212121 Seminar Netz- und Datensicherheit					
212122 Seminar Current Topics in Device Firmware Security					
212125 Software and Internet Security Seminar					
212126 Seminar Implementation Security (bis SoSe 23)					
Unterrichtssprache Deutsch oder Englisch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Studiendekan IT-Sicherheit Lehrende: siehe jeweiliges Seminar					
Verwendung des Moduls B.Sc. IT-Sicherheit					
Lernziele (learning outcomes) Nach dem erfolgreichen Abschluss des Moduls <ul style="list-style-type: none"> • verfügen Studierende über vertiefte wissenschaftliche Kenntnisse in dem ausgewählten Seminarthema 					

- haben Studierende das Halten eines wissenschaftlichen Vortrags praktisch eingeübt und können Forschungsergebnisse eigenständig in einem didaktisch wohl aufbereiteten Vortrag vermitteln
- können die Teilnehmer konstruktives Feedback formulieren und entgegennehmen

Inhalt

Es werden Masterseminare zu mehreren relevanten Themen aus der IT-Sicherheit angeboten, wie beispielsweise zu Netz- und Datensicherheit, Implementation Security, Human Centred Security and Privacy oder Kryptographie. Von den angebotenen Themen wählen die Studierenden abhängig von den eigenen Interessen und den individuellen Vertiefungswünschen ein Thema aus. Dieses sollen die Studierenden selbstständig bearbeiten. Dazu gehören die Literaturrecherche, die Einarbeitung in das Thema und schließlich die Präsentation. Nähere Informationen sind zu den jeweiligen Seminaren im Vorlesungsverzeichnis zu entnehmen.

Lehrformen

Seminar

Prüfungsformen

Seminarvortrag

Voraussetzungen für die Vergabe von Credits**Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)**

3/149: B.Sc. IT-Sicherheit [PO 20]

3/150: B.Sc. IT-Sicherheit [PO 22]

Titel des Moduls: Web-Engineering					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester Siehe Prüfungsordnung	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Web-Engineering (128968 + 128969)			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße 200 Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr.-Ing. Markus König Lehrende: Prof. Dr.-Ing. Markus König Stephan Embers, M.Sc.					
Verwendung des Moduls B.Sc. Angewandte Informatik B.Sc. Informatik M.Sc. IT-Sicherheit/Informationstechnik					
Lernziele (learning outcomes) Die Entwicklung von Web-Anwendungen und Web-Services ist zentraler Bestandteil der Digitalisierung. Ziel der Lehrveranstaltung ist die Vermittlung von Grundlagen und bewährten Verfahren in der Web-Entwicklung. Studierende lernen konzeptuelle technologische Bausteine kennen: Transportverfahren, Webseitendarstellung, dynamische Web-Anwendungen und Web-Services. Über das konzeptuelle Verständnis hinaus werden praktische Kompetenzen vermittelt. Dazu werden moderne Werkzeuge der Web-Entwicklung, sowohl server- als auch clientseitig, vorgestellt und in den Übungssitzungen praktisch vertieft. Während der Umsetzung einfacher Web-Anwendungen stehen auch analytische Fähigkeiten im Fokus: Studierende werden befähigt, verschiedene Verfahren in Hinblick auf Performanz und Wartbarkeit zu bewerten. Diese Fähigkeiten sind in der kritischen Planungsphase von Software-Projekten unerlässlich. Nach dem erfolgreichen Abschluss des Moduls: <ul style="list-style-type: none"> • kennen Studierende gängige Konzepte der Web-Entwicklung in den Aspekten Präsentation, Transport und Bereitstellung von Daten • beherrschen Studierende grundlegende Fähigkeiten in Webseitendarstellung, dynamischen Web-Anwendungen und modernen Services (Node.js) 					
Inhalt Im Rahmen des Moduls werden den Studierenden aktuelle Techniken und Kenntnisse im Bereich der Web-Entwicklung aufgezeigt. Thematisch wird der Bereich der server- und clientseitigen Entwicklung abgedeckt. JavaScript stellt dabei eine zentrale Rolle dar. Folgende Lehrinhalte werden behandelt: <ul style="list-style-type: none"> • Einführung in clientseitige Web-Entwicklung: HTML, CSS, JavaScript, Web Components • Transportverfahren und deren Nutzung: Representational State Transfer (REST), Asynchrones JavaScript und XML (AJAX) • Serverseitige Entwicklung mit Node.js und weiterführende Technologien 					
Lehrformen Synchrone Onlinevorlesung, Tutorien als seminaristischer Unterricht, zusätzlich Selbststudium mit ergänzend bereitgestellten Materialien und Aufgaben.					
Prüfungsformen Schriftliche Modulabschlussprüfung (120 Minuten)					
Voraussetzungen für die Vergabe von Credits Bestandene schriftliche Modulabschlussprüfung					

