

Modulhandbuch Bachelor of Science (B.Sc.)

IT-Sicherheit / Informationstechnik [P022]

Stand: Sommersemester 2024

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



Studienplan Bachelor IT- Sicherheit / Informationstechnik der Ruhr-Universität Bochum

Nr	Modul	Umfang (LP)	Empfohlenes Semester	Bewertung
Pflichtbereich				
1	Mathematik 1	9	1	benotet
2	Informatik 1	9	1	benotet
3	Technische Informatik 1	5	1	benotet
4	Einführung in die Kryptographie 1	5	1	benotet
5	Mathematik 2	9	2	benotet
6	Informatik 2	8	2	benotet
7	Technische Informatik 2	5	2	benotet
8	Einführung in die Kryptographie 2	5	2	benotet
9	Computernetze	5	2	benotet
10	Informatik 3	8	3	benotet
11	Software Engineering	5	3	benotet
12	Elektrotechnik	6	3	benotet
13	Netzsicherheit 1	5	3	benotet
14	Grundlagenpraktikum ITS	3	3	unbenotet
15	Signale und Systeme	5	4	benotet
16	Netzsicherheit 2	5	4	benotet
17	Betriebssysteme	5	4	benotet
18	Einführung in die Usable Security	5	4	benotet
19	Systemsicherheit	5	4	benotet
20	Kryptographie	8	5	benotet
Wahlpflichtbereich				
21	Vertiefungspraktikum/Projektarbeit*	4	5	unbenotet
22	Vertiefungsseminar*	3	5	benotet
23	Vertiefungsmodule**	15	4-5	benotet
Wahlbereich				
24	Freie Wahlfächer***	8	1-6	unbenotet
Praktische Ausbildung				
25	Praktische Ausbildung****	15	6	unbenotet
Abschlussarbeit				
26	Bachelorarbeit und Kolloquium	12 + 3	6	benotet

* Informationen zu den im Semester wählbaren Vertiefungspraktika und Vertiefungsseminaren befinden sich im Vorlesungsverzeichnis.

** Hier müssen Vertiefungsmodule aus dem Bereich der IT-Sicherheit / Informationstechnik im Umfang von mindestens 15 LP gewählt werden. Informationen zu den wählbaren Modulen befinden sich im jeweils aktuellen Modulhandbuch.

*** Hier können (nahezu) alle Veranstaltungen des Vorlesungsverzeichnisses der RUB, sowie Veranstaltungen im Rahmen der Universitätsallianz Ruhr gewählt werden.

**** Hier ist ein Industriepraktikum zu absolvieren.

Angebotene Vertiefungsmodule

	Lehrveranstaltung	Lehreinheit	Umfang (CP)	Semester	Bewertung
Vertiefungsmodule					
	Datenschutz	Informatik	5	WS, nicht im WS 23/24	benotet
	Digitale Forensik	Informatik	5	WS	benotet
	Einführung ins Hardware Reverse Engineering	Informatik	5	WS	benotet
	Implementierung kryptographischer Verfahren	Informatik	5	WS	benotet
	Introduction to Blockchain Security	Informatik	5	WS	benotet
	Kryptographie auf hardwarebasierten Plattformen	Informatik	5	WS	benotet
	Quantum Information and Computation	Informatik	5	WS	benotet
	Web-und Browsersicherheit	Informatik	5	WS	benotet
	Boolesche Funktionen mit Anwendungen in der Kryptographie	Informatik	5	SS	benotet
	Einführung in die künstliche Intelligenz	Informatik	5	SS	benotet
	Highlights of Theoretical Computer Science	Informatik	10	SS	benotet
	Programmanalyse	Informatik	5	SS	benotet
	Public Key Kryptanalyse 1	Informatik	5	SS	benotet
	Autonomous Vehicles and Artificial Intelligence	Informatik	5	Letztmalig SS 23	benotet
	Aufbau eines Managementsystems für Informationssicherheit nach DIN ISO / IEC 27001	Informatik	4	Letztmalig SS 23	benotet
	Information Theory	Informatik	5	Letztmalig SS 23	benotet
	Logik in der Informatik	Informatik	5	Letztmalig WS 22/23	benotet
	Message Level Security	Informatik	5	Letztmalig WS 22/23	benotet
	Model Checking	Informatik	5	Letztmalig SS 23	benotet
	Processor Security	Informatik	5	Letztmalig SS 23	benotet
	Proofs are programs	Informatik	5	Letztmalig SS 23	benotet
	Red- and Blue-Teaming	Informatik	5	Letztmalig SS 23	benotet
	Software Protection	Informatik	5	Letztmalig SS 23	benotet

Angebotene Vertiefungsseminare und Vertiefungspraktika

	Lehrveranstaltung	Lehreinheit	Umfang (CP)	Semester	Bewertung
Vertiefungsseminare					
	Human Centered Security and Privacy	Informatik	3	WS/SS	benotet
	Information Security Seminar	Informatik	3	WS/SS	benotet
	Seminar Netz- und Datensicherheit	Informatik	3	WS/SS	benotet
	Seminar on Applied Privacy and Anonymity	Informatik	3	WS/SS	benotet
	Seminar on Current Topics for Systems Security and Privacy	Informatik	3	WS/SS	benotet
	Seminar Software and Internet Security	Informatik	3	WS/SS	benotet
	Seminar Security Engineering	Informatik	3	WS/SS	benotet
	Seminar zur symmetrischen Kryptographie	Informatik	3	WS/SS	benotet
	Seminar zur Real World Cryptoanalysis	Informatik	3	WS	benotet
	Perlen der theoretischen Informatik (ehemals Grenzen in der theoretischen Informatik)	Informatik	3	WS	benotet
	Seminar Quantum Cryptography	Informatik	3	WS	benotet
	Seminar Ressourceneffiziente Systemsoftware	Informatik	3	WS	benotet
	Perlen der theoretischen Informatik	Informatik	3	WS	benotet
	Seminar Randomisierte Algorithmen	Informatik	3	SS	benotet
	Current topics in microarchitectural security	Informatik	3	SS	benotet
	Fortgeschrittene Themen des Model Checking	Informatik	3	unregelmäßig	benotet
	Seminar Satisfiability	Informatik	3	Letztmalig SS 23	benotet
	Seminar Quantum Algorithms	Informatik	3	Letztmalig SS 23	benotet

	Seminar Implementation Security	Informatik	3	Letztmalig SS 23	benotet
Vertiefungspraktika					
	Bachelor-Vertiefungspraktikum Wireless Physical Layer Security	ETIT	4	WS/SS	unbenotet
	Forschungspraktikum Human-Centred Security	Informatik	4	WS/SS	unbenotet
	Initial Research in Information Security (Bachelor-Project)	Informatik	4	WS/SS	unbenotet
	Praktikum zur Hackertechnik	Informatik	4	WS/SS	unbenotet
	Projekt Netz- und Datensicherheit	Informatik	4	WS/SS	unbenotet
	Projekt Eingebettete Sicherheit	Informatik	4	WS/SS	unbenotet
	Praktikum ARM Processors for Embedded Cryptography	Informatik	4	WS	unbenotet
	Praktikum Implementing Post-Quantum Standards and Challenges	Informatik	4	WS	unbenotet
	Praktikum TLS Implementierung	Informatik	4	WS	unbenotet
	Praktische Kryptanalyse von symmetrischen Chiffren	Informatik	4	SS	unbenotet
	Practical IoT Hacking	Informatik	4	SS	unbenotet
	Practical Course on Blockchain Security	Informatik	4	SS	unbenotet
	Initial Research in Internet Security	Informatik	4	SS	unbenotet
	Initial Research in Software Security	Informatik	4	SS	unbenotet
	Projekt Research in Security Engineering	Informatik	4	SS	unbenotet

Abkürzungen:

ETIT: Fakultät für Elektrotechnik und Informationstechnik

SS: Sommersemester

WS: Wintersemester

CP: Creditpoints

MODULHANDBUCH

Übersicht der Module

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

Pflichtbereich

Usable Security

Mathematik 1

Informatik 1

Technische Informatik 1

Einführung in die Kryptographie 1

Mathematik 2

Mathematik 2

Informatik 2

Technische Informatik 2

Einführung in die Kryptographie 2

Computernetze

Informatik 3

Software Engineering

Elektrotechnik

Netzsicherheit 1

Grundlagenpraktikum ITS

Signale und Systeme

Netzsicherheit 2

Betriebssysteme

Systemsicherheit

Kryptographie

Wahlpflichtbereich

Boolesche Funktionen mit Anwendungen in der Kryptographie

Digitale Forensik

Einführung in die künstliche Intelligenz

Einführung ins Hardware Reverse Engineering

Highlights of Theoretical Computer Science [B.Sc.]

Implementierung kryptographischer Verfahren

Introduction to Blockchain Security

Kryptographie auf hardwarebasierten Plattformen

Programmanalyse [B.Sc.]

Public Key Kryptanalyse 1 [B.Sc]
Quantum Information and Computation
Red- and Blue-Teaming (kein Angebot im SoSe 24)
Web-und Browsersicherheit
Vertiefungspraktikum IT-Sicherheit
Vertiefungsseminar (B.Sc. IT-Sicherheit)

Wahlbereich

Freie Wahlmodule

Praktische Ausbildung

Industriepraktikum IT-Sicherheit

Bachelorarbeit

Abschlussarbeit (B.Sc. IT-Sicherheit)

Titel des Moduls: Usable Security Usable Security					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester 4	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Einführung in die Usable Security and Privacy (211036)			Kontaktzeit 60 h	Selbststudium	Gruppengröße 100 Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Angela Sasse Lehrende: Prof. Dr. Angela Sasse M.A. Jennifer Friedauer					
Verwendung des Moduls B.Sc. IT-Sicherheit/ Informationstechnik M.Sc. IT-Sicherheit/ Netze und Systeme					
Vorkenntnisse Allgemeine Kenntnisse der IT-Sicherheit					
Lernziele (learning outcomes) Die Studierenden verstehen, warum die Usability technischer Systeme entscheidenden Einfluss auf deren Sicherheit haben kann. Darüber hinaus sollen Sie in die Lage versetzt werden, einfache Studien zur Usability selbst durchzuführen.					
Inhalt Diese Veranstaltung vermittelt Kenntnisse der Usable Security und Privacy. Die Themen umfassen insbesondere: <ul style="list-style-type: none"> • Benutzbare Authentifizierung • Nutzer und Phishing • Vertrauen/ Trust, PKI, PGP • Privatheit und Tor-Privacy policies • Design und Auswertung von Benutzerstudien 					
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 180 ECTS) 5/150: B.Sc. IT-Sicherheit/ Informationstechnik [PO 22] 5/149: B.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: Mathematik 1 Mathematics 1					
Modul-Nr./Code	Credits 9 CP	Workload 270 h	Semester	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Mathematik 1 - Grundlagen			Kontaktzeit 105 h	Selbststudium 180 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen Erfolgreiches Bestehen der Modulklausur.		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Gregor Leander Lehrende: Prof. Dr. Gregor Leander					
Verwendung des Moduls Bachelor Informatik Bachelor IT-Sicherheit					
Vorkenntnisse					
Lernziele (learning outcomes) Nach dem erfolgreichen Abschluss des Moduls -kennen Studierende grundlegende Begriffe und Schreibweisen der Mathematik - können Studierende die erlernten Techniken selbstständig anwenden und mathematische Sachverhalte darstellen - kennen Studierende die Grundlagen abstrakter mathematischer Strukturen und verschiedene Beispiele für Gruppen, Ringe und Körper - verstehen die Studierenden den abstrakten Vektorraum-begriff über beliebigen Körpern, können mit linearer Unabhängigkeit, Dimensionen und mit linearen Abbildungen umgehen - sind Studierende in der Lage, lineare Gleichungssysteme explizit zu lösen sowie Eigenwerte und Eigenvektoren zu berechnen					
Inhalt Dieses Modul gibt eine allgemeine Einführung in mathematische Grundlagen und behandelt wichtige Gebiete der Linearen Algebra. Folgende Themengebiete werden behandelt: <ul style="list-style-type: none"> • Grundlagen der Mathematik • Grundlegende mathematische Begriffe • Schreibweisen • Aussagenlogik • Mengenlehre • Relationen Algebraische Grundlagen • ganze Zahlen • Restklassen • Gruppen-, Ringe- und Körper-Axiome Lineare Algebra • Vektorräume • Basen • Dimension • Skalarprodukte • lineare Abbildungen • lineare Gleichungssysteme • Basiswechsel • Determinanten • Eigenwerttheorie 					

Lehrformen

Vorlesung und Übungen

Prüfungsformen

Klausurarbeit (120 Minuten)

Voraussetzungen für die Vergabe von Credits

Erfolgreiches Bestehen der Modulklausur.

