RUHR-UNIVERSITÄT BOCHUM

RUB

Master Studiengang IT-Sicherheit / Informationstechnik PO 13

Modulhandbuch

Fakultät für Elektrotechnik und Informationstechnik

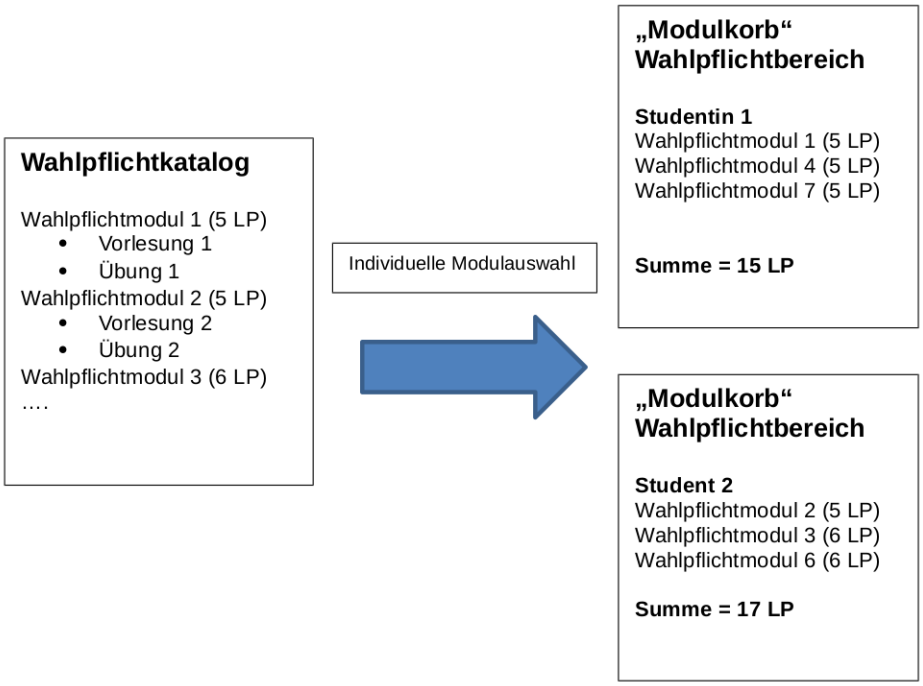
Erläuterung zum Wahlpflichtbereich des Studiengangs

Bei den Wahlpflichtbereichen (Anwendungen der IT-Sicherheit, Theorie der IT-Sicherheit und Informatik) handelt es sich jeweils um einen „Modulkorb“, der sich aus verschiedenen Modulen zusammensetzt. Die wählbaren Module sind im Wahlpflichtkatalog zusammengestellt. Die Studierenden können mit ihrer konkreten Auswahl eigene Schwerpunkte setzen.

Die Leistungspunkte (LP) jedes einzelnen Moduls werden den Studierenden nach der bestandenen Modulprüfung gutgeschrieben. Jedes einzelne Modul kann dabei innerhalb eines Semesters abschlossen werden.

Der Wahlpflichtbereich, also der Modulkorb, ist abgeschlossen, wenn die Studierenden Module aus dem zugehörigen Wahlpflichtkatalog im angegebenen Umfang abgeschlossen haben.

Die nachfolgende Grafik verdeutlicht diese Zusammenhänge:



Inhaltsverzeichnis

Kapitel 1

Module

1.1 Anwendungen der IT-Sicherheit

Nummer: 149912
Kürzel: WPF-MSITSIT-anwendungen-its
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: Mindestens 450 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: $\geq$15

Ziele: Die Studierenden haben ein vertieftes Verständnis in ausgewählten Themen der IT-Sicherheit. Sie kennen entsprechende Methoden und sind befähigt, diese zielgerichtet einzusetzen bzw. anzuwenden.

Inhalt: Anwendungsspezifische Vertiefung der IT-Sicherheit. Vertiefungen können beispielsweise in der Netzsicherheit, der eingebetten Sicherheit, oder der Systemsicherheit liegen.

Es sind Module aus dem Wahlpflichtkatalog des Studienschwerpunktes auszuwählen. Jedes Modul besteht aus je einer Lehrveranstaltung (Vorlesung + Übung) mit eigener Modulabschlussprüfung.

Zur Vermeidung von Mehrfachbeschreibungen jeweils identischer Module und Lehrveranstaltungen, wird direkt auf die Lehrveranstaltungsbeschreibung verwiesen, die auch die jeweils zugehörigen LP enthält.

Insgesamt sind im Wahlpflichtbereich Module im Gesamtumfang von mindestens 15 Leistungspunkten zu wählen.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

141251: Aktuelle Themen im Bereich der Internet-Sicherheit	4 SWS	(S.16)
141348: Aufbau eines Managementsystems für Informationssicherheit nach DIN ISO/IEC 27001	3 SWS	(S.21)
141342: Betriebssystemsicherheit	4 SWS	(S.25)
141480: Einführung in die Datenanalyse mit Anwendungen in der IT-Sicherheit und Privatsphäre	3 SWS	(S.36)
141247: Introduction to System Safety Engineering and Management	2 SWS	(S.51)
148219: Kryptanalytische Werkzeuge	4 SWS	(S.53)
148203: Kryptographie auf programmierbarer Hardware	4 SWS	(S.55)
141252: Message-Level Security	4 SWS	(S.131)
141032: Methoden der Benutzer-Authentisierung	3 SWS	(S.133)
141028: Physical Attacks and Countermeasures	4 SWS	(S.141)
148215: Private and Anonymous Communication	4 SWS	(S.146)
141241: Programmanalyse	4 SWS	(S.149)
141030: Software-Implementierung kryptographischer Verfahren	4 SWS	(S.158)
141033: Usable Security and Privacy	3 SWS	(S.165)
148216: Wireless Security	4 SWS	(S.171)

1.2 Informatik

Nummer: 149913
Kürzel: WPF-MSITSIT-informatik
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: Mindestens 450 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: $\geq$15

Ziele: Die Studierenden haben ein vertieftes Verständnis in ausgewählten Themen der theortischen oder praktischen Informatik. Sie kennen entsprechende Methoden und sind befähigt, diese zielgerichtet einzusetzen bzw. anzuwenden.