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)

5/168: B.Sc. Angewandte Informatik [PO 22]

5/170: B.Sc. Angewandte Informatik [PO 20]

5/158: B.Sc. Informatik [PO 22]

5/165: B.Sc. Informatik [PO 20]

5/91: M.Sc. IT-Sicherheit/Informationstechnik [PO 22]

5/84: M.Sc. IT-Sicherheit/Informationstechnik [PO 20]

Titel des Moduls: Ze-ro-Know-ledge Proof Sys-tems					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen 211032: Ze-ro-Know-ledge Proof Sys-tems			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen keine		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Jun. Prof. Dr. Nils Fleischhacker Lehrende: Jun. Prof. Dr. Nils Fleischhacker					
Verwendung des Moduls M.Sc. IT-Sicherheit Informationstechnik M.Sc. IT-Sicherheit Netze und Systeme					
Lernziele (learning outcomes) A deep understanding of the Foundations and Applications of Zero-Knowledge Proof Systems. This includes an understanding of the necessary underlying assumptions, the lower bound on what is possible to achieve, as well as efficient instantiations from concrete assumptions.					
Inhalt Zero-Knowledge protocols are important building blocks for more complex cryptographic protocols. This class covers foundational aspects of zero-knowledge proofs, including: Lower bounds and round complexity, necessary assumptions, communication complexity, and zero-knowledge in a quantum world, as well as theoretical and practical constructions and their security proofs. Topics: Cryptography, Interactive Proof Systems, Zero-Knowledge Proofs, Provable Security					
Lehrformen Lecture with exercise					
Prüfungsformen Written Exam / Oral Exam The form of examination will be determined at the beginning of the lecture.					
Voraussetzungen für die Vergabe von Credits Bestandene Modulabschlussprüfung					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) 5/91: M.Sc. IT-Sicherheit Informationstechnik [PO 22] 5/84: M.Sc. IT-Sicherheit Informationstechnik [PO 20] 5/99: M.Sc. IT-Sicherheit Netze und Systeme [PO 22] 5/96: M.Sc. IT-Sicherheit Netze und Systeme [PO 20]					

Titel des Moduls: Freie Wahlfächer free electives					
Modul-Nr./Code	Credits 25 CP	Workload	Semester	Turnus	Dauer Semester
Lehrveranstaltungen			Kontaktzeit siehe Lehrveranstaltungen	Selbststudium	Gruppengröße Studierende
Unterrichtssprache			Teilnahmevoraussetzungen siehe Lehrveranstaltungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Lehrende:					
Verwendung des Moduls					
Lernziele (learning outcomes) Durch die freie Wahl von Lehrveranstaltungen können die Studierenden fachliche und überfachliche Schwerpunkte setzen. Sie beherrschen entsprechend ihrer Wahl verschiedene, das Studium ergänzende Schlüsselqualifikationen und haben ihr Fachwissen vertieft.					
Inhalt siehe Lehrveranstaltungen					
Lehrformen					
Prüfungsformen					
Voraussetzungen für die Vergabe von Credits					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)					

Titel des Moduls: Masterarbeit und Kolloquium (ITS)					
Modul-Nr./Code	Credits 30 CP	Workload	Semester	Turnus	Dauer Semester
Lehrveranstaltungen			Kontaktzeit	Selbststudium	Gruppengröße Studierende
Unterrichtssprache			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Lehrende:					
Verwendung des Moduls					
Lernziele (learning outcomes)					
Inhalt					
Lehrformen					
Prüfungsformen					
Voraussetzungen für die Vergabe von Credits					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)					