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

9/165: B.Sc. Informatik [PO 22]

9/150: B.Sc. IT-Sicherheit [PO 22]

9/149: B.Sc. IT-Sicherheit [PO 20]

Titel des Moduls: Informatik 1 Computer Science 1					
Modul-Nr./Code	Credits 8 CP	Workload 240 h	Semester 1	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Vorlesung und Übung: Informatik 1 (212004)			Kontaktzeit 90 h	Selbststudium 150 h	Gruppengröße 400 Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen keine		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Tobias Glasmachers Lehrende: Prof. Dr. Tobias Glasmachers					
Verwendung des Moduls B.Sc. Informatik [PO 20] B.Sc. IT-Sicherheit [PO 20 + PO 22] B.Sc. Angewandte Informatik [PO 20] B.Sc. Elektrotechnik und Informationstechnik [PO 20 + PO 13]					
Vorkenntnisse keine					
Lernziele (learning outcomes) Nach dem erfolgreichen Abschluss des Moduls <ul style="list-style-type: none"> • kennen die Studierenden die wichtigsten Konzepte imperativer und objektorientierter Programmierung • können die Studierenden eigene Programme entwerfen und implementieren • können die Studierenden mit Grundbegriffen der Informatik wie etwa Korrektheit, Laufzeit, Boolesche Algebra, Invarianten und abstrakten Datentypen arbeiten • sind Studierende in der Lage, die einfachen Datenstrukturen (Arrays, Dictionaries) gezielt einzusetzen und kennen Standardalgorithmen darauf, insbesondere zum Sortieren von Arrays 					
Inhalt Zentrales Thema der Veranstaltung ist das Erlernen der Programmierung und der wichtigsten Programmierkonzepte sowie die ersten Grundbegriffe der Informatik: <ul style="list-style-type: none"> • Imperative Programmierung (Variablen, Kontrollstrukturen, Funktionen und Rekursion, Fehlerbehandlung, Ereignisbehandlung) • Einfache Datenstrukturen (Array und Dictionary) • Objektorientierung (Klassen, Sichtbarkeit, Schnittstellen, Vererbung) • Einführung in eine Reihe von Informatik-Konzepten (Invarianten, Laufzeitanalyse, Sortieralgorithmen, Repräsentation von Daten im Rechner, Boolesche Algebra) Die Veranstaltung nutzt die Programmiersprache TScript ("teaching script") für einen möglichst einfachen und motivierenden Einstieg in die Programmierung. Gegen Ende der Vorlesung erfolgt ein Umstieg auf die Programmiersprache Python.					
Lehrformen Vorlesung und Übungen					
Prüfungsformen Schriftliche Modulabschlussprüfung (150 Minuten)					

Voraussetzungen für die Vergabe von Credits

Bestandene schriftliche Modulabschlussprüfung

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

8/170: B.Sc. Informatik [PO 20]

8/170: B.Sc. Angewandte Informatik [PO 20]

8/150: B.Sc. IT-Sicherheit/ Informationstechnik [PO 22]

8/149: B.Sc. IT-Sicherheit/ Informationstechnik [PO 20]

Titel des Moduls: Technische Informatik 1
Technical Computer Science 1

Modul-Nr./Code	Credits 5 CP	Workload 150 Stunden	Semester siehe Prüfungsordnung	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Rechnerarchitektur (141142)			Kontaktzeit 4 SWS	Selbststudium	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen keine		

Modulbeauftragte/r und hauptamtlich Lehrende

Modulbeauftragte/r: Prof. Philipp Niemann
 Lehrende: Prof. Philipp Niemann

Verwendung des Moduls

B.Sc. Angewandte Informatik
 B.Sc. Informatik
 B.Sc. IT-Sicherheit/ Informationstechnik

Vorkenntnisse

Es werden die Fähigkeit für strukturiertes, algorithmisches Denken sowie das Erfassen von komplexen Abhängigkeiten und Interaktionsmustern vorausgesetzt.

Lernziele (learning outcomes)

Nach dem erfolgreichen Abschluss des Moduls

- kennen die Studierenden Zusammenhänge und haben Detailkenntnisse von den Komponenten und der Funktionsweise moderner Computersysteme. Dies schließt neben dem Prozessor auch das Speichersystem und die Schnittstellen zu weiteren Systemkomponenten ein
- sind die Studierenden auf der Basis dieser Kenntnisse in der Lage, Computersysteme und deren Komponenten bezüglich verschiedener Metriken, wie z.B. Energieverbrauch, Rechenleistung, Speicherperformance etc. auf deren Eignung für eine bestimmte Aufgabe zu bewerten
- haben die Studierenden die grundsätzliche Arbeitsweise und den prinzipiellen Aufbau von Prozessoren auf der Ebene der Mikroarchitektur verstanden und sind in der Lage, den Einfluss von Architekturmerkmalen, wie z.B. Pipelining oder Out-of-Order-Execution, auf die Befehlsausführung zu analysieren

Inhalt

Die Veranstaltung Rechnerarchitektur befasst sich mit dem Aufbau und der Funktion moderner Prozessoren und Computersysteme. Ausgehend von grundlegenden Computerstrukturen wie der Von-Neumann- und der Harvard-Architektur werden der Aufbau, die Klassifizierung und die technische Realisierung von Rechnersystemen dargestellt. Hierbei wird die Programmierung auf Assemblerebene sowie die Verarbeitung von Programmen durch einen Prozessor erläutert. Darauf aufbauend folgen Methoden zur Leistungsbewertung von Prozessoren auf der Basis von standardisierten Benchmarks und verschiedene Metriken, um die Ergebnisse einordnen zu können.

Der inhaltliche Schwerpunkt der Vorlesung stellt die tiefgehende Analyse der Mikroarchitekturebene eines Prozessors dar, wobei sowohl der Datenpfad als auch das Steuerwerk im Rahmen der Vorlesung schrittweise entwickelt und erläutert werden. Auf der Basis des in der Vorlesung vorgestellten Prozessors werden dann moderne Verfahren zur Leistungssteigerung und deren Einsatzgebiete vorgestellt. Neben dem eigentlichen Prozessor wird auch das Speichersystem moderner Computer und verschiedene Schnittstellen zu internen und externen Komponenten des Computersystems behandelt.

Alle Themen werden mit aktuellen Beispielen aus verschiedenen Bereichen der Technik erläutert, sodass neben dem im Detail vorgestellten Beispielprozessor mit MIPS Architektur auch moderne Hochleistungsprozessoren mit x86-64 ISA, Prozessoren für eingebettete Systeme auf Basis der ARM-Architektur, extrem energiesparende

Prozessoren auf Basis des MSP430, wie sie beispielsweise in IoT-Geräten zum Einsatz kommen, und anwendungsspezifische Spezialprozessoren auf Basis der Tensilica Xtensa Plattform vorgestellt werden.

Lehrformen

Vorlesung (als Folien und Tafelvortrag) und Übungen, bei denen die vorgestellten Konzepte und Techniken praktisch umgesetzt werden, teilweise mit Rechnerübungen.

Prüfungsformen

Schriftliche Modulabschlussprüfung (120 Minuten)

Voraussetzungen für die Vergabe von Credits

Bestandene schriftliche Modulabschlussprüfung.

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

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

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

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

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

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

Titel des Moduls: Einführung in die Kryptographie 1					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Einführung in die Kryptographie 1 (212010)			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße 300 Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen keine		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr.-Ing. Christof Paar Lehrende: Prof. Dr.-Ing. Christof Paar					
Verwendung des Moduls B.Sc. IT-Sicherheit B.Sc. Informatik B.Sc. Angewandte Informatik M.Sc. IT-Sicherheit/ Netze und Systeme					
Vorkenntnisse					
Lernziele (learning outcomes) Nach erfolgreichem Abschluss des Moduls verfügen die Studierenden über Kenntnisse der grundlegenden Anwendungen symmetrischer Verfahren und über Grundkenntnisse der asymmetrischen Kryptographie. Sie können entscheiden, unter welchen Bedingungen man in der Praxis bestimmte Verfahren einsetzt und wie die Sicherheitsparameter zu wählen sind. Mit den Grundlagen des abstrakten Denkens in der IT Sicherheitstechnik sind sie vertraut. Zum anderen erreichen die Studierenden durch Beschreibungen ausgewählter praxisrelevanter Algorithmen, wie z. B. des AES- oder RSA-Algorithmus, ein algorithmisches und technisches Verständnis zur praktischen Anwendung. Die Studierenden erhalten dabei einen Überblick über in der Praxis eingesetzten Lösungen. Sie sind in der Lage, argumentativ eine bestimmte Lösung zu verteidigen. Die Vorlesungen werden auch als Videos in Deutsch und Englisch angeboten. Die Studierenden können daher durch das zweisprachige eLearning-Angebot Sprachkompetenzen in der Wissenschaftssprache Englisch erwerben.					
Inhalt Das Modul bietet einen allgemeinen Einstieg in die Funktionsweise moderner Kryptographie und ihrer Bedeutung für die IT-Sicherheit. Es werden grundlegende Begriffe und mathematisch/technische Verfahren der Kryptographie erläutert. Praktisch relevante symmetrische und asymmetrische Verfahren und Algorithmen werden vorgestellt und an praxisrelevanten Beispielen erläutert. Die Vorlesung lässt sich in zwei Teile gliedern: Die Grundlagen der symmetrischen Kryptographie einschließlich der Beschreibung einiger historischer Verschlüsselungsverfahren (Caesar Chiffre, Affine Chiffre), aktueller symmetrischer Verfahren (AES, 3-DES) und grundlegender Konzepte wie dem One-Time-Pad und Stromchiffren werden im ersten Teil behandelt. Benötigte mathematische Grundlagen, insbesondere modulares Rechnen und endliche Körper, werden ebenfalls aus					

Anwendersicht eingeführt.

Der zweite Teil besteht aus einer Einführung in die asymmetrische Kryptographie und der Vorstellung eines ihrer wichtigsten Stellvertreter, dem RSA-Verfahren. Hierzu wird eine Einführung in die Grundlagen der Zahlentheorie durchgeführt, die für die asymmetrische Kryptoverfahren relevant sind (u. a. Ringe ganzer Zahlen und der euklidische Algorithmus).

In beiden Vorlesungsteilen werden aktuelle Sicherheitseinschätzungen und Implementierungsaspekte der vorgestellten Chiffren auch jeweils diskutiert.

Lehrformen

Vorlesung mit Übung

Prüfungsformen

Klausurarbeit (120 Minuten)

Voraussetzungen für die Vergabe von Credits

Erfolgreiches Bestehen der Modulklausur.

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

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

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

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

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

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

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

5/96 : M.Sc. IT-Sicherheit/ Netze und Systeme [PO20]

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

Titel des Moduls: Mathematik 2 Mathematics 2					
Modul-Nr./Code	Credits 9 CP	Workload 270 h	Semester 2	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Mathematik 2 - Algorithmische Mathematik			Kontaktzeit 105 h	Selbststudium 180 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen keine		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Christian Stump Lehrende: Prof. Dr. Christian Stump					
Verwendung des Moduls B.Sc. Informatik B.Sc. IT-Sicherheit					
Vorkenntnisse					
Lernziele (learning outcomes) Nach dem erfolgreichen Abschluss des Moduls <ul style="list-style-type: none"> • kennen Studierende grundlegende Begriffe, Beweismethoden und Algorithmen aus der elementaren Zahlentheorie • können Studierende die Beweistechniken selbstständig anwenden und mathematische Sachverhalte darstellen • kennen Studierende erste Sätze und Methoden aus der Kombinatorik und insbesondere aus der Graphentheorie und verstehen deren strukturelle Eigenschaften • kennen Studierende erste fundamentale Algorithmen aus der Zahlentheorie und der Kombinatorik, können diese formalisieren, selbstständig implementieren sowie deren Laufzeiten analysieren 					
Inhalt Diese Lehrveranstaltung behandelt die folgenden Themen: - Euklidischer Algorithmus, Gruppen-, Ring-, Körperaxiome, Symmetriegruppen, Polynomarithmetik, formale Potenzreihen, modulare Arithmetik, Lemma von Bezout, Kleiner Satz von Fermat, diskreter Logarithmus, RSA-Verschlüsselungsverfahren, Primzahltests, Chinesischer Restesatz, p-adische Brüche, Newton-Verfahren, Asymptotische Notation durch Landausymbole, Binomialkoeffizienten, Rekursionsgleichungen, Erzeugendefunktionen, Prinzip der Inklusion-Exklusion, Vier-FarbenProblem, Dijkstra-Algorithmus, Satz von Cayley, Hamiltonkreise, Google PageRank Algorithmus, Satz von Perron-Frobenius. Konkrete Algorithmen werden in Computeralgebra-Systemen implementiert.					
Lehrformen Vorlesung mit Übungen					
Prüfungsformen Schriftliche Modulabschlussprüfung über 180 Minuten					
Voraussetzungen für die Vergabe von Credits Bestandene Modulabschlussprüfung und erfolgreiche Teilnahme an den praktischen Übungen am Rechner					

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

9/165: B.Sc. Informatik [PO 22]

9/158: B.Sc. Informatik [PO 20]

9/150: B.Sc. IT-Sicherheit [PO 22]

9/149: B.Sc. IT-Sicherheit [PO 20]

Titel des Moduls: Mathematik 2 Mathematics 2					
Modul-Nr./Code	Credits 9 CP	Workload 270 h	Semester 2	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Logik in der Informatik (212013) und Wahrscheinlichkeit in der Informatik (212028)			Kontaktzeit 90 h	Selbststudium 180 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Thomas Zeume Lehrende: Prof. Dr. Thomas Zeume, Prof. Dr. Alex May					
Verwendung des Moduls B.Sc. Informatik					
Vorkenntnisse					
Lernziele (learning outcomes) Nach dem erfolgreichen Abschluss des Moduls <ul style="list-style-type: none"> • kennen die Studierenden lernen wie sich Problemstellungen durch geeignete logische Systeme modellieren lassen, • beherrschen die Studierenden Syntax und Semantik verschiedener logischer Systeme und können diese nutzen, • kennen die Studierenden einige klassische logische Kalküle und und können diese durchführen, • haben die Studierenden ein grundlegendes Verständnis für die Logik-Programmierung entwickelt und können insbesondere einfache Sachverhalte durch Prolog-Programme ausdrücken. • kennen die Studierende grundlegende Begrifflichkeiten der Wahrscheinlichkeitstheorie wie Zufallsvariablen, sowohl im Diskreten als auch im Kontinuierlichen, und können diese sicher anwenden. • beherrschen Studierende die Bestimmung von Momenten, wie dem Erwartungswert und der Varianz, im Diskreten mit Hilfe der Technik der z-Transformation. • erlernen Studierende verschiedene für die Informatik bedeutende Verteilungen wie die Binomial-, Geometrische, Poisson, Uniforme, Exponential- und Normal-Verteilung und können diese sicher anwenden. • sind Studierende in der Lage, die vorgestellten Techniken mit Hilfe der Computer-Algebra Sage in Python zu implementieren. 					
Inhalt Logische Methoden spielen in vielen modernen Anwendungen der Informatik eine wichtige Rolle und der vielfältige Einsatz von Zufallsbits ist grundlegend für die Entwicklung effizienter Algorithmen. Aus Datenbanken werden relevante Informationen mit Hilfe auf Logik basierender Anfragesprachen extrahiert; die formale Verifikation von Software und Hardware basiert auf logischen Spezifikationssprachen und Algorithmen für diese; und Methoden für das automatisierte Schlussfolgern in der künstlichen Intelligenz haben ihre Grundlage in der formalen Logik. In diesem Modul werden die formalen Grundlagen von modernen Logiken behandelt, mit einem Fokus auf ihrer Anwendung in der Informatik. Neben der klassischen Aussagenlogik und Prädikatenlogik betrachten wir auch					

Modallogik. Für jede dieser Logiken formalisieren wir Syntax und Semantik, lernen wie sich informatische Szenarien in ihnen modellieren lassen, und betrachten Algorithmen und Kalküle für Unerfüllbarkeit und Folgerungsbeziehung.