Inhalt: Vertiefung in verschiedenen Themen der theoretischen oder praktischen Informatik.

Es sind Module aus dem Wahlpflichtkatalog des Studienschwerpunktes auszuwählen. Jedes Modul besteht aus je einer Lehrveranstaltung (Vorlesung + Übung) mit eigener Modulabschlussprüfung.

Zur Vermeidung von Mehrfachbeschreibungen jeweils identischer Module und Lehrveranstaltungen, wird direkt auf die Lehrveranstaltungsbeschreibung verwiesen, die auch die jeweils zugehörigen LP enthält.

Insgesamt sind im Wahlpflichtbereich Module im Gesamtumfang von mindestens 15 Leistungspunkten zu wählen.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

150304: Datenbanksysteme	6 SWS	(S.28)
150322: Datenstrukturen	6 SWS	(S.30)
150320: Effiziente Algorithmen	6 SWS	(S.35)
141168: Embedded Multimedia	4 SWS	(S.38)
141374: Fundamentals of GPU Programming	3 SWS	(S.43)
141044: Grundlagen der automatischen Spracherkennung	4 SWS	(S.45)
141145: Hardware / Software Codesign	4 SWS	(S.47)
141144: Hardware Modeling and Simulation	4 SWS	(S.49)
310002: Künstliche Neuronale Netze	2 SWS	(S.59)
141150: Multi-Core Architekturen und deren Programmierung	4 SWS	(S.135)
310509: Nebenläufige Programmierung	3 SWS	(S.137)
148171: Sprachimplementierung	6 SWS	(S.160)
150240: Theoretische Informatik	6 SWS	(S.163)
310502: Vision in Man and Machine	3 SWS	(S.167)
148202: Web-Engineering	3 SWS	(S.168)
128968: Web-Engineering	4 SWS	(S.170)

1.3 Master-Praktikum ITS

Nummer: 149918
Kürzel: prak_MS_ITS
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 90 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 3

Ziele: Die Studierenden sind befähigt, in einem kleinen Team Aufgaben aus dem Bereich der IT-Sicherheit zu lösen und die Ergebnisse in ingenieurwissenschaftlicher Weise zu dokumentieren. Sie können gezielt Methoden der strukturierten Analyse anwenden und deren Wirkung analysieren.

Inhalt: Das Modul besteht aus einem Praktikum oder einem Projekt.

In den Praktika werden fortgeschrittene Themen der IT-Sicherheit behandelt. Mögliche Themen sind hier die FPGA-Programmierung von Kryptoverfahren oder Trusted Computing.

In einem Projekt werden komplexe Themen eigenständig im Verlauf eines Semesters bearbeitet. Mögliche Themen sind Implementierung von Webbasierten Sicherheitsmechanismen, oder SmartCard Implementierungen.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

1.4 Master-Seminar ITS

Nummer: 149917
Kürzel: sem_MS_ITS
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 90 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 3

Ziele: Die Studierenden sind befähigt, selbständig Literatur zu einem gegebenen Thema zu sichten, die wesentlichen Inhalte zu erfassen und diese wiederzugeben. Sie haben die Schlüsselqualifikationen zur Präsentation ihrer Ergebnisse: sowohl die schriftliche Ausarbeitung eines Themas, als auch Präsentationstechniken und rhetorische Techniken.

Inhalt: Einzelthemen aus dem gewählten Seminarthema werden in Vorträgen dargestellt. Die Studierenden halten jeweils einen Vortrag, hören die Vorträge der anderen Studierenden und diskutieren die Inhalte miteinander. Dabei geht es nicht um die reine Wissensvermittlung, sondern das Erlernen des wissenschaftlichen Diskurses. Daraus resultiert eine Anwesenheitspflicht an der zu Beginn des Seminars festgelegten Anzahl von Einzelterminen.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

1.5 Master-Startup ITS

Nummer: 149875
Kürzel: masterstartupits
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: Keine Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 1

Ziele: Erleichterung des Einstiegs in das Studium; Vernetzung der Studierenden untereinander; Einsicht in Berufsbilder, Karrieremöglichkeiten etc.

Inhalt: Studienbegleitende Informationen, Exkursionen, Vorträge etc.

Prüfungsform: Es handelt sich um eine freiwillige Zusatzveranstaltung.

Veranstaltungen:

140002: Master-Startup ITS 2 SWS (S.127)

1.6 Masterarbeit ITS

Nummer: 149890
Kürzel: MA-ITS
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 900 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 30

Ziele: Die Teilnehmer sind mit Arbeitsmethoden der wissenschafltichen Forschung und der Projektorganisation vertraut. Ihre fortgeschrittenen Kenntisse und Arbeitsergebnisse können sie verständlich präsentieren.