Für viele zentrale Probleme der Informatik sind Lösungen überhaupt nur mit Hilfe von Zufallsbits bekannt. Oft beschleunigen Zufallsbits Algorithmen, oder erlauben eine besonders elegante Analyse der Korrektheit bzw. der Laufzeit. Das Modul verschafft einen Überblick über die vielfältigen Einsatzmöglichkeiten von Zufallsbits im Algorithmen-Design. Die Studierenden erlernen Techniken zum Einsatz von Zufallsbits in Algorithmen (sogenannte probabilistische Algorithmen), sowohl bei der Korrektheits- als auch bei der Laufzeit-Analyse, und implementieren diese in einem Computeralgebra-System.

Lehrformen

Hörsaalvorlesung mit Medienunterstützung, Tutorien als seminaristischer Unterricht, zusätzlich Selbststudium mit ergänzend bereitgestellten Materialien und Aufgaben

Prüfungsformen

Schriftliche Modulabschlussprüfung über 180 Minuten

Voraussetzungen für die Vergabe von Credits

Bestandene schriftliche Modulabschlussprüfung

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

9/158: B.Sc. Informatik [PO 22]

9/170: B.Sc. Informatik [PO 20]

Titel des Moduls: Informatik 2 Computer Science 2					
Modul-Nr./Code	Credits 8 CP	Workload 240 h	Semester 2	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Informatik 2 - Algorithmen und Datenstrukturen (211002)			Kontaktzeit 90 h	Selbststudium 150 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen keine		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Maike Buchin Lehrende: Prof. Maike Buchin					
Verwendung des Moduls B.Sc. Informatik B.Sc. Angewandte Informatik B.Sc. IT-Sicherheit/ Informationstechnik					
Vorkenntnisse Inhalte der Module Informatik 1 und Mathematik 1 bzw. Höhere Mathematik 1, insbesondere Programmieren und lineare Algebra					
Lernziele (learning outcomes) Nach dem erfolgreichen Abschluss des Moduls: <ul style="list-style-type: none"> • können Studierende Algorithmen formal beschreiben und deren Korrektheit beweisen • können Studierende die Laufzeit und den Speicherbedarf von Algorithmen und Datenstrukturen analysieren und bewerten • kennen Studierende grundlegende Datenstrukturen • kennen Studierende grundlegende Schemata zum Entwurf von Algorithmen sind Studierende in der Lage, Algorithmen und Datenstrukturen für spezifische Probleme zu entwickeln • haben die Studierenden die Grundlagen der Programmiersprache Python kennengelernt 					
Inhalt Die Vorlesung gibt einen systematischen Überblick über den Entwurf und die Analyse von Algorithmen und Datenstrukturen. Dazu werden zunächst grundlegende Methoden der Analyse (insbesondere Korrektheit, Laufzeit und Speicherbedarf) von Algorithmen vorgestellt. Anschließend werden einige Algorithmen zum Sortieren und Suchen analysiert. Ebenfalls werden verschiedene grundlegende Datenstrukturen (Listen, Felder, Suchbäume und Heaps) vorgestellt. Schließlich werden Graphen betrachtet, und zwar ihre Darstellung und diverse Algorithmen auf Graphen (Durchläufe, kürzeste Wege, minimale Spannbäume). In den Übungen lernen die Studierenden sowohl die theoretische Analyse von Algorithmen und Datenstrukturen als auch deren praktische Umsetzung in eine moderne Programmiersprache (z.B. Python).					
Lehrformen Hörsaalvorlesung mit Medienunterstützung und theoretische sowie praktische Übungen am Rechner					
Prüfungsformen Schriftliche Modulabschlussprüfung über 150 Minuten					
Voraussetzungen für die Vergabe von Credits Bestandene schriftliche Modulabschlussprüfung					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)					

8/158: B.Sc. Informatik [PO 22]

8/165: B.Sc. Informatik [PO 20]

8/168: B.Sc. Angewandte Informatik [PO 22]

8/170: B.Sc. Angewandte Informatik [PO 20]

8/150: B.Sc. IT-Sicherheit/ Informationstechnik [PO 22]

8/149: B.Sc. IT-Sicherheit/ Informationstechnik [PO 22]

Titel des Moduls: Technische Informatik 2					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Digitaltechnik für ITS und Informatik (211014, ab SoSe 23) Digitaltechnik (141304, bis SoSe 22)			Kontaktzeit 60 h	Selbststudium 90	Gruppengröße Studierende
Unterrichtssprache Deutsch, Vorlesungs- und Übungsfolien auf Englisch			Teilnahmevoraussetzungen keine		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Tim Güneysu Lehrende: Prof. Dr. Tim Güneysu					
Verwendung des Moduls B.Sc. Informatik B.Sc. IT-Sicherheit					
Vorkenntnisse Inhalte des Moduls Mathematik 1 – Grundlagen. Vorausgesetzt wird ein generelles Interesse an technischen Systemen, die Fähigkeit zu strukturieren, algorithmischem Denken sowie die Fähigkeit zum Erfassen von komplexen Abhängigkeiten und Interaktionsmustern.					
Lernziele (learning outcomes) Nach erfolgreichem Abschluss des Moduls haben die Studierenden umfassende Kenntnisse in Boolescher Algebra, Struktur und Funktionsweise grundlegender digitaler Schaltungen, Kostenoptimierung digitaler Funktionsgruppen, Techniken zur takt-synchronen Verarbeitung von Daten, Kodierung und Verarbeitung von Daten, Struktur und Funktionsweise solcher Grundfunktionalitäten, die insbesondere in Mikroprozessorarchitekturen zentrale Bestandteile sind, erworben. Die Studierenden sind in der Lage, grundlegende Schaltungskonzepte digitaler Logik- und Funktionsblöcke zu verstehen, ihr Zusammenspiel zu analysieren, die Funktionalität zu bewerten und einfache Blöcke selbst zu entwickeln. Weiterhin werden die Bewertung und Entwicklung von mehrstufigen kombinatorischen Logikblöcken sowie von Finite State Machines (FSMs) behandelt. Die Studierenden erlernen die Hardwarebeschreibungssprache Verilog, und zu jedem Thema der Vorlesung werden Verilog-Beispiele gegeben. Die Vorlesung befasst sich ausschließlich mit (takt-)synchronen Schaltungen.					
Inhalt Der Kurs gibt einen systematischen Überblick über die folgenden Themen: Boolesche Algebra, Realisierung boolescher Funktionen, Minimierung boolescher Funktionen, Multiplexer, Kodierer, Dekodierer, fehlererkennende und fehlerkorrigierende Codes, Addierer, Subtrahierer, Multiplizierer, Hardwarebeschreibungssprache Verilog, Speicherelemente (Flipflops), sequentielle Schaltungen, Zähler, Schieberegister, RAM, Finite State Machines (FSMs), Timing-Analyse sequentieller Schaltungen, und kurzer Überblick über FPGAs.					
Lehrformen Die Vorlesung wird als seminaristischer Unterricht abgehalten, die Übungen entweder am Rechner oder mit Stift und Papier.					
Prüfungsformen Schriftliche Modulabschlussprüfung über 120 Minuten					

Voraussetzungen für die Vergabe von Credits

Bestandene Modulabschlussprüfung und erfolgreiche Teilnahme an Übungen

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 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]

Titel des Moduls: Einführung in die Kryptographie 2

Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Einführung in die Kryptographie 2 (211009)			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße 300 Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen Keine		

Modulbeauftragte/r und hauptamtlich Lehrende

Modulbeauftragte/r: Prof. Dr.-Ing. Christof Paar
Lehrende: Prof. Dr.-Ing. Christof Paar

Verwendung des Moduls

B.Sc. IT-Sicherheit
B.Sc. Informatik
B.Sc. Angewandte Informatik
M.Sc. IT-Sicherheit/ Netze und Systeme

Vorkenntnisse

Inhalte der Vorlesung "Einführung in die Kryptographie 1"

Lernziele (learning outcomes)

Nach erfolgreichem Abschluss des Moduls verfügen die Studierenden über Kenntnisse der grundlegenden Anwendungen asymmetrischer und hybrider Verfahren. Sie können entscheiden, unter welchen Bedingungen man in der Praxis bestimmte Verfahren einsetzt und wie die Sicherheitsparameter zu wählen sind. Mit den Grundlagen des abstrakten Denkens in der IT Sicherheitstechnik sind sie vertraut. Zum anderen erreichen die Studierenden durch Beschreibungen ausgewählter praxisrelevanter Algorithmen, wie z.B. des Diffie-Hellmann-Schlüsselaustausch oder ECC-basierten Verfahren, ein algorithmisches und technisches Verständnis zur praktischen Anwendung. Die Studierenden erhalten dabei einen Überblick über die in Unternehmen eingesetzten Lösungen. Sie sind in der Lage, argumentativ eine bestimmte Lösung zu verteidigen. Die Vorlesungen werden zusätzlich auch als Videos in Deutsch und Englisch angeboten. Die Studierenden können daher durch das zweisprachige eLearning-Angebot Sprachkompetenzen in der Wissenschaftssprache Englisch erwerben.

Inhalt

Das Modul bietet einen allgemeinen Einstieg in die Funktionsweise moderner Kryptografie und Datensicherheit. Es werden grundlegende Begriffe und mathematisch/technische Verfahren der Kryptografie und der Datensicherheit erläutert. Praktisch relevante asymmetrische Verfahren und Algorithmen werden vorgestellt und an praxisrelevanten Beispielen erläutert. Die Vorlesung lässt sich in zwei Teile gliedern:

Der erste Teil beginnt mit einer Einleitung zu asymmetrischen Verfahren und deren wichtigsten Stellvertretern (Diffie-Hellman, elliptische Kurven). Der Schwerpunkt liegt auf der algorithmischen Einführung der asymmetrischen Verfahren, die sowohl Verschlüsselungsalgorithmen als auch digitale Signaturen beinhalten. Abgeschlossen wird dieser Teil durch Hashfunktionen, die eine große Rolle für digitalen Signaturen und Message Authentication Codes (MACs oder kryptografische Checksummen) spielen.

Im zweiten Teil der Vorlesung werden Grundlagen von Sicherheitslösungen aufbauend auf den Konzepten der symmetrischen und asymmetrischen Kryptographie besprochen. Dabei wird vor allem auf die in Unternehmen

notwendigen und eingesetzten Lösungen (PKI, digitale Zertifikate etc.) eingegangen.

Lehrformen

Vorlesung mit Übungen

Prüfungsformen

Klausurarbeit (120 Minuten)

Voraussetzungen für die Vergabe von Credits

Bestandene schriftliche Modulabschlussprüfung.

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

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

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

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

5/158: B.Sc. Informatik [PO 20]

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

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

5/96 : M.Sc. IT-Sicherheit / Netze und Systeme [PO20]

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

Titel des Moduls: Computernetze Computer Networks					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester 2	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Computernetze (211006)			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße 400 Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Dr.-Ing. Christian Mainka Lehrende: Dr.-Ing. Christian Mainka					
Verwendung des Moduls B.Sc. Informatik B.Sc. Angewandte Informatik B.Sc. IT-Sicherheit / Informationstechnik					
Vorkenntnisse					
Lernziele (learning outcomes) Nach dem erfolgreichen Abschluss des Moduls <ul style="list-style-type: none"> • kennen Studierende die wichtigsten Standards, die das heutige Internet verwendet. • kennen Studierende grundlegende Angriffskonzepte auf Computernetzwerke • verstehen Studierende den Zusammenhang zwischen den einzelnen Schichten eines Computernetzwerks und der darin enthaltenen Protokolle • können Studierende die wichtigsten Netzwerktools für Analysezwecke anwenden 					
Inhalt Die Vorlesung gibt eine Einführung in grundlegenden Protokolle und Anwendungen von Computernetzen. Der Schwerpunkt der Vorlesung liegt auf Standardprotokollen und -Algorithmen, wie sie in modernen Computernetzwerken (zum Beispiel im Internet) eingesetzt werden. Anhand eines Schichtenmodells werden die wichtigsten Grundlagen nach dem Top-Down Ansatz vorgestellt und analysiert. Dazu gehören zum Beispiel auf der obersten Schicht DNS und HTTPS im Application Layer; TCP und UDP im Transport Layer; IPv4/IPv6 und Routing Algorithmen im Network Layer; sowie MAC und ARP im untersten Link Layer. Neben der reinen Funktionsweise dieser Standards werden Sicherheitsaspekte auf allen Schichten betrachtet. Ergänzend zur Vorlesung werden Übungsaufgaben über die eLearning Plattform Moodle gestellt und in der Übungsstunde besprochen. Weiterhin wird in jeder Übung ein "Tool der Woche" vorgestellt. Dabei handelt es sich jeweils um eine spezielle Software, die man als "Netzwerker" unbedingt kennen sollte (z.B. traceroute, nmap, ...). Alle besprochenen Tools sind frei verfügbar und werden den Studenten als eine Lernplattform (virtuelle Maschine) zur Verfügung gestellt. Als Primärliteratur wird "Computernetzwerke: Der Top-Down Ansatz" von Kurose und Ross (Pearson Verlag) verwendet.					
Lehrformen Moodle-Unterstützte Hausaufgaben mit praxisnahen, computerunterstützten Übungen. Tool-der-Woche: Vorstellung, Einarbeitung, und Verwendung von Netzwerkrelevanten Computer analysetools.					
Prüfungsformen schriftliche Modulabschlussprüfung von 120 min					

Voraussetzungen für die Vergabe von Credits

Bestandene schriftliche Modulabschlussprüfung

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

Titel des Moduls: Informatik 3 Computer Science 3					
Modul-Nr./Code	Credits 8 CP	Workload 240 h	Semester 3	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Informatik 3 - Theoretische Informatik (212002)			Kontaktzeit 90 h	Selbststudium 150 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen keine		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Thomas Zeume Lehrende: Prof. Dr. Thomas Zeume					
Verwendung des Moduls B.Sc. Informatik B.Sc. Angewandte Informatik B.Sc. IT-Sicherheit/ Informationstechnik					
Vorkenntnisse					
Lernziele (learning outcomes) Nach dem erfolgreichen Abschluss des Moduls <ul style="list-style-type: none"> • beherrschen die Studierenden den professionellen Umgang mit Berechnungsmodellen und ihren Beziehungen zu Sprachklassen. Dazu gehört die intellektuelle und methodische Fähigkeit, den Nachweis der Zugehörigkeit bzw. Nichtzugehörigkeit zu einer solchen Klasse zu führen. • ist durch Einüben von Beweistechniken wie wechselseitige Simulation oder berechenbare Reduktionen bei den Studierenden die Einsicht gereift, dass an der Oberfläche verschieden aussehende Konzepte im Kern identisch sein können. Zudem erlaubt dies den Studierenden, neue Anwendungsprobleme selbstständig zu klassifizieren. • haben die Studierenden mit der Turingmaschine ein einfach handhabbares Rechnermodell erlernt, das ihnen fortan als Abstraktion für alle möglichen Rechner dient. • haben die Studierenden fundamentale Einsichten erlangt, welche Probleme mithilfe von Rechnern effizient entschieden, zum Teil entschieden oder prinzipiell nicht entschieden werden können. Dadurch erlangen Sie ein tieferes Verständnis von der Komplexität von Berechnungsproblemen. 					
Inhalt Die Lehrveranstaltung gibt einen systematischen Überblick über die folgenden Themengebiete: <ul style="list-style-type: none"> • Endliche Automaten und reguläre Ausdrücke • Kellerautomaten und kontextfreie Grammatiken • Turingmaschinen und Entscheidbarkeit • Nichtdeterminismus und NP-Vollständigkeitstheorie 					
Lehrformen Hörsaalvorlesung mit Medienunterstützung und Übungen, bei denen die vorgestellten Konzepte und Techniken praktisch umgesetzt werden, teilweise mit Rechnerübungen.					
Prüfungsformen Schriftliche Modulabschlussprüfung (180 Minuten)					

Voraussetzungen für die Vergabe von Credits

Bestandene schriftliche Modulabschlussprüfung

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

8/165: B.Sc. Informatik [PO 22]

8/158: B.Sc. Informatik [PO 22]

8/168: B.Sc. Angewandte Informatik [PO 22]

8/170: B.Sc. Angewandte Informatik [PO 20]

8/150: B.Sc. IT-Sicherheit/ Informationstechnik [PO 22]

8/149: B.Sc. IT-Sicherheit/ Informationstechnik [PO 20]

Titel des Moduls: Software Engineering Software Engineering					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester 3	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen 212000: Software Engineering			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße 350 Studierende
Unterrichtssprache			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Thorsten Berger Lehrende: Prof. Dr. Thorsten Berger					
Verwendung des Moduls					
Vorkenntnisse					
Lernziele (learning outcomes)					
Inhalt					
Lehrformen					
Prüfungsformen					
Voraussetzungen für die Vergabe von Credits					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 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] 5/150: B.Sc. IT-Sicherheit/Informationstechnik [PO22] 5/149: B.Sc. IT-Sicherheit/Informationstechnik [PO20]					

Titel des Moduls: Elektrotechnik					
Modul-Nr./Code 149034	Credits 6 CP	Workload 180 h	Semester 1. Semester (BaET)	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Elektrotechnik 1 - Elektrische Netzwerke			Kontaktzeit 75 h	Selbststudium 105 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen Keine		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr.-Ing. Ilona Rolfes Lehrende: Prof. Dr.-Ing. Ilona Rolfes					
Verwendung des Moduls B.Sc. IT-Sicherheit (PO 20 + PO22)					
Vorkenntnisse <p>Empfohlene Vorkenntnisse</p> Ma­the­ma­ti­sche Vor­kennt­nis­se über die Grund­la­gen der Dif­fe­ren­ti­al- und In­te­gral­rech­nung sowie der Li­nea­ren Al­ge­bra 					
Lernziele (learning outcomes) Die Studierenden beherrschen die Grundlagen und Gesetze zur Berechnung von Strömen und Spannungen in elektrischen Gleich- und Wechselstromkreisen. Sie haben die Fähigkeit, elektrische Netzwerke zu analysieren, mathematisch korrekt zu beschreiben und umzuwandeln. Sie haben die Grundlagen der komplexen Wechselstromrechnung verstanden und können diese auf praktische Beispiele anwenden.					
Inhalt <ul style="list-style-type: none"> Lineare Gleichstromschaltungen: Zählpfeile; Strom- und Spannungsquellen; Die Kirchhoff'schen Gleichungen; einfache Widerstandsnetzwerke (Spannungsteiler, Stromteiler); reale Strom- und Spannungsquellen; Wechselwirkungen zwischen Quelle und Verbraucher (Zusammenschaltung von Spannungsquellen, Leistungsanpassung, Wirkungsgrad); Superpositionsprinzip; Analyse umfangreicher Netzwerke. Übergang zu zeitabhängigen Strom und Spannungsformen: Übersicht sowie Einführung verschiedener Kenngrößen (Mittelwert, Gleichrichtwert, Effektivwert, Maximalwert, Spitzenwert, Spitze-Spitze-Wert, Schwingungsbreite). Wechselstrom und Wechselspannung: Das Zeigerdiagramm; Komplexe Wechselstromrechnung; Beschreibung konzentrierter RLC Bauelemente und idealer Quellen; Einführung der Ortskurven; Berechnung einfacher Wechselstromkreise über die komplexe Ebene; Energie und Leistung bei Wechselspannung; Leistungsanpassung. Analyse von Netzwerken: Maschenstromverfahren; Knotenpotenzialverfahren. Einführung zu Zweitoren: Torbedingung; Zweitorgleichungen in Matrixform (Impedanz-, Admittanz-, Hybrid-, Kettenform); Zweitoreigenschaften (Reziprozität, Symmetrie); Matrizen elementarer Zweitore. 					
Lehrformen Vorlesung und Übungen					
Prüfungsformen Klausurarbeit (120 Minuten)					
Voraussetzungen für die Vergabe von Credits Erfolgreiches Bestehen der Modulklausur.					

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

6/149: B.Sc. IT-Sicherheit [PO 22]

6/150: B.Sc. IT-Sicherheit [PO 22]

Titel des Moduls: Netzsicherheit 1

Network Security 1

Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester 3. Semester	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Netzsicherheit 1 (212012)			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen		

Modulbeauftragte/r und hauptamtlich Lehrende

Modulbeauftragte/r: Prof. Jörg Schwenk
Lehrende: Prof. Dr. Jörg Schwenk

Verwendung des Moduls

B.Sc. IT-Sicherheit / Informationstechnik
M.Sc. IT-Sicherheit / Netze und Systeme
M.Sc. Angewandte Informatik

Vorkenntnisse

Grundkenntnisse in TCP/IP, Grundkenntnisse der Sicherheitstechnik, Kenntnisse der Grundlagen von Kommunikationssystemen auf dem Niveau der Informatik, insbesondere der Fachinformatiker (z.B. c't).

Lernziele (learning outcomes)

Studierende verfügen nach erfolgreichem Abschluss des Moduls über ein umfassendes Verständnis der technischen Aspekte von Netzsicherheit. Sie haben erkannt, dass Kryptographie alleine nicht ausreicht, um sicherheitstechnische Probleme zu lösen. Sie haben ein umfassendes Systemverständnis für komplexe IT-Systeme erworben. Durch eigenständige Überlegungen zur Verbesserung der Netzsicherheit bereiten sich die Studierenden auf ihre Rolle im Berufsleben vor. Sie können neue Probleme analysieren und neue Lösungsmöglichkeiten entwickeln. Sie können im Gespräch den Nutzen der von ihnen erarbeiteten Lösungen argumentativ begründen. Sie haben verstanden, dass nicht-technische Faktoren wie Fragen der Haftung und der entstehenden Kosten Entscheidungen zur IT-Sicherheit maßgeblich mit beeinflussen.

Inhalt

You can find our Moodle course via the [Moodle Search](#)

Wenn Kryptographie in einer technischen Umgebung wie einem Computer-, Daten- oder Telefonnetz eingesetzt wird, hängt die Sicherheit außer von rein kryptographischen Faktoren auch von der technischen Einbettung der Verschlüsselungs- und Signaturalgorithmen ab. Prominente Beispiele (für fehlerhafte Einbettungen) sind EFAIL (efail.de), Angriffe auf die WLAN-Verschlüsselungssysteme WEP und WPA (KRACK) und diverse Angriffe auf TLS (Bleichenbacher, POODLE, DROWN, ROBOT). Das Modul „Netzsicherheit 1“ beschäftigt sich mit konkreten Netzen zur Datenübertragung und beleuchtet diese von allen Seiten auf ihre Sicherheit hin. Es umfasst folgende Teile:

- Einführung: Internet
- Einführung: Vertraulichkeit
- Einführung: Integrität
- Einführung: Kryptographische Protokolle
- PPP-Sicherheit (insb. PPTP), EAP-Protokolle
- WLAN-Sicherheit (WEP, WPA, Wardriving, KRACK)
- GSM- und UMTS-Mobilfunk (Authentisierung und Verschlüsselung)
- IPSec (ESP und AH, IKEv1 und v2, Angriffe auf IPSec)
- Dateiverschlüsselung mit OpenPGP (Datenformat, Efail, Klima-Rosa)

- E Mail-Verschlüsselung mit S/MIME (SMTP, Datenformat, Efail, POP3, IMAP)

Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studierenden stellen selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit an.

Lehrformen

Den aktuellen Moodle Kurs finden Sie über die [Moodle Suche](#)

Der Inhalt der Vorlesung wird über Youtube-Videos und Materialien in Moodle zur Verfügung gestellt. Ergänzend dazu gibt es in Präsenz eine Vertiefungsvorlesung. Dort werden keine neuen Themen vorgestellt, sondern die Themen der Online-Materialien werden vertiefend behandelt. Ob eine Aufzeichnung der Präsenzveranstaltung möglich ist, muss noch geklärt werden. Durch diese Mischform aus Online-Materialien und Vertiefung in Präsenz soll die Teilnahme aller Studierenden auch bei möglicherweise erhöhtem Krankenstand im Winter gewährleistet werden.

Prüfungsformen

Schriftliche Modulabschlussprüfung (120 Minuten)

Voraussetzungen für die Vergabe von Credits

Bestandene schriftliche Modulabschlussprüfung

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

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

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: Grundlagenpraktikum ITS					
Modul-Nr./Code	Credits 3 CP	Workload	Semester 3	Turnus jedes Semester	Dauer 1 Semester
Lehrveranstaltungen			Kontaktzeit	Selbststudium 45 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen Anmeldung über FlexNow Für Studierende, die in der PO 2020 eingeschrieben sind, ist die Anmeldung zum Grundlagenpraktikum ITS erst nach erfolgtem Beratungsgespräch möglich.		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Jörg Schwenk Lehrende: M. Sc. Dominik Noss					
Verwendung des Moduls B.Sc. IT-Sicherheit/Informationstechnik					
Vorkenntnisse Grundlagen der Bedienung eines Computers werden vorausgesetzt. Programmierkenntnisse sind hilfreich.					
Lernziele (learning outcomes) Die Studierenden kennen praktische Aspekte der IT-Sicherheit sowie der (Un-)Sicherheit konkreter Verfahren und Produkte.					
Inhalt					
ZIELE:					
Die Studierenden kennen praktische Aspekte der IT-Sicherheit sowie der (Un-)Sicherheit konkreter Verfahren und Produkte.					
INHALT:					
In 10 Versuchen und 2 Ersatzversuchen wird eine praktische Einführung in die IT-Security gegeben. Jeder Versuch muss anhand eines Handouts vorbereitet werden, und eine kurze Versuchsauswertung muss abgegeben werden. Die Themen umfassen zur Zeit (Anpassungen aufgrund aktueller Entwicklungen sind möglich):					
<ul style="list-style-type: none"> • Kryptographische Angriffe auf RSA • Angriffe in geschichteten Netzwerken • Buffer Overflow Attacken • Forensische Analyse eines Ransomware-Angriffs • PDF-Security • Programmatische Analyse von Netzwerkdaten mit LibPcap • Einführung in Linux • MD5 Kollisionen in Postscript • Netzwerk-Analyse mit nmap & Wireshark • Phishing 					

- Web Angriffe

Die Themen werden in Zweierteams bearbeitet. Jedes Team fertigt zum nächsten Praktikumstermin eine schriftliche Versuchsauswertung nach den Auswertungshinweisen an. Alle schriftlichen Versuchsauswertungen sind bei den jeweiligen Betreuenden abzugeben.