Inhalt: Weitgehend eigenständige Lösung einer wissenschaftlichen Aufgabe unter Anleitung. Teilnahme an 5 Kolloquiumsvorträgen über die Ergebnisse von Masterarbeiten in der Fakultät ET & IT. Präsentation der eigenen Ergebnisse der Masterarbeit im Kolloquium.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

144102: Masterarbeit ITS (S.129)

1.7 Nichttechnische Wahlfächer

Nummer: 149891
Kürzel: ntWafa-ITS
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: Mindestens 150 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: ≥ 5

Ziele: Innerhalb des Moduls setzen die Studierenden entsprechend ihrer Interessen verschiedene Schwerpunkte. Dafür steht Ihnen das breite Angebot der ganzen Universität zur Verfügung. Sie beherrschen entsprechend ihrer Auswahl verschiedene Schlüsselqualifikationen.

Inhalt: Die nichttechnischen Wahlfächer erweitern die Soft Skills. Z.B. wird die englische Fachsprache verbessert, in die Grundlagen der Rechtswissenschaften eingeführt oder Grundkenntnisse der Betriebswirtschaft vermittelt. Bei der Auswahl haben die Studierenden die Möglichkeit eine Auswahl entsprechend der eigenen Interessen zu treffen.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

141105: Nichttechnische Veranstaltungen (S.139)

1.8 Theorie der IT-Sicherheit

Nummer: 149911
Kürzel: WPF-MSITSIT-theorie-its
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: Mindestens 450 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: $\geq$15

Ziele: Die Studierenden haben ein vertieftes Verständnis in ausgewählten Themen der IT-Sicherheit. Sie kennen entsprechende Methoden und sind befähigt, diese zielgerichtet einzusetzen bzw. anzuwenden.

Inhalt: Theoriespezifische Vertiefung der IT-Sicherheit. Vertiefungen können beispielsweise in der Netzsicherheit, der eingebetten Sicherheit, oder der Systemsicherheit liegen.

Es sind Module aus dem Wahlpflichtkatalog des Studienschwerpunktes auszuwählen. Jedes Modul besteht aus je einer Lehrveranstaltung (Vorlesung + Übung) mit eigener Modulabschlussprüfung.

Zur Vermeidung von Mehrfachbeschreibungen jeweils identischer Module und Lehrveranstaltungen, wird direkt auf die Lehrveranstaltungsbeschreibung verwiesen, die auch die jeweils zugehörigen LP enthält.

Insgesamt sind im Wahlpflichtbereich Module im Gesamtumfang von mindestens 15 Leistungspunkten zu wählen.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148207: Algebraische Codierung für die sichere Datenübertragung	3 SWS	(S.18)
150334: Asymmetrische Kryptanalyse	3 SWS	(S.20)
141244: Authentische Schlüsselvereinbarung: Formale Modelle und Anwendungen	4 SWS	(S.23)
150361: Cryptocurrencies	3 SWS	(S.27)
150332: Deep Learning	2 SWS	(S.32)
148229: Digitale Signaturen	4 SWS	(S.33)
141213: Fundamentals of Data Science	4 SWS	(S.41)
150343: Kryptographische Protokolle	4 SWS	(S.57)
141212: Physical-Layer Security	4 SWS	(S.143)
150353: Privatheit und Authentizität	3 SWS	(S.147)
150355: Probabilistische Algorithmen	4 SWS	(S.148)
150277: Public Key Verschlüsselung	4 SWS	(S.151)
150318: Quantenalgorithmen	4 SWS	(S.152)
150345: Randomness in Cryptography	3 SWS	(S.153)
150359: Sicherheit und Privatheit für Big Data	3 SWS	(S.156)
150351: Symmetrische Kryptanalyse	4 SWS	(S.162)
150232: Zahlentheorie	6 SWS	(S.173)

1.9 Wahlfächer

Nummer: 149898
Kürzel: Wafa-ITS
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: Mindestens 750 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: $\geq$25

Ziele: Die Studierenden haben vertiefte Kenntnisse in technischen oder nichttechnischem Gebieten entsprechend ihrer Wahl. Dies beinhaltet sowohl die fachliche Vertiefung als auch den Erwerb von Schlüsselqualifikationen.

Inhalt: Bei der Auswahl geeigneter Lehrveranstaltungen kann das Vorlesungsverzeichnis der Ruhr-Universität verwendet werden. Dies schließt Veranstaltungen aller Fakultäten, des Optionalbereichs und des Zentrums für Fremdsprachenausbildung (Veranstaltungen aus Master-, Bachelor- oder Diplomstudiengängen) mit ein, also auch die Angebote der nichttechnischen Veranstaltungen . Im Rahmen einer Kooperationsvereinbarung mit der Fakultät für Elektrotechnik und Informationstechnik der TU Dortmund ist auch die Wahl dort angebotener Veranstaltungen möglich.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

141106: freie Veranstaltungswahl (S.40)

Kapitel 2

Veranstaltungen

2.1 141251: Aktuelle Themen im Bereich der Internet-Sicherheit

Nummer:	141251
Lehrform:	Vorlesungen und Übungen
Medienform:	Moodle
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozent:	Dr.-Ing. Juraj Somorovsky
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
angeboten im:	Wintersemester

Termine im Wintersemester:

Beginn: Montag den 07.10.2019
Vorlesung Montags: ab 08:15 bis 09:45 Uhr im ID 04/413
Übung Montags: ab 10:15 bis 11:45 Uhr im ID 04/413

Ziele:

- Aktuelle Forschungsthemen kennenlernen
- Details über neueste Angriffe und Sicherheitsmechanismen lernen

Inhalt: In der Vorlesung werden ausgewählte Themen der IT-Sicherheit behandelt, die vom Lehrstuhl NDS in den letzten Jahren publiziert wurden. Die Themen ergänzen Inhalte aus den Vorlesungen Netzsicherheit 1 und 2:

- Angriffe auf IKE
- TLS Fuzzing und State learning
- Angriffe auf Gridcoin
- Invalid curve attacks
- Angriffe auf eIDAS Infrastrukturen
- Efail
- Printer Hacking
- UI-Redressing und Clickjacking
- Document Object Model
- Die Technik hinter Google Docs
- Sicherheitsmodelle im Bereich von Instant Messaging
- TLS 1.3 und 0-RTT

Voraussetzungen: XXX

Empfohlene Vorkenntnisse: Die Veranstaltung baut (unter anderem) auf diesen Kursen auf:

- Netzsicherheit 1 und 2
- Einführung in die Kryptographie

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 38 Stunden sind für die Klausurvorbereitung vorgesehen.

exam: schriftlich, 120 Minuten

2.2 148207: Algebraische Codierung für die sichere Datenübertragung

Nummer: 148207
Lehrform: Vorlesungen und Übungen
Medienform: Tafelanschrieb
Verantwortlicher: Prof. Dr. Jörg Schwenk
Dozent: Dr.-Ing. Klaus Huber
Sprache: Deutsch
SWS: 3
Leistungspunkte: 4
angeboten im:

Ziele: Die Studierenden beherrschen detailliert die gängigsten Blockcodes wie BCH-, RS- und Goppacodes. Am Schluss der Vorlesung sind die Studierenden mit den Grundprinzipien der algebraischen Codierungstheorie vertraut und in der Lage Codierer und Decodierer für Standardcodes zu entwickeln.

Inhalt: Die (algebraische) Kanalcodierung stellt Methoden und Verfahren bereit, um Nachrichten gegenüber zufälligen Störungen auf einem Übertragungskanal zu sichern. Sie ist damit neben der Kryptologie ein wichtiges Gebiet der IT-Sicherheit. Die angewandten Prinzipien und Hilfsmittel sind sowohl in Codierung als auch Kryptologie oft dieselben oder ähnlich. So werden beispielsweise in beiden Disziplinen endliche Körper umfassend genutzt, in der algebraischen Codierung sind die benutzten Körper allerdings meist verhältnismäßig klein. Als weiteres Beispiel wäre der Euklidsche Algorithmus zu nennen, der in Kryptologie und Codierung eine zentrale Rolle spielt.

Gliederung

1. Übersicht und Einführung
2. Grundlagen
    - Lineare, Nichtlineare Codes,
    - Fehlererkennung und Korrektur,
    - Generator- und Prüfmatrizen,
    - Codeschranken,
    - Hammingcodes
3. Die wichtigsten Codeklassen
    - BCH-, RS-, Goppacodes
4. Decodierverfahren für die Hammingmetrik
    - Verfahren zur Decodierung von BCH-, RS-, und Goppacodes mittels des erweiterten Euklidschen Algorithmus.

5. Codes für andere Metriken
    - Berlekamps negazyklische Codes für die Lee-Metrik
    - Izyklische Codes für die Mannheim Metrik
6. Das Kryptosystem von McEliece
7. Die MacWilliamstransformation

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Spezielle Vorkenntnisse sind nicht erforderlich. Die nötigen mathematischen Hilfsmittel (z.B. endliche Körper oder zahlentheoretische Grundlagen) werden je nach Bedarf während der Vorlesung erarbeitet und mit Übungsaufgaben vertieft.

Arbeitsaufwand: 120 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 3 SWS entsprechen in Summe 42 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 22 Stunden sind für die Prüfungsvorbereitung vorgesehen.

exam: schriftlich, 120 Minuten

2.3 150334: Asymmetrische Kryptanalyse

Nummer: 150334
Lehrform: Vorlesungen und Übungen
Verantwortlicher: Prof. Dr. Alexander May
Dozent: Prof. Dr. Alexander May
Sprache: Deutsch
SWS: 3
Leistungspunkte: 4
angeboten im: Wintersemester

Ziele: Die Studierenden beherrschen die wichtigsten Algorithmen in der Kryptanalyse

Inhalt: Die Vorlesung gibt einen Einblick in fortgeschrittene Methoden der Kryptanalyse. Der Stoffplan umfasst die folgenden Themen:

- Pollards p-1 Methode
- Faktorisieren mit Elliptischen Kurven
- Pohlig-Hellman Algorithmus
- Cold-Boot Angriffe und Fehlerkorrektur von SchlŸsseln
- Generalisiertes Geburtstagsproblem
- Lšssen von polynomiellen Gleichungssystemen mit Gršbnerbasen
- Hilbert Basissatz und Buchberger Algorithmus
- Fourier und Hadamard Walsh Transformation

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Inhalte der Vorlesungen:
  - Einführung in die Kryptographie 1 und 2
  - Einführung in die asymmetrische Kryptanalyse

Arbeitsaufwand: 120 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 3 SWS entsprechen in Summe 42 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 22 Stunden sind für die Klausurvorbereitung vorgesehen.

exam: mündlich, 30 Minuten

2.4 141348: Aufbau eines Managementsystems für Informationssicherheit nach DIN ISO/IEC 27001

Nummer:	141348
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozent:	Dr.-Ing. Sebastian Uellenbeck
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	4
angeboten im:	Wintersemester und Sommersemester

Termine im Wintersemester:

Vorbesprechung: Freitag den 11.10.2019 ab 11:15

Termine im Sommersemester:

Vorbesprechung: Freitag den 05.04.2019 ab 09:15 bis 10:00 Uhr im ID 03/471

Ziele: Die Studierenden haben ein fundiertes Verständnis über den Aufbau eines ISMS nach ISO 27001 und kennen die notwendigen Schritte, um ein Unternehmen zur Zertifizierungsreife zu begleiten.