EINFÜHRUNGSVERANSTALTUNG

Wichtige Informationen zur Durchführung erhalten Sie bei der Einführungsveranstaltung. Diese findet via Zoom statt. Teilnahme an der Einführungsveranstaltung ist verpflichtend und wichtig für den reibungslosen Ablauf des Praktikums!

WINTERSEMESTER vs. SOMMERSEMESTER

Das Grundlagenpraktikum ITS wird in allen Semestern angeboten.
Im **Sommersemester** gibt es **einen** wöchentlichen Termin.
Im **Wintersemester** gibt es **drei** wöchentliche Termine.

Lehrformen

Praktikum

Prüfungsformen

Praktikum

Voraussetzungen für die Vergabe von Credits

Das Praktikum ist bestanden, sobald 10 Versuche bestanden wurden

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

unbenotet

Titel des Moduls: Signale und Systeme					
Modul-Nr./Code 149056	Credits 5 CP	Workload 150 h	Semester 2. Semester (PO20) 4. Semester (PO22)	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Systemtheorie 1 - Signale und Systeme			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr.-Ing. Rainer Martin Lehrende: Prof. Dr.-Ing. Rainer Martin					
Verwendung des Moduls Bachelor Elektrotechnik und Informationstechnik (PO 20 + PO 13) IT-Sicherheit / Informationstechnik (PO 13 + PO20 + PO22)					
Vorkenntnisse <p>Vorlesung Mathematik 1</p>					
Lernziele (learning outcomes) Die Studierenden beherrschen die wesentlichen Grundlagen der Systemtheorie. Sie kennen die mathematische Beschreibung von Signalen und Systemen im Zeitbereich und deren wesentliche Merkmale. Sie kennen die Grundlagen der Wahrscheinlichkeitsrechnung und können mit diskreten und kontinuierlichen Zufallsvariablen rechnen. Sie verstehen die Grundbegriffe der Informationstheorie und können diese anwenden.					
Inhalt 1. Signale und Systeme Signale, Kenngrößen und Eigenschaften von Signalen, Elementare Operationen, Signalsynthese und Signalanalyse, periodischer Signale, Analog-Digital und Digital-Analog Umsetzung, lineare und nichtlineare Systeme 2. Einführung in die Wahrscheinlichkeitsrechnung Einführung und Definitionen, Mehrstufige Zufallsexperimente, Diskrete Zufallsvariablen, Kontinuierliche Zufallsvariablen 3. Grundbegriffe der Informationstheorie Grundlegende Fragestellungen der Informationstheorie, Entropiebegriffe, Anwendungen					
Lehrformen Vorlesung und Übungen					
Prüfungsformen Klausurarbeit (120 Minuten)					

Voraussetzungen für die Vergabe von Credits

Erfolgreiches Bestehen der Modulklausur.

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

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

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

Titel des Moduls: Netzsicherheit 2
Network Security 2

Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester Siehe Prüfungsordnung	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Netzsicherheit 2 (211013)			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße 150 Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen		

Modulbeauftragte/r und hauptamtlich Lehrende

Modulbeauftragte/r: Prof. Dr. Jörg Schwenk
 Lehrende: Prof. Dr. Jörg Schwenk

Verwendung des Moduls

B.Sc. IT-Sicherheit/ Informationstechnik
 M.Sc. IT-Sicherheit/ Netze und Systeme
 M.Sc. Angewandte Informatik

Vorkenntnisse

Grundkenntnisse in TCP/IP, Grundkenntnisse der Sicherheitstechnik, Kenntnisse der Grundlagen von Kommunikationssystemen auf dem Netzwerkebene (z.B. Netzwerke, Netzwerkelemente, Netzwerkelemente, Netzwerkelemente)

Lernziele (learning outcomes)

Studierende verfügen nach erfolgreichem Abschluss des Moduls über ein umfassendes Verständnis der technischen Aspekte von Netzsicherheit. Sie haben erkannt, dass Kryptographie alleine nicht ausreicht, um sicherheitstechnische Probleme zu lösen. Sie haben ein umfassendes Systemverständnis für komplexe IT-Systeme erworben. Durch eigenständige Überlegungen zur Verbesserung der Netzsicherheit bereiten sich die Studierenden auf ihre Rolle im Berufsleben vor. Sie können neue Probleme analysieren und neue Lösungsmöglichkeiten entwickeln. Sie können im Gespräch den Nutzen der von ihnen erarbeiteten Lösungen argumentativ begründen. Sie haben verstanden, dass nicht-technische Faktoren wie Fragen der Haftung und der entstehenden Kosten Entscheidungen zur IT-Sicherheit maßgeblich mit beeinflussen.

Inhalt

Wenn Kryptographie in einer technischen Umgebung wie einem Computer-, Daten- oder Telefonnetz eingesetzt wird, hängt die Sicherheit außer von rein kryptographischen Faktoren auch von der technischen Einbettung der Verschlüsselungs- und Signaturalgorithmen ab. Prominente Beispiele (für fehlerhafte Einbettungen) sind EFAIL (efail.de), Angriffe auf die WLAN-Verschlüsselungssysteme WEP und WPA (KRACK) und diverse Angriffe auf TLS (Bleichenbacher, POODLE, DROWN, ROBOT). Das Modul „Netzsicherheit“ beschäftigt sich mit konkreten Netzen zur Datenübertragung und beleuchtet diese von allen Seiten auf ihre Sicherheit hin. Es umfasst folgende Teile:

- Sicherheit von HTTP (HTTP Authentication, Secure HTTP, Architektur von SSL/TLS)
- Transport Layer Security (TLS1.2, Versionen SSL 2.0 bis TLS 1.3)
- Angriffe auf SSL und TLS (BEAST, CRIME, POODLE, Lucky13, Bleichenbacher, DROWN, Heartbleed, Invalid Curve)
- Secure Shell - SSH
- das Domain Name System und DNSSEC (faktorisierte Schlüssel)
- Sicherheit von Webanwendungen (HTML, URI, XSS, CSRF, SQLi, SSO)
- XML- und JSON-Sicherheit

Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die

Studierenden stellen selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit an.

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 180 ECTS)

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

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

5/96 : M.Sc. IT-Sicherheit/ Netze und Systeme [PO20]

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

5/105: M.Sc. Angewandte Informatik

Titel des Moduls: Betriebssysteme
Operating Systems

Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester 4	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Betriebssysteme (211005)			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße 350 Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen keine		

Modulbeauftragte/r und hauptamtlich Lehrende

Modulbeauftragte/r: Prof. Dr.-Ing. Timo Hönic
 Lehrende: Prof. Dr.-Ing. Timo Hönic

Verwendung des Moduls

B.Sc. Informatik
 B.Sc. Angewandte Informatik
 B.Sc. IT-Sicherheit/Informationstechnik

Vorkenntnisse

<p>Grundkenntnisse der Informatik (Inhalte der Module Informatik 1 – Programmierung und Technische Informatik 1 – Rechnerarchitektur)</p>

Lernziele (learning outcomes)

Nach dem erfolgreichen Absolvieren des Moduls

- erlangen die Studierenden ein solides Grundverständnis von modernen Betriebssystemen, ihrer Funktion und ihrer Implementierung
- sind die Studierenden in der Lage, verschiedene Aspekte eines Betriebssystems wie Prozess- und Speichermanagement zu verstehen und zu nutzen, sie können dabei verschiedene Designentscheidungen eigenständig analysieren und bewerten
- sind die Studierenden in der Lage, bestimmte Aspekte eines Betriebssystems selbst zu designen und diese argumentativ zu verteidigen

Inhalt

In diesem Modul werden die wichtigsten Grundlagen zu Betriebssystemen vorgestellt. Dazu gehören zum Beispiel:

- Betriebssystemkonzepte
- Prozesse und Threads, Interprozesskommunikation
- Scheduling-Mechanismen
- Speicherverwaltung, Speicherabstraktionen, Paging
- Dateisysteme
- Eingabe- und Ausgabeverwaltung
- Algorithmen zur Vermeidung von Deadlocks
- Grundlagen der Sicherheit von Betriebssystemen

In den letzten Wochen der Veranstaltung, abhängig vom verfügbaren Zeitfenster, werden spezielle Themen wie beispielsweise Multimedia-Betriebssysteme, Multiprozessorsysteme und Entwurf von Betriebssystemen, behandelt.

Um den Bezug zu modernen Betriebssystemen (aktuellen Versionen von Linux, Windows und macOS) herzustellen, werden die Themen an praktischen Beispielen illustriert. Dies ermöglicht es den Studierenden, die in der Vorlesung besprochenen Themen praktisch nachzuvollziehen.

Lehrformen

Die Vorlesung wird als seminaristischer Unterricht mit Medienunterstützung abgehalten. eLearning unterstützte Hausaufgaben mit praxisnahen, am Rechner zu implementierenden Übungen werden alle zwei Wochen vergeben und in der Übungsstunde besprochen.

Prüfungsformen

Schriftliche Modulabschlussprüfung (90 Minuten)

Voraussetzungen für die Vergabe von Credits

Bestandene schriftliche Modulabschlussprüfung

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

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

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

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

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

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

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

Titel des Moduls: Systemsicherheit System Security					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Systemsicherheit (211011)			Kontaktzeit 60 h	Selbststudium 90 h	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 B.Sc. IT-Sicherheit/ Informationstechnik B.Sc. Informatik M.Sc. Angewandte Informatik M.Sc. IT-Sicherheit/ Netze und Systeme					
Vorkenntnisse Background in Cryptographic primitives (encryption methods, signatures, MACs, hash functions), principles of communication networks, is recommended.					
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 popular systems and protocols, and • analyze / reason about basic protection mechanisms for modern OSs, software, and hardware systems. Students will also develop the ability to reason about the security of a given protocol and independently develop appropriate security defenses and security models. 					
Inhalt While clearly beneficial, the large-scale deployment of online services has resulted in the increase of security threats against existing services. As the size of the global network grows, the incentives of attackers to abuse the operation of online applications also increase and their advantage in mounting successful attacks becomes considerable. These cyber-attacks often target the resources, availability, and operation of online services. With an increasing number of services relying on online resources, integrating proper security measures therefore becomes integral to ensure the correct functioning of every online service. In this course, we discuss important theoretical and analytical aspects in system security. The focus of the course is to understand basic attack strategies on modern systems and platforms, with a focus on side-channel attacks, software-based attacks, malware analysis, as well as software-based defenses (e.g., address space randomization and non-executable memory) and hardware-based defenses (e.g., using TPMs and TEEs). Other topics of the course include analyzing the security of modern cryptocurrencies and ML platforms, and similar aspects in system security. An integral part of this course are exercises and homeworks, which aim to deepen the understanding of the material with practical examples.					
Lehrformen					

Prüfungsformen**Voraussetzungen für die Vergabe von Credits****Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)**

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

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

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

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

5/105: M.Sc. Angewandte Informatik

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: Kryptographie Cryptography					
Modul-Nr./Code	Credits 8 CP	Workload 240 h	Semester siehe Prüfungsordnung / see examination regulations	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Kryptographie (212017)			Kontaktzeit 6 SWS (90 h)	Selbststudium 150 h	Gruppengröße 100 Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Jun.-Prof. Nils Fleischhacker Lehrende: Jun.-Prof. Nils Fleischhacker					
Verwendung des Moduls B.Sc. IT-Sicherheit/ Informationstechnik M.Sc. IT-Sicherheit/ Netze und Systeme M.Sc. Computer Science M.Sc. Angewandte Informatik					
Vorkenntnisse Inhalte der Vorlesungen Einführung in die Kryptographie 1 und 2					
Lernziele (learning outcomes) Die Studierenden haben ein Verständnis der wesentlichen mathematischen Methoden und Verfahren, auf denen moderne kryptographische Verfahren beruhen. Die Tiefe der Behandlung der Verfahren geht deutlich über das in den vorhergehenden Veranstaltungen vermittelte Maß hinaus. Die Teilnehmer sind zur Analyse und dem Design aktueller und zukünftiger kryptographischer Methoden befähigt. Zudem weisen sie ein Bewusstsein für Methodik und Mächtigkeit verschiedenster Angriffsszenarien auf.					
Inhalt Es wird eine Einführung in moderne Methoden der symmetrischen und asymmetrischen Kryptographie geboten. Dazu wird ein Angreifermodell definiert und die Sicherheit der vorgestellten Verschlüsselungs-, Hash- und Signaturverfahren unter wohldefinierten Komplexitätsmaßnahmen in diesem Angreifermodell nachgewiesen. Themenubersicht: <ul style="list-style-type: none"> • Sichere Verschlüsselung gegenüber KPA-, CPA- und CCA-Angreifern • Pseudozufallsfunktionen und -permutationen • Message Authentication Codes • Kollisionsresistente Hashfunktionen • Blockchiffren • Konstruktion von Zufallszahlengeneratoren • Diffie-Hellman Schlüsselaustausch • Trapdoor Einwegpermutationen • Public Key Verschlüsselung: RSA, ElGamal, Goldwasser-Micali, Rabin, Paillier • Einwegsignaturen • Signaturen aus kollisionsresistenten Hashfunktionen • Random-Oracle Modell 					

Lehrformen

Vorlesung und 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 180 ECTS)

8/150: B.Sc. IT-Sicherheit/ Informationstechnik [PO 22]

8/149: B.Sc. IT-Sicherheit/ Informationstechnik [PO 20]

8/99: M.Sc. IT-Sicherheit/ Netze und Systeme [PO 22]

8/96: M.Sc. IT-Sicherheit/ Netze und Systeme [PO 20]

8/97: M.Sc. Computer Science

8/105: M.Sc. Angewandte Informatik

Titel des Moduls: Boolesche Funktionen mit Anwendungen in der Kryptographie					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Boolesche Funktionen mit Anwendungen in der Kryptographie (211020)			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Deutsch (bei Bedarf Englisch)			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Nils-Gregor Leander Lehrende: Prof. Dr. Nils-Gregor Leander					
Verwendung des Moduls B.Sc. IT-Sicherheit/ Informationstechnik M.Sc. IT-Sicherheit/ Netze und Systeme					
Vorkenntnisse Grundlegende Kenntnisse über endliche Körper.					
Lernziele (learning outcomes) Die Studierenden lernen die theoretischen Hintergründe von Booleschen Funktionen kennen.					
Inhalt In dieser Vorlesung beschäftigen wir uns mit der Theorie von Booleschen Funktionen. Der Fokus liegt hierbei auf den kryptographisch relevanten Kriterien für Boolesche Funktionen wie Nicht-Linearität und differentielle Uniformität.					
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 180 ECTS) 5/150: B.Sc. IT-Sicherheit/ Informationstechnik [PO 22] 5/149: B.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: Digitale Forensik					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Digitale Forensik (211017)			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Studiendekan IT-Sicherheit Lehrende: Dr. Christofer Fein					
Verwendung des Moduls B.Sc. IT-Sicherheit/ Informationstechnik B.Sc. Informatik M.Sc. IT-Sicherheit/ Netze und Systeme					
Vorkenntnisse <p>Erfahrung in systemnaher Programmierung sowie der Programmiersprache C sind hilfreich für das Verständnis der vermittelten Themen.</p>					
Lernziele (learning outcomes) Die Studierenden beherrschen verschiedene Konzepte, Techniken und Tools aus dem Themengebiet der digitalen Forensik. Sie kennen die relevanten Konzepte und haben ein Überblick zum Forensischen Prozess. Es ist grundlegendes Verständnis von verschiedenen Methoden zur Sammlung, Analyse und Aufbereitung digitaler Spuren in IT-Systemen vorhanden. Die Studierenden können eigenständig neue Probleme analysieren und neue Lösungsmöglichkeiten entwickeln. Sie können mit diesem Verständnis mit ihren Kollegen über Probleme der Computerforensik diskutieren und auftretende Probleme im Gespräch korrekt klassifizieren.					
Inhalt Digitale Forensik befasst sich mit der Sammlung, Analyse und Aufbereitung digitaler Spuren in IT-Systemen. Im Rahmen der Vorlesung werden diese drei Themenbereiche vorgestellt und jeweils erläutert, mit welchen Verfahren und Ansätzen man diese Aufgaben erreichen kann. Ein Schwerpunkt der Vorlesung liegt auf dem Bereich der Analyse von Dateisystemen. Dazu werden verschiedene Arten von Dateisystemen detailliert vorgestellt und diskutiert, wie relevante Daten erfasst, analysiert und aufbereitet werden können. Darüber hinaus werden weitere Themen aus dem Bereich der digitalen Forensik behandelt, z.B. die Analyse von Smartphones und SQLite-Datenbanken. Ein integraler Teil der Veranstaltung sind die Übungen, die den Stoff mit praktischen Beispielen verdeutlichen und vertiefen.					
Lehrformen Vorlesung mit Übung als Blockveranstaltung					
Prüfungsformen Schriftliche Modulabschlussprüfung (120 Minuten)					
Voraussetzungen für die Vergabe von Credits Bestandene schriftliche Modulabschlussprüfung					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS) 5/150: B.Sc. IT-Sicherheit/ Informationstechnik [PO 22]					

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

5/170: B.Sc. Informatik [PO 22]

5/158: B.Sc. Informatik [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: Einführung in die künstliche Intelligenz Introduction to Artificial Intelligence					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Introduction to Artificial Intelligence (211045)			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße 250 Studierende
Unterrichtssprache Englisch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Sen Cheng Lehrende: Prof. Dr. Laurenz Wiskott, Prof. Dr. Tobias Glasmachers, Prof. Dr. Sen Cheng, Prof. Dr. Gregor Schöner, Prof. Dr. Nils Jansen Prof. Dr. Setareh Maghsudi Prof. Dr. Christian Straßer					
Verwendung des Moduls B.Sc. Informatik (Pflichtmodul) B.Sc. Angewandte Informatik (Pflichtmodul) B.Sc. IT-Sicherheit/Informationstechnik (Wahlpflichtmodul)					
Vorkenntnisse					
Lernziele (learning outcomes)					
Inhalt					
Lehrformen					
Prüfungsformen Written module final exam (120 minutes)					
Voraussetzungen für die Vergabe von Credits					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS) 5/158: B.Sc. Informatik [PO 22] 5/170: B.Sc. Informatik [PO 20] 5/168: B.Sc. Angewandte Informatik [PO 22] 5/170: B.Sc. Angewandte Informatik [PO 20]					

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

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

Titel des Moduls: Einführung ins Hardware Reverse Engineering

Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Einführung ins Hardware Reverse Engineering (212025)			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße 30 Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen		

Modulbeauftragte/r und hauptamtlich Lehrende

Modulbeauftragte/r: Prof. Dr.-Ing. Christof Paar
Lehrende: Prof. Dr.-Ing. Christof Paar
Julian Speith
Simon Klix
Nils Albartus

Verwendung des Moduls

B.Sc. IT-Sicherheit/ Informationstechnik

Vorkenntnisse

<p>Inhalte der Vorlesungen “Technische Informatik 1 - Rechnerarchitektur” und “Technische Informatik 2 - Digitaltechnik”.</p>

Lernziele (learning outcomes)

Die Studierenden sind mit den grundlegenden Aspekten des Entwurfs komplexer logischer Schaltkreise vertraut. Dazu gehören unter anderem das Verständnis von ASIC- und FPGA-Architekturen und der entsprechenden Workflows, sowie die Anwendung der dazugehörigen Tools unter der praktischen Verwendung von Hardwarebeschreibungssprachen (HDLs). Weiterhin haben die Studierenden ein tiefgehendes theoretisches Verständnis der verschiedenen Schritte des Hardware Reverse Engineering Prozesses und sind sich der Implikationen bewusst. Des Weiteren erlangen die Studierenden im Rahmen mehrerer praktischer Projekte ein tiefgehendes Verständnis verschiedener Gate-level Netlist Reverse Engineering Methoden und werden ideal auf Abschlussarbeiten in diesem Bereich vorbereitet

Inhalt

Das sogenannte Reverse Engineering von Geräten spielt sowohl für legitime Nutzer als auch für Hacker eine wichtige Rolle. Auf der einen Seite kann Reverse Engineering Unternehmen und Regierungen dabei unterstützen, Verletzungen am geistigen Eigentum oder gezielte Manipulationen aufzuspüren. Auf der anderen Seite setzen Hacker Reverse Engineering ein, um kostengünstig das geistige Eigentum anderer zu stehlen und zu kopieren, oder auch um durch den Einbau von Hintertüren Programme und Hardware-Schaltungen zu manipulieren. Um die ersten Schritte im Hardware Reverse Engineering erfolgreich zu gehen, ist es zunächst einmal wichtig, dass die grundlegenden Konzepte des (Forward) Engineerings integrierter Schaltkreise erlernt werden. Der Inhalt dieser Vorlesung gliedert sich daher im Wesentlichen in die folgenden beiden Teile:

Teil I: Grundprinzipien

des VLSI Entwurfs (VLSI steht für Very-large-scale integration) - Einführung in logische (kombinatorische) Schaltkreise - Sequentielle Schaltkreise - Hardware Description Languages (HDLs) - Einführung in ASIC- und FPGA-Architekturen - ASIC- und FPGA-Workflows

Teil II: Hardware Reverse Engineering - PCB Analyse, Delaying, und Bildverarbeitung - FPGA Bitstream Reverse Engineering - Reverse Engineering von Gate-Level-Netzlisten

Lehrformen

Vorlesung mit Übung

Prüfungsformen

Projektarbeit und Abschlussvortrag

Voraussetzungen für die Vergabe von Credits

Bestandene Modulabschlussprüfung und erfolgreiche Teilnahme an den praktischen Übungen am Rechner.

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

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

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

Titel des Moduls: Highlights of Theoretical Computer Science [B.Sc.]
Highlights of Theoretical Computer Science [B.Sc.]

Modul-Nr./Code	Credits 10 CP	Workload 300 h	Semester siehe Prüfungsordnung	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Highlights of Theoretical Computer Science (211057)			Kontaktzeit 90 h	Selbststudium 210	Gruppengröße 40 Studierende
Unterrichtssprache Englisch			Teilnahmevoraussetzungen Successful completion of an introductory course on theoretical computer science (covering formal languages, basics of complexity theory including NP-completeness and reductions, basics of computability theory). Interest and motivation to learn about theoretical concepts.		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Michael Walter Prof. Dr. Thomas Zeume Lehrende: Prof. Dr. Michael Walter Prof. Dr. Thomas Zeume Dr. Vladimir Lysikov					
Verwendung des Moduls B.Sc. Informatik B.Sc. Angewandte Informatik B.Sc. IT-Sicherheit / Informationstechnik					
Vorkenntnisse					
Lernziele (learning outcomes) You will know some of the most important results and insights of modern theoretical computer science. You will learn approaches and techniques that go well beyond a first course. You will be able to recognize when these can be used and how to adapt them to new situations. You will be able to independently acquire new knowledge in this area.					
Inhalt The insights and techniques of modern theoretical computer science have been key for advances in all areas of computer science. In this course, we will discuss some highlights and the techniques that underpin them. Possible topics that we might cover: <ul style="list-style-type: none"> • Computational models (is there life beyond Turing machines?) • Kolmogorov complexity (what is the shortest program that produces some output?) • Communication complexity (how many bits must Alice and Bob exchange to jointly solve a problem?) • Fine-grained complexity (are some easy problems easier than others? and why?) • Fast multiplication of numbers and matrices (can you beat the high-school method?) • Randomness (does it really help to compute faster?) • Circuit lower bounds (why is it so hard to prove that problems are hard?) • Convex optimization (how to maximize profit if all you can ask are yes/no questions) • Hardness of approximation (how easy is it to find near-optimal solutions?) • Cryptography and computation 					

If you enjoyed your first course in theoretical computer science in the Bachelor's and would like to deepen your knowledge by getting an overview of the fascinating theory of computing, then this course will be exactly right for you.

Lehrformen

Vorlesung mit Übung

Prüfungsformen

Final module examination. Format will depend on number of participants.

Voraussetzungen für die Vergabe von Credits

Bestandene Modulabschlussprüfung

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

10/158: B.Sc. Informatik [PO 22]

10/170: B.Sc. Informatik [PO 20]

10/168: B.Sc. Angewandte Informatik [PO 22]

10/170: B.Sc. Angewandte Informatik [PO 20]

10/150: B.Sc. IT-Sicherheit / Informationstechnik [PO 22]

10/149: B.Sc. IT-Sicherheit / Informationstechnik [PO 20]