Inhalt: Die Lehrveranstaltung vermittelt fokussiert Inhalte aus der ISO/IEC 27001 Auditorensicht. Dazu ist folgende Gliederung geplant:

- Zielsetzung
- Prinzipien und Terminologien
- Auditprinzipien gemäß ISO 19011:2011 Richtlinien
- ISO 19011
- ISO 27001:2013 Dokumentation
- Auditvorbereitung: Pre-Audit Meeting und Auditpläne
- Vorbereitung von Checklisten
- Audittechniken
- Auditorenpräsentationen
- Auditergebnisse und Abschlusstreffen

- Abweichungen, Bericht der Beobachtungen und Folgemaßnahmen
- Folgemaßnahmen

Weitergehend werden technische Lösungsmittel besprochen, die auf dem Weg zur ISO 27001 Zertifizierung hilfreich sein können. Hierzu zählen unter anderem Security Information and Event Management Systeme (SIEM) und Identity Management Systeme (IdM).

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Vorkenntnisse über Systemsicherheit und Netzsicherheit z. B. aus den Vorlesungen Systemsicherheit 1/2 und Netzsicherheit 1/2.

Arbeitsaufwand: 120 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 3 SWS entsprechen in Summe 42 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 22 Stunden sind für die Prüfungsvorbereitung vorgesehen.

exam: schriftlich, 90 Minuten

2.5 141244: Authentische Schlüsselvereinbarung: Formale Modelle und Anwendungen

Nummer:	141244
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk M. Sc. Sebastian Lauer M. Sc. Paul Rösler
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
angeboten im:	Sommersemester

Termine im Sommersemester:

Beginn: Dienstag den 02.04.2019
Vorlesung Dienstags: ab 12:15 bis 13:45 Uhr im ID 04/413
Übung Dienstags: ab 14:00 bis 15:45 Uhr im ID 04/413

Ziele: Die Studierenden verstehen die Besonderheit kryptographischer Protokolle, bei denen nicht mehr ein Algorithmus im Vordergrund steht, sondern die Interaktion verschiedener Einheiten. Sie kennen die wichtigsten Konzepte bzgl. der beweisbaren Sicherheit von Protokollen. Die wichtigsten Bausteine kryptographischer Protokolle werden behandelt, so dass die Studierenden in der Lage sind, direkt in die wissenschaftliche Literatur zu diesem Thema einzusteigen.

Inhalt: Diese Vorlesung bietet eine Einführung in das Gebiet der kryptographischen Protokolle, die den Einsatz bekannter und neuer Verfahren der Kryptographie in der Kommunikation zwischen mehreren Instanzen beschreibt. Hierbei wird sowohl Wert auf die Beschreibungen als auch auf die Sicherheit gelegt. Die Vorlesung umfasst folgende Themen:

- Kryptographische Grundlagen (Kurze Widerholung der Wahrscheinlichkeitstehorie, Informationstheorie, etc.)
- Beweisbare Sicherheit
- Analyse von Schlüsselaustauschprotokollen, mit besonderem Fokus auf praktische Beispielprotokolle (wie TLS oder SSH)

Die Zusammenstellung ist nicht fest und kann nach Absprache mit den Hörern auch geändert werden.

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Grundkenntnisse Kryptographie
- Empfehlung: Durcharbeiten der ersten 40 Folien vom Skript Kryptographie I von Prof. Alexander May

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 38 Stunden sind für die Klausurvorbereitung vorgesehen.

exam: schriftlich, 120 Minuten

2.6 141342: Betriebssystemsicherheit

Nummer:	141342
Lehrform:	Vorlesungen und Übungen
Medienform:	e-learning rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozenten:	Prof. Dr. Thorsten Holz Dr.-Ing. Robert Gawlik
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
angeboten im:	Wintersemester

Termine im Wintersemester:

Beginn: Montag den 07.10.2019
Vorlesung Montags: ab 14:15 bis 15:45 Uhr im ID 04/471
Vorlesung Montags: ab 14:15 bis 15:45 Uhr im ID 04/459
Übung Montags: ab 16:15 bis 17:45 Uhr im ID 04/471
Übung Montags: ab 16:15 bis 17:45 Uhr im ID 04/459

Ziele: Die Studierenden beherrschen theoretische und praktische Aspekte der Sicherheit von Betriebssystemen und sind zu einer kritischen Betrachtung der Systemsicherheit in der Lage.

Inhalt: Im ersten Teil der Veranstaltung werden verschiedene Sicherheitsaspekte von Betriebssystemen vorgestellt und erläutert. Dazu werden sowohl wichtige Angriffsmethoden (z.B. *Buffer Overflows* oder *Race Conditions*) als auch Abwehrstrategien (z.B. nicht-ausführbarer Speicher oder *Address Space Layout Randomization*) diskutiert. Andere Themen, die im Mittelpunkt dieses Teils der Vorlesung stehen, sind Virtualisierung/Hypervisor sowie das sogenannte Einsperrungs-Problem (*Confinement Problem*) und die damit verbundene Analyse der verdeckten Kanäle in einem Computer-System.

Im zweiten Teil der Veranstaltung liegt der Schwerpunkt auf Schadsoftware. Dazu werden zunächst die Grundbegriffe in diesem Bereich erläutert und danach verschiedene Methoden zur Erkennung von Schadsoftware diskutiert. Wichtige Algorithmen in diesem Bereich werden vorgestellt und verschiedene Ansätze für Intrusion Detection Systeme werden behandelt.

Im praktischen Teil der Veranstaltung wird die Sicherheit von mehreren realen Systemen analysiert. Ein integraler Teil der Veranstaltung sind die Übungen, die den Stoff mit praktischen Beispielen veranschaulichen und vertiefen.

http://10kstudents.eu/s/img/10K_students_logo.png

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Erfahrung in systemnaher Programmierung sowie der Programmiersprache C sind hilfreich für das Verständnis der vermittelten Themen.

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 38 Stunden sind für die Klausurvorbereitung vorgesehen.

exam: schriftlich, 120 Minuten

2.7 150361: Cryptocurrencies

Nummer:	150361
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Jun. Prof. Dr. Sebastian Faust
Dozent:	Jun. Prof. Dr. Sebastian Faust
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	4.5
angeboten im:	

Ziele: Verständnis von kryptographischen Protokollen und Techniken im Einsatzgebiet von digitalen Währungen

Inhalt: Die Studierenden erlenen kryptographische Verfahren und Protokolle, die in der digitalen Wirtschaft eingesetzt werden. Neben Brands eCash verfahren, werden wird eine Einführung in kryptographische Währungen wie z.B. Bitcoin gegeben.

Themen sind: - kryptographische Protokolle - eCash - Kryptographische Währungen basierend auf Proof of Works (z.B. Bitcoin & Litecoin) - Alternative Mining Puzzles - Alternative kryptographische Währungen basierend auf Proof of Stake - Broadcast Verschlüsselung und sicheres Verteilen von digitalen Inhalten

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse aus der Vorlesung Kryptographie

Arbeitsaufwand: 135 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 3 SWS ergeben 42 Stunden Anwesenheit. Zum Lösen der Übungsaufgaben sind zwei Stunden je Woche vorgesehen. Es verbleiben 65 Stunden zur Vor- und Nachbereitung und zur Prüfungsvorbereitung.

exam: schriftlich, 120 Minuten

2.8 150304: Datenbanksysteme

Nummer: 150304
Lehrform: Vorlesungen und Übungen
Verantwortlicher: Dr. Edgar Korthauer
Dozent: Dr. Edgar Korthauer
Sprache: Deutsch
SWS: 6
Leistungspunkte: 9
angeboten im: Wintersemester

Termine im Wintersemester:

Beginn: Montag den 08.10.2018
Vorlesung Montags: ab 14:00 bis 16:00 Uhr im HNC 20
Vorlesung Freitags: ab 14:00 bis 16:00 Uhr im HMA 20
Übung (alternativ) Dienstags: ab 08:00 bis 10:00 Uhr im HZO 60
Übung (alternativ) Dienstags: ab 10:00 bis 12:00 Uhr im HZO 80
Übung (alternativ) Dienstags: ab 14:00 bis 16:00 Uhr im NC 3/99

Ziele: Die Studierenden sind in der Lage einschlägige Systemdokumentation und wissenschaftliche Literatur über Datenbanksysteme zu verstehen.

Inhalt:

- Implementierungstechniken für Datenstrukturen, die in Datenbanken Verwendung finden
- Konzeptionelle Grundlagen des Entity-Relationship-Modells
- Relationenalgebra
- Relationenkalkül
- Elemente der Sprache SQL und verwandter Systeme
- Normalformenlehre
- Optimierung von Anfragen durch Transformation
- Aspekte der parallelen Ausführung und Fehlerbehebung für Transaktionen

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundlagen der Informatik und Datenstrukturen

Arbeitsaufwand: 270 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Kontaktzeit in der Vorlesung und der Übung entspricht 84 Stunden (56 Stunden Vorlesung und 28 Stunden Übung). Für die Nachbereitung der Vorlesung und die Vorbereitung der Übung werden jeweils 62 Stunden veranschlagt. Für die Prüfungsvorbereitung sind weitere 62 Stunden vorgesehen.

exam: schriftlich, 90 Minuten

2.9 150322: Datenstrukturen

Nummer: 150322
Lehrform: Vorlesungen und Übungen
Medienform: Folien
Tafelanschrieb
Verantwortlicher: Prof. Dr. Hans Ulrich Simon
Dozent: Prof. Dr. Hans Ulrich Simon
Sprache: Deutsch
SWS: 6
Leistungspunkte: 9
angeboten im: Sommersemester

Termine im Sommersemester:

Vorlesung Dienstags: ab 14:00 bis 16:00 Uhr im HNC 30
Vorlesung Donnerstags: ab 14:00 bis 16:00 Uhr im HNC 30
Übung (alternativ) Dienstags: ab 12:00 bis 14:00 Uhr im NB 3/99
Übung (alternativ) Dienstags: ab 12:00 bis 14:00 Uhr im NC 2/99
Übung (alternativ) Dienstags: ab 16:00 bis 18:00 Uhr im NB 02/99

Ziele: Die Vorlesung soll die Fähigkeit schulen, bekannte Datenstrukturen professionell einzusetzen, neue Datenstrukturen bei Bedarf selbst zu entwerfen, die Korrektheit eines Algorithmus sauber zu begruenden und seine Laufzeit zu analysieren.

Inhalt: Nach einer Besprechung grundlegender Datentypen (wie Listen, Stacks, Queues und B“aume) werden zunaechst Datenstrukturen diskutiert, die zur Repräsentation von Mengen geeignet sind und dabei bestimmte Mengenoperationen unterstützen (wie zum Beispiel Dictionaries, Priority Queues und UNION-FIND-Datenstruktur). Weiterhin gehen wir auf Repräsentationen von Graphen ein, behandeln diverse Graphalgorithmen (wie zum Beispiel Tiefen- und Breitensuche, kürzeste Wege, transitive Hülle, starke Komponenten und minimaler Spannbaum) sowie diverse Sortierverfahren (Mergesort, Heapsort, Quicksort, Bucketsort, Radixsort).

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Elementare Sprachmerkmale der Programmiersprache Java ™,
- Mathematik-Kenntnisse im Umfang von „Höhere Mathematik I und II“

Arbeitsaufwand: 270 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Kontaktzeit in der Versnatlatung beträgt 84 Stunden (14 Wochen zu je 6 SWS). Zur Vor- und Nachbereitung sind 126 Stunden sowie für die Prüfungsvorbereitung 60 Stunden vorgesehen.

exam: schriftlich, 180 Minuten

Literatur:

[1] Drake, Peter "Data Structures and Algorithms in Java", Prentice Hall, 2005
[2] Dieker, Stefan, Güting, Ralf H. "Datenstrukturen und Algorithmen", Teubner Verlag, 2004

2.10 150332: Deep Learning

Nummer:	150332
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien
	Tafelanschrieb
Verantwortlicher:	Jun. Prof. Dr. Asja Fischer
Dozent:	Jun. Prof. Dr. Asja Fischer
Sprache:	Deutsch
SWS:	2
Leistungspunkte:	5
angeboten im:	Wintersemester

Termine im Wintersemester:

Beginn: Donnerstag den 11.10.2018
Vorlesung Donnerstags: ab 10:00 bis 12:00 Uhr im NA 02/99

Ziele: Die Vorlesung hat das Ziel, einen Einblick in dieses Gebiet zu vermitteln. Zu Beginn werden die grundlegenden Begriffe und Konzepte des maschinellen Lernens eingeführt. Im weiteren Verlauf wird auf verschiedene neuronale Netze, Gradienten-basierte Optimierungsverfahren und generative Modelle eingegangen.

Inhalt: Deep Learning ist ein Untergebiet des maschinellen Lernens, welches in den letzten Jahren zu Durchbrüchen in zahlreichen Anwendungsgebieten (wie z.B. in der Objekt- und Spracherkennung und der maschinellen Übersetzung) geführt hat.

Deep Learning Methoden finden unter anderem Anwendung im Bereich IT Security

Empfohlene Vorkenntnisse: Grundkenntnisse der Linearen Algebra und Wahrscheinlichkeitstheorie sind von Vorteil.

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 15 Wochen zu je 2 SWS ergeben 30 Stunden Anwesenheit. Es verbleiben 120 Stunden zur Vor- und Nachbereitung und zur Prüfungsvorbereitung.

exam: schriftlich, 120 Minuten

2.11 148229: Digitale Signaturen

Nummer:	148229
Lehrform:	Vorlesungen und Übungen
Medienform:	Tafelanschrieb
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr.-Ing. Tibor Jager
	M. Sc. Sebastian Lauer
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
angeboten im:	

Ziele: Im Rahmen dieser Vorlesung wird ein solides Grundverständnis für die Konstruktion von sicheren digitalen Signaturverfahren vermittelt. Grundlegende und moderne Techniken werden in der Vorlesung erklärt und anhand von Übungsaufgaben vertieft. Dies stellt eine ideale Vorbereitung auf eine forschungsnahe Abschlussarbeit in der (theoretischen) Kryptographie dar.

Inhalt:

- Grundlagen zu digitalen Signaturen
- Einmalsignaturverfahren
- Chamäleon-Hashfunktionen
- RSA-basierte Signaturverfahren
- Pairing-basierte Signaturverfahren
- Ausgewählte praktische Signaturverfahren und Angriffe

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Vorausgesetzt werden grundlegende Kryptographie-Kenntnisse, wie sie in der Vorlesung "Einführung in die Kryptographie und Datensicherheit" vermittelt werden. Dies schliesst zum Beispiel ein Grundverständnis des RSA-Verfahrens und des diskreten Logarithmusproblems ein.

Grundkenntnisse der theoretischen Informatik (z.B. Reduktionsbeweise) oder fortgeschrittene Kenntnisse der Kryptographie und diskreten Mathematik sind empfehlenswert.

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der

Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 5 Stunden pro Woche, in Summe 70 Stunden, erforderlich. Etwa 24 Stunden sind für die Klausurvorbereitung vorgesehen.

exam: schriftlich, 90 Minuten

2.12 150320: Effiziente Algorithmen

Nummer:	150320
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien
	Internet
	Tafelanschrieb
Verantwortlicher:	Priv.-Doz. Dr. Daniela Kacso
Dozent:	Priv.-Doz. Dr. Daniela Kacso
Sprache:	Deutsch
SWS:	6
Leistungspunkte:	9
angeboten im:	Sommersemester

Ziele: Die Studierenden kennen grundlegende Datenstrukturen und effiziente Algorithmen und sind mit Analysetechniken vertraut (Korrektheitsbeweis und Laufzeitanalyse).

Inhalt: Die Lehrveranstaltung kann sowohl in das Gebiet der praktischen als auch in das Gebiet der theoretischen Informatik eingeordnet werden. Die zentralen Themen sind die folgenden:

- Berechnung kürzester Pfade in einem Graphen bei ganzzahligen Kantenkosten
- Berechnung eines maximalen Flusses in einem Transportnetzwerk
- Berechnung einer optimalen Lösung bei einem Zuordnungsproblem (auch Matching-Problem genannt)

Darüberhinaus beschäftigen wir uns mit Anwendungen dieser grundlegenden Probleme.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Inhalte der Veranstaltung “Datenstrukturen”

Arbeitsaufwand: 270 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 6 SWS ergeben 84 Stunden Anwesenheit. Zur Vor-und Nachbereitung sind 126 Stunden sowie für die Prüfungsvorbereitung 60 Stunden vorgesehen.

exam: schriftlich, 120 Minuten

2.13 141480: Einführung in die Datenanalyse mit Anwendungen in der IT-Sicherheit und Privatsphäre

Nummer:	141480
Lehrform:	Vorlesungen und Übungen
Medienform:	Moodle rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr. rer. nat. Sascha Fahl
Dozent:	Prof. Dr. rer. nat. Sascha Fahl
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	4
angeboten im:	

Ziele: Die Studierenden erlernen die grundlegenden Fähigkeiten Datensätze wie sie etwa im Rahmen von Benutzerstudien oder Logfiles mit Bezug zu IT-Sicherheit anfallen mit Hilfe von empirischen und visuellen Methoden zu analysieren. Darüber hinaus erlangen sie praktische Fertigkeiten im Umgang mit der statistischen Auswertung mit der Programmiersprache Python und diversen Datenanalysebibliotheken.

Inhalt: Die Vorlesung behandelt insbesondere folgende Themen:

Einführung

- Überblick
- Motivation
- Statistische Grundlagen

Methodische Grundlagen

- Einführung in die Datenerhebung (z.b. Experiment- und Surveydesign)
- Einführung explorative Datenauswertung
- Deskriptive Statistik
- Hypothesentests
- Korrelation/Regressionsanalyse

Zentrale Themen

- Statistische Verfahren zur Datenauswertung
- Python zur statistischen Auswertung
- Visuelle Datenauswertung
- Case Studies

Voraussetzungen: Keine

Empfohlene Vorkenntnisse: Keine besonderen Vorkenntnisse erforderlich, Grundkenntnisse der IT-Sicherheit und Erfahrungen in Python sind aber hilfreich.

Arbeitsaufwand: 120 Stunden

Der Arbeitsaufwand setzt sich wie folgt zusammen: 15 Wochen zu je 3 SWS Anwesenheit (entspricht in Summe 45 Stunden). Für die Nachbereitung der Vorlesung und Vor- und Nachbereitung der Übung sind etwa 3 Stunden pro Woche, in Summe 45 Stunden, erforderlich. Etwa 30 Stunden sind für die Klausurvorbereitung vorgesehen.

exam: schriftlich, 120 Minuten

2.14 141168: Embedded Multimedia

Nummer:	141168
Lehrform:	Vorlesung mit integrierten Übungen
Medienform:	Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Rainer Martin
Dozent:	Dr. Wolfgang Theimer
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	6
angeboten im:	Sommersemester

Termine im Sommersemester:

Beginn:

Ziele: Die Studierenden erwerben grundlegende Fertigkeiten für das Systemdesign, die Implementierung, sowie die Integrations- und Testphase von Multimedialösungen im Bereich Embedded Systems. Sie sind befähigt, Hardware- und Softwarearchitekturen von eingebetteten Multimediasystemen zu bewerten. Sie sammeln anhand einer Linux-basierten Plattform Programmiererfahrungen und lösen in einem Projektteam eine Aufgabe aus dem Bereich der Multimediakommunikation.

Inhalt: Die Lehrveranstaltung vermittelt die Grundlagen zur Durchführung von Entwicklungsarbeiten im Bereich der eingebetteten Systeme, und hat den Fokus Multimediatechnologien. Zu Beginn der Vorlesung wird eine kurze Einführung in die Entwicklungsprozesse wie System Engineering, Softwareentwicklung und Testvorgehen gegeben, um die Projektteams methodisch vorzubereiten. Anschließend werden grundlegende Hardware- und Softwarearchitekturen von Embedded Systems präsentiert, um sie zu befähigen, Lösungskonzepte einordnen zu können. Der Fokus der Lehrveranstaltung liegt danach in der detaillierten Analyse einer eingebetteten Plattform am Beispiel des Raspberry Pi. Die Nutzung der Prozessorplattform und der Peripheriekomponenten wird anhand der plattformübergreifenden Entwicklungsumgebung Qt Creator unter C/C++ vertieft. Im Rahmen der praktischen Umsetzung in einem Projektteam erwerben die Studierenden die Fähigkeiten, gemeinsam ein Entwicklungsproblem zu strukturieren, ein Lösungskonzept zu entwickeln, und unter Zuhilfenahme von existierenden Softwaremodulen zu einer Gesamtlösung zu integrieren. Die Herangehensweise an die Problemstellung und die Lösung sind vom Projektteam zu dokumentieren und abschließend allen Teilnehmern zu präsentieren.

Voraussetzungen:

- Kenntnis der Programmiersprache C/C++

Empfohlene Vorkenntnisse:

- Objektorientierte Programmierung
- Grundlagen der Signalverarbeitung

Arbeitsaufwand: 180 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Zusätzlich entsteht Programmieraufwand für die praktische Implementierung studienbegleitender Projektaufgaben. Dafür werden in Summe 86 Stunden angesetzt. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind in Summe 14 Stunden, erforderlich. Etwa 24 Stunden sind für die Klausurvorbereitung vorgesehen.

exam: schriftlich, 120 Minuten

2.15 141106: freie Veranstaltungswahl

Nummer: 141106
Lehrform: Beliebig
Verantwortlicher: Dekan
Dozent: Dozenten der RUB
Sprache: Deutsch
angeboten im: Wintersemester und Sommersemester

Ziele: Innerhalb des Moduls setzen die Studierenden entsprechend ihrer Interessen verschiedene Schwerpunkte. Dafür steht Ihnen das breite Angebot der