Titel des Moduls: Implementierung kryptographischer Verfahren					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Implementierung kryptographischer Verfahren (212020)			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen keine		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr.-Ing. Tim Güneysu Lehrende: Dr.-Ing. Pascal Sasdrich					
Verwendung des Moduls B.Sc. IT-Sicherheit/ Informationstechnik M.Sc. IT-Sicherheit/ Netze und Systeme					
Vorkenntnisse Grundkenntnisse der Programmiersprache C bzw. C++, Vorlesung “Einführung in die Kryptographie I”;					
Lernziele (learning outcomes) Studierende erlernen die grundlegenden Algorithmen für die effiziente Implementierung rechenintensiver Kryptoverfahren. Insbesondere den Umgang von Algorithmen mit sehr langen Operanden haben sie nach Abschluss des Moduls verstanden, ebenso wie das Zusammenspiel von Implementierungsmethoden und kryptographischer Sicherheit.					
Inhalt Diese Vorlesung gibt eine Einführung in Verfahren zur schnellen und sicheren Implementierung kryptographischer Algorithmen. Im ersten Teil werden Methoden zum effizienten Potenzieren ausführlich behandelt, da diese für alle verbreiteten asymmetrischen Verfahren von großer Bedeutung sind. Für den weit verbreiteten RSA Algorithmus werden zudem spezielle Beschleunigungsverfahren vorgestellt. Im zweiten Teil werden Algorithmen für effiziente Langzahlarithmetik entwickelt. Zunächst werden grundlegende Methoden zur Darstellung von Langzahlen in Rechnern und Verfahren zur Addition vorgestellt. Der Schwerpunkt dieses Teils liegt auf Algorithmen zur effizienten modularen Multiplikation. Neben dem Karatsuba-Algorithmus wird die Montgomery-Multiplikation behandelt. Im dritten Teil werden sichere Implementierungen besprochen. Es erfolgt eine Einführung in aktive und passive Seitenkanalattacken. Es werden aktive Attacken gegen Blockchiffren und RSA vorgestellt. Als wichtige Vertreter der passiven Attacken werden die Grundlagen von SPA (simple power analysis) und DPA (differential power analysis) eingeführt.					
Lehrformen Vorlesung mit Übungen					
Prüfungsformen Die Endnote ergibt sich zu 70% aus einer Klausur (120 Minuten) und zu 30% aus studienbegleitenden Programmierprojekten (auch zum Nachschreibetermin)					
Voraussetzungen für die Vergabe von Credits Bestandene Modulabschlussprüfung					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS) 5/150: B.Sc. IT-Sicherheit/ Informationstechnik [PO 22] 5/149: B.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: Introduction to Blockchain Security Introduction to Blockchain Security					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße Studierende
Unterrichtssprache Englisch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Ghassan Karame Lehrende: Prof. Dr. Ghassan Karame					
Verwendung des Moduls B.Sc. IT-Sicherheit					
Vorkenntnisse <p>Hintergrundwissen in Systemsicherheit, Netzwerksicherheit, kryptographischen Primitiven (Verschlüsselungsmethoden, Signaturen, MACs, Hashfunktionen), Prinzipien von Kommunikationsnetzwerken, wird vorausgesetzt.</p>					
Lernziele (learning outcomes) Nach Abschluss dieses Kurses sollen die Teilnehmer in der Lage sein: <ul style="list-style-type: none"> • über die Sicherheits- und Datenschutzdefinitionen von offenen Zahlungssystemen nachzudenken. • die Sicherheit von PoW-Blockchains vor dem Hintergrund des aktuellen Stands der Technik und der gemeldeten Angriffe zu erklären. • die möglichen Netzwerksicherheits- und kryptografischen Gegenmaßnahmen zur Abwehr von Angriffen auf Blockchains erläutern zu können. • die besten Sicherheits-/Privatsphärenpraktiken, um die Sicherheit bestehender Blockchains zu verbessern, erläutern und relevante Lehren für die Entwicklung von Blockchain-Technologien der nächsten Generation ziehen zu können. 					
Inhalt Das Hauptziel des Kurses ist es, einen umfassenden Überblick über die Sicherheit und den Datenschutz von Blockchain-Technologien zu geben. Die Kursteilnehmer werden auch in die grundlegenden Sicherheits- und Datenschutzbestimmungen bestehender populärer Währungen eingeführt und mit den neuesten Angriffen und Bedrohungen vertraut gemacht, die gegen bestehende Systeme/Einführungen gemeldet wurden. Die Teilnehmer werden auch über die Wirksamkeit der Kombination von Sicherheitsprimitiven auf Netzwerkebene mit neuartigen kryptographischen Primitiven zur Abwehr von Angriffen auf Zahlungssysteme nachdenken.					
Lehrformen Vorlesung mit Übung					
Prüfungsformen Schriftliche Modulabschlussprüfung (120 min)					
Voraussetzungen für die Vergabe von Credits Bestandene schriftliche Modulabschlussprüfung					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS) 5/150: B.Sc. IT-Sicherheit [PO 22]					

Titel des Moduls: Kryptographie auf hardwarebasierten Plattformen
Cryptography on hardware-based platforms

Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung / see examination regulations	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Kryptographie auf hardwarebasierten Plattformen (212019)			Kontaktzeit 4 SWS (60 h)	Selbststudium 90 h	Gruppengröße 50 Studierende
Unterrichtssprache Deutsch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr.-Ing. Tim Güneysu Lehrende: Prof. Dr.-Ing. Tim Güneysu					
Verwendung des Moduls B.Sc. IT-Sicherheit/ Informationstechnik B.Sc. Angewandte Informatik [nur bis einschließlich WS 22/23] M.Sc. IT-Sicherheit/ Netze und Systeme [nur bis einschließlich WS 22/23] M.Sc. Computer Science					
Vorkenntnisse					
Lernziele (learning outcomes) Die Studierenden kennen die Konzepte der praxisnahen Hardwareentwicklung mit abstrakten Hardwarebeschreibungssprachen (VHDL) und die Simulation von Hardwareschaltungen auf FPGAs. Sie beherrschen Standardtechniken der hardwarenahen Prozessorentwicklung und sind zur Implementierung von symmetrischen und asymmetrischen Kryptosystemen auf modernen FPGA-Systemen in der Lage.					
Inhalt Kryptographische Systeme stellen aufgrund ihrer Komplexität ins- besondere an kleine Prozessoren und eingebettete Systeme hohe Anforderungen. In Kombination mit dem Anspruch von hohem Datendurchsatz bei geringsten Hardwarekosten ergeben sich hier für den Entwickler grundlegende Probleme, die in dieser Vorlesung beleuchtet werden sollen. Die Vorlesung behandelt die interessantesten Aspekte, wie man aktuelle kryptographische Verfahren auf praxisnahen Hardwaresystemen implementiert. Dabei werden Kryptosysteme wie die Blockchiffre AES, die Hashfunktionen SHA-1 sowie asymmetrische Systeme RSA und ECC behandelt. Weiterhin werden auch spezielle Hardwareanforderungen wie beispielsweise der Erzeugung echten Zufalls (TRNG) sowie der Einsatz von Physically Unclo- nable Functions (PUF) besprochen. Die effiziente Implementierung dieser Kryptosysteme, insbesondere in Bezug auf die Optimierung für Hochgeschwindigkeit, wird auf modernen FPGAs besprochen und in praktischen Übungen mit Hilfe der Hardwarebeschreibungssprache VHDL umgesetzt. 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 Bestandene schriftliche Modulabschlussprüfung; Durch die erfolgreiche Teilnahme am Übungsbetrieb können bis zu 10 Prozent Bonuspunkte erworben werden, die auf das Ergebnis der Modulklausur angerechnet werden					

können.

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

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

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

5/97: M.Sc. Computer Science

Titel des Moduls: Programmanalyse [B.Sc]					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Programmanalyse (211015)			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 B.Sc. IT-Sicherheit/ Informationstechnik B.Sc. Informatik					
Vorkenntnisse keine					
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 mündliche oder schriftliche Modulabschlussprüfung (wird zu Beginn des Semester bekanntgegeben), Anmeldung: FlexNow					
Voraussetzungen für die Vergabe von Credits Bestandene Modulabschlussprüfung					

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

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

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

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

5/170: B.Sc. Informatik [PO 22]

Titel des Moduls: Public Key Kryptanalyse 1 [B.Sc]
Public Key Cryptanalysis 1 [B.Sc]

Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung	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					
Vorkenntnisse Vorausgesetzt werden elementare Kenntnisse der Lineare Algebra (Mathematik 1 & Informatiker) und ein Interesse an algorithmischen Techniken und Kryptographie, in Theorie und Praxis (umgesetzt mit Hilfe des Computeralgebra-Systems Sage).					
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 <ul style="list-style-type: none"> • 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 kodierungsbasierter 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 180 ECTS)

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

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

Titel des Moduls: Quantum Information and Computation
Quantum Information and Computation

Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung / see examination regulations	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Quantum Information and Computation (212011)			Kontaktzeit 4 SWS (60 h)	Selbststudium 90 h	Gruppengröße 40 Studierende
Unterrichtssprache Deutsch oder Englisch (depends on audience)			Teilnahmevoraussetzungen Keine		

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 (auf Antrag)
 M.Sc. IT-Sicherheit/ Netze und Systeme (auf Antrag)
 M.Sc. Computer Science

Vorkenntnisse

<p>Familiarity with linear algebra (in finite dimensions) and
probability (with finitely many outcomes) at the level of a first Bachelors course; we will briefly remind you of the more difficult bits in class. In addition, some mathematical maturity, since we will discuss precise mathematical statements and rigorous proofs. No background in physics is required.</p>

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:

- 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

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.

Lehrformen

Lecture with Exercise

Prüfungsformen

Final written module exam (180 minutes)

Voraussetzungen für die Vergabe von Credits

Passed written exam

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 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]

5/97: M.Sc. Computer Science

Titel des Moduls: Red- and Blue-Teaming (kein Angebot im SoSe 24)
Red- and Blue-Teaming (no offer in Summer 24)

Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung	Turnus Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Red- and Blue Teaming (212024)			Kontaktzeit 60 h	Selbststudium 90 h	Gruppengröße 30 Studierende
Unterrichtssprache Deutsch (Material auf Englisch)			Teilnahmevoraussetzungen		

Modulbeauftragte/r und hauptamtlich Lehrende

Modulbeauftragte/r: Prof. Dr. Jörg Schwenk
 Lehrende: Dr.-Ing. Martin Grothe

Verwendung des Moduls

B.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

Vorkenntnisse

<p>Zielgruppe:</p>

<p>Das Ni­veau rich­tet sich vor­ran­gig an Ba­che­lor Stu­den­ten mit kei­ner oder ge­rin­ger Er­fah­rung im of­fen­si­ven bzw. de­fen­si­ven Se­cu­ri­ty Tes­ting. Gleich­zei­tig sind er­fah­re­ne CTF Spie­ler herz­lich will­kom­men und ich freue mich über einen regen Aus­tausch in der Ver­an­stal­tung.</p>

Gute Kenntnisse der internen Funktionsweise von Linux und Windows Betriebssystem (s. u.

Buchempfehlungen)

Der Umgang mit Bash und Powershell sollte für jeden Teilnehmer selbstverständlich sein

Absolvieren des Wargames "Bandit" von Overthewire.org

Gute Englischkenntnisse

Da der Kurs sehr ins Detail geht werden folgende Buchempfehlungen zu den Internas der Betriebssysteme ausgesprochen: How Linux works (3rd Edition, ISBN-13: 9781718500402), Windows Internals Part 1 (ISBN-13: 978-0735684188)

Lernziele (learning outcomes)

In diesem Modul werden die Studierenden lernen, was die Aufgaben, Ziele und Pflichten eines Red Teams und eines Blue Teams sind. Dazu wird zu Beginn der Veranstaltung erklärt, wann welche Art von Sicherheitsüberprüfung in einem Unternehmen oder Organisation sinnvoll ist und welche Ziele damit überhaupt erreicht werden können. Dadurch sollen die Studierenden neben den technischen Kenntnissen und praktischen Fertigkeiten auch Projektorganisation, Budget Planung und das Verfassen von Berichten über Ihre Arbeit erlernen.

Inhalt

Die bisher geplanten Inhalte sind wie folgt aufgeschlüsselt:

Theorie:

- Einführung in das Thema Sicherheitsüberprüfungen (Kategorien, Nutzen/Ziele, Planung und Ablauf)
- Red Teaming: Ursprünge und Geschichte des Red Teamings; Wichtige Standards, Best Practices und Organisationen; Arten, Aufgaben und Ziele eines Red Team Einsatzes; Planung, Ablauf und Nachbereitung eines Red Teaming Einsatzes
- Blue Teaming: Einführung ins Blue Teaming; Wichtige Standards, Best Practices und Organisationen;

- Arten, Aufgaben und Ziele eines Blue Teams; Planung und Aufbau eines Blue Teams in der Organisation
- Angriffe: Windows Clients und Server Systeme (inkl. Active Directory Domainen); Linux Server und Clients; Simulation von APTs auf Basis von Threat Modelling und dem MITRE ATT&CK Framework

Praxis:

- Die Bausteine aus der Theorie werden in Übungen und Hausaufgaben erklärt, vertieft und praktisch umgesetzt.
- Dabei sollen die Aufgaben das Verständnis der Theorie erleichtern und das eigentliche praktische Umsetzen ermöglichen.
- Umgang mit gängigen Penetration Testing Tools die in Kali Linux enthalten sind: Metasploit, PSEmpire, Mimikatz, nmap, SET, Bloodhound, etc.
- Umgang mit gängigen Tools aus dem Blue Teaming: nmap, Zeek, Snort, ELK/HELK, AIDE, auditD, rkhunter, usw.

Lehrformen

Blockkurs in der vorlesungsfreien Zeit

Prüfungsformen

Schriftliche Modulabschlussprüfung (120 Minuten)

Voraussetzungen für die Vergabe von Credits

Bestandene schriftliche Modulabschlussprüfung

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

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

5/149: B.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: Vertiefungspraktikum IT-Sicherheit

Modul-Nr./Code	Credits 4 CP	Workload 120 h	Semester 5	Turnus Wintersemester und Sommersemester	Dauer 1 Semester
Lehrveranstaltungen Die aktuellen Praktika sind hervorgehoben: <ul style="list-style-type: none"> • Praktische Kryptanalyse von symmetrischen Chiffren (211401) • Projekt Netz- und Datensicherheit (212412) • Forschungspraktikum Human-Centred Security (212408) • Initial Research in Information Security (212402) • Praktikum TLS Implementierung (212414) • Praktikum zur Hackertechnik (Hackerpraktikum) (212413) • Bachelor-Praktikum ARM Processors for Embedded Cryptography (212406) • Developer Centered Security (212417) • Praktikum Implementing Post-Quantum Standards and Challenges (212416) • Praktikum Wireless Physical Layer Security (142025) • Practical Course on Blockchain Security (211428) • Practical IoT Hacking (244429) • Initial Research in Internet Security (211430) • Initial Research in Software Security (211432) • Projekt Eingebettete Sicherheit 			Kontaktzeit je nach Veranstaltungswahl	Selbststudium abhängig von der Praktikumswahl	Gruppengröße Studierende
Unterrichtssprache abhängig von der Praktikumswahl: Deutsch oder Englisch			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Studiendekan der IT-Sicherheit Lehrende: siehe Praktikumsbeschreibung					
Verwendung des Moduls B.Sc. IT-Sicherheit					
Vorkenntnisse abhängig vom gewählten Praktikum					

Lernziele (learning outcomes)

Nach dem erfolgreichen Abschluss des Moduls

- haben Studierende Ihre Fähigkeiten in der Analyse und dem Einsatz von Verfahren zur Sicherung von IT-Systemen vertieft und erweitert
- je nach gewählten Praktikum können noch weitere Lernziele dazu kommen

Inhalt

Es werden im Winter- und/oder Sommersemester Praktika zu folgenden Themen angeboten:

- Praktische Kryptanalyse von symmetrischen Chiffren (211401)
- Projekt Netz- und Datensicherheit (212412)
- Forschungspraktikum Human-Centred Security (212408)
- Initial Research in Information Security (212402)
- Praktikum TLS Implementierung (212414)
- Praktikum zur Hackertechnik (Hackerpraktikum) (212413)
- Research in Software/Internet Security (2124)
- Bachelor-Praktikum ARM Processors for Embedded Cryptography (212406)
- Developer Centered Security (212417)
- Praktikum Implementing Post-Quantum Standards and Challenges (212416)
- Praktikum Wireless Physical Layer Security (142025)
- Practical Course on Blockchain Security (211428)
- Practical IoT Hacking (244429)
- Initial Research in Internet Security (211430)
- Initial Research in Software Security (211432)
- Projekt Research in Security Engineering (211435)

Weiterführende Informationen zu den jeweiligen Praktika finden Sie im Vorlesungsverzeichnis im Modul Vertiefungspraktikum IT-Sicherheit unter "Veranstaltungen".

Lehrformen

Praktikum im Block oder als semesterbegleitende Veranstaltung.

Prüfungsformen

Praktikum

Voraussetzungen für die Vergabe von Credits

Aktive Teilnahme und erfolgreiche Bearbeitung der praktischen Aufgabenstellungen. Ggf. ist die Anfertigung einer schriftlichen Dokumentation erforderlich.

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

unbenotet

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

Modul-Nr./Code	Credits 3 CP	Workload 90 h	Semester	Turnus jedes Semester	Dauer Semester
Lehrveranstaltungen Die aktuellen Seminare sind jeweils hervorgehoben. 211104 Human Centred Security and Privacy 211110 Seminar Real-World Kryptanalyse 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 () 211133 Seminar on Current Topics for Systems Security and Privacy 212109 Information Security Seminar Bachelor 212111 Seminar Ressourceneffiziente Systemssoftware 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) 211134 Seminar: Current topics in microarchitectural security 211139 Seminar Randomisierte Algorithmen			Kontaktzeit 30 h	Selbststudium	Gruppengröße Studierende
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					

Vorkenntnisse

Die Vertiefungsseminare beziehen sich in der Regel auf Inhalte aus bestimmten Pflicht- oder Vertiefungsmodulen, die im Vorfeld absolviert worden sein sollten.

Lernziele (learning outcomes)

Nach dem erfolgreichen Abschluss des Moduls

- 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 Bachelorseminare 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 180 ECTS)**

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

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

Titel des Moduls: Web- und Browsersicherheit					
Modul-Nr./Code	Credits 5 CP	Workload 150 h	Semester siehe Prüfungsordnung	Turnus Wintersemester	Dauer 1 Semester
Lehrveranstaltungen Web- und Browsersicherheit (212061)			Kontaktzeit	Selbststudium 90 h	Gruppengröße 30 Studierende
Unterrichtssprache Vorlesung und Prüfung finden in Englisch statt.			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Prof. Dr. Jörg Schwenk Lehrende: Dr.-Ing. Mario Heiderich					
Verwendung des Moduls B.Sc. IT-Sicherheit/ Informationstechnik M.Sc. IT-Sicherheit/ Netze und Systeme					
Vorkenntnisse Grundkenntnisse in Webprogrammierung Gute Englischkenntnisse 					
Lernziele (learning outcomes) Studierende verfügen nach erfolgreichem Abschluss des Moduls über ein umfassendes Verständnis der technischen Aspekte von Web- und Browsersicherheit. Sie haben ein umfassendes Systemverständnis für komplexe Webanwendungen erworben. Durch eigenständige Überlegungen und deren Umsetzung in praktischen Projekten zur Verbesserung der Netzsicherheit bereiten sich die Studierenden auf ihre Rolle im Berufsleben vor. Sie können neue Probleme analysieren und neue Lösungsmöglichkeiten entwickeln. Sie können im Gespräch den Nutzen der von ihnen erarbeiteten Lösungen argumentativ begründen.					
Inhalt Die Vorlesung wird als Blockveranstaltung angeboten. Die Veranstaltung ist auch für Studierende geeignet, die bereits XML- und Webservicesicherheit/Websicherheit gehört haben und ihr Wissen vertiefen möchten. Dies ist jedoch keine Voraussetzung. What to bring: <ul style="list-style-type: none">• A Laptop, OS doesn't matter• Working Internet Connection Kapitel 1: History & Basics <ul style="list-style-type: none">• The History of Web Security and Web Attacks• The History of Browsers• HTML, JavaScript, CSS Kapitel 2: HTTP, Server, SQLi <ul style="list-style-type: none">• Attacks using HTTP and SSL/TLS• SQL Injections					

- Uploads
- SSRF, XXE & XEE

Kapitel 3: Cookies, Sessions, XSS

- Cookies & Sessions
- Same Origin Policy
- Authentication & Authorization
- The Basics of Cross-Site Scripting

Kapitel 4: Advanced XSS

- Advanced XSS
- mXSS and DOM Mutations

Kapitel 5: Browsers & Beyond

- The DOM
- DOM Clobbering & DOM XSS
- jQuery, Expression Injections, AngularJS
- postMessage XSS
- SVG
- Flash Security

Kapitel 6: Sandboxing & Random Bits

- JavaScript Sandboxing
- The Human Factor
- Stories from the Real World

Lehrformen

Blockveranstaltung in der vorlesungsfreien Zeit

Prüfungsformen

Schriftliche Modulabschlussprüfung (120 Minuten)

Voraussetzungen für die Vergabe von Credits

Bestandene schriftliche Modulabschlussprüfung

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

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

5/149: B.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 Wahlmodule					
Modul-Nr./Code	Credits 8 CP	Workload 240 h	Semester	Turnus Jedes Semester	Dauer 1 Semester
Lehrveranstaltungen			Kontaktzeit abhängig von der Veranstaltungswahl	Selbststudium Je nach Veranstaltungswahl	Gruppengröße Studierende
Unterrichtssprache Je nach Veranstaltungswahl			Teilnahmevoraussetzungen		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Studienfachberatung IT-Sicherheit Lehrende:					
Verwendung des Moduls B.Sc. IT-Sicherheit					
Vorkenntnisse abhängig von Veranstaltungswahl					
Lernziele (learning outcomes) Die Studierenden beherrschen entsprechend ihrer Wahl verschiedene, das Studium ergänzende Schlüsselqualifikationen und haben ihr Fachwissen vertieft.					
Inhalt Durch die freie Wahl von Lehrveranstaltungen aus dem gesamten Angebot der RUB, UARuhr und UNIC können die Studierenden fachliche und überfachliche Schwerpunkte anhand ihrer eigenen Interessen setzen. Je nach Veranstaltungswahl werden unterschiedliche Inhalte vermittelt.					
Lehrformen abhängig von Veranstaltungswahl					
Prüfungsformen abhängig von Veranstaltungswahl					
Voraussetzungen für die Vergabe von Credits abhängig von Veranstaltungswahl					
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS) unbenotet					

Titel des Moduls: Industriepraktikum IT-Sicherheit					
Modul-Nr./Code	Credits 15 CP	Workload 450h	Semester 6	Turnus Wintersemester und Sommersemester	Dauer Semester
Lehrveranstaltungen			Kontaktzeit	Selbststudium	Gruppengröße Studierende
Unterrichtssprache			Teilnahmevoraussetzungen siehe Prüfungsordnung		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Studiendekan IT-Sicherheit Lehrende:					
Verwendung des Moduls B.Sc. IT-Sicherheit					
Vorkenntnisse					
Lernziele (learning outcomes) Mit dem Industriepraktikum gewinnen die Studierenden Einblicke in die spätere Berufstätigkeit, in die betrieblichen Arbeitsweisen und Sozialstrukturen. Sie lernen u.a. Prüf-, Entwurfs- und Entwicklungsmethoden sowie Verfahrens- und Betriebsaufgaben im Bereich der IT-Sicherheit kennen. Kommunikative und soziale Schlüsselqualifikationen sind aus dem Umgang mit Vorgesetzten und Teammitgliedern bekannt.					
Inhalt Das Industriepraktikum soll vorrangig in Industriebetrieben, Dienstleistungsunternehmen und technischen Behörden abgeleistet werden, in denen Tätigkeiten im Bereich IT-Sicherheit durchgeführt werden. Die Betriebs- oder Gruppengröße spielt keine Rolle. Es muss eine verantwortliche Betreuerin bzw. ein verantwortlicher Betreuer das Praktikum begleiten. Eine Praktikantentätigkeit im eigenen Betrieb sowie im Betrieb von Verwandten oder der/des Lebenspartnerin/-s ist nicht zulässig. Der Gesamtumfang des Praktikums muss mindestens 450 Stunden betragen. Es dauert in der Regel drei Monate und kann in Teilzeit oder Vollzeit absolviert werden. Dies ist abhängig von der vereinbarten wöchentlichen Arbeitszeit. Eventuelle Fehltage z. B. durch Krankheit oder Betriebsurlaub sind genauso nachzuholen wie Fehltage durch gesetzliche Feiertage, sofern die geforderte Gesamtstundenzahl ansonsten nicht erreicht wird. Das Praktikum ist in der Regel in einem Betrieb und ohne Unterbrechung im sechsten Fachsemester durchzuführen. Eine Aufteilung auf mehrere Zeiträume bzw. verschiedene Betriebe ist jedoch prinzipiell zulässig. Die Durchführung des Praktikums im vollen Umfang und das Erstellen einer Dokumentation über die im Praktikum durchgeführten Tätigkeiten sind Bestandteil der Bachelorprüfung. Es handelt sich um ein Pflichtpraktikum.					
Bestandteile (1) eigenständige Suche nach einem Praktikumsplatz mit Tätigkeiten im Bereich IT-Sicherheit (2) Anmeldung vor Praktikumsbeginn über das Prüfungsamt Informatik (3) Durchführung des Praktikums mit Dokumentation der Tätigkeiten (4) Abgabe eines Berichts (Dokumentation der Tätigkeiten)					
Sonstiges					

Grundsätzlich sind auch andere Tätigkeiten anerkennungsfähig, wenn der Zweck des Praktikums erfüllt ist.

Eine abgeschlossene Ausbildung oder eine Berufstätigkeit (auch nebenberuflich, wie z.B. eine Werkstudententätigkeit) in einem der IT-Sicherheit affinen Bereich kann auf Antrag angerechnet werden.

Lehrformen

Prüfungsformen

Abgabe eines Berichtes

Voraussetzungen für die Vergabe von Credits

Durchführung des Praktikums und Abgabe eines Berichtes

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

unbenotet

Titel des Moduls: Abschlussarbeit (B.Sc. IT-Sicherheit)					
Modul-Nr./Code	Credits 15 CP	Workload 450h	Semester 6	Turnus Wintersemester und Sommersemester	Dauer 1 Semester
Lehrveranstaltungen a) Bachelor-Thesis (12 CP) b) Colloquium (3 CP)			Kontaktzeit	Selbststudium	Gruppengröße Studierende
Unterrichtssprache			Teilnahmevoraussetzungen Erfolgreich abgeschlossene Module im Umfang von mindestens 135 LP. In der PO22 zusätzlich: erfolgreiches Bestehen aller Pflichtmodule der ersten vier Semester.		
Modulbeauftragte/r und hauptamtlich Lehrende Modulbeauftragte/r: Studiendekan IT-Sicherheit Lehrende:					
Verwendung des Moduls B.Sc. IT-Sicherheit [PO20] B.Sc. IT-Sicherheit [PO22]					
Vorkenntnisse					
Lernziele (learning outcomes) Die Bachelorarbeit soll zeigen, dass die oder der Studierende in der Lage ist, innerhalb einer vorgegebenen Frist eine anspruchsvolle Fragestellung der Informatik unter Anwendung der im Bachelorstudium erworbenen Methoden selbstständig zu bearbeiten. Darüber hinaus wird der Erwerb von Grundkenntnissen der wissenschaftlichen Arbeit einschließlich der Projektorganisation sowie die Präsentation der erarbeiteten Ergebnisse erwartet. Während der Bachelorarbeit werden die folgenden Kompetenzen erworben bzw. ausgebaut: <ul style="list-style-type: none"> • Vertieftes Wissen im Bereich der bearbeiteten Aufgabenstellung • Wissenschaftliches Arbeiten und Schreiben • Projekt- und Zeitmanagement • Präsentation wissenschaftlicher Ergebnisse • Rhetorik und sprachliche Kompetenz • Fächerübergreifendes Denken und Arbeiten 					
Inhalt a) Bearbeitung und Lösung einer wissenschaftlichen Aufgabe im Bereich der Informatik unter Anleitung. Die im Bachelorstudium erworbenen Kenntnisse, Kompetenzen und Methoden sollen angewendet werden. Die Ergebnisse der Arbeit sind schriftlich zu verfassen. (12CP) b) Im Anschluss an die Bearbeitung der Bachelorarbeit werden die Ergebnisse in Form eines Kolloquium-Vortrags präsentiert. Als Vorbereitung müssen die Studierenden mindestens fünf Kolloquium-Vorträge anderer Studierenden besuchen und kritisch mitdiskutieren. Außerdem werden sie dazu eingeladen und motiviert, Vorträge des wissenschaftlichen Personals und anderer Gastwissenschaftler zu besuchen und an den Diskussionen aktiv teilzunehmen. (3CP)					
Lehrformen Projektarbeit					

Prüfungsformen

Schriftliche Ausarbeitung der gestellte Aufgabe und Präsentation der Ergebnisse im Kolloquium

Voraussetzungen für die Vergabe von Credits

Positive Bewertung der Bachelorarbeit und des Kolloquiums sowie Teilnahme an anderen wissenschaftlichen Vorträgen

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 180 ECTS)

15/150: B.Sc. IT-Sicherheit/ Informationstechnik [PO 22]

15/149: B.Sc. IT-Sicherheit /Informationstechnik [PO 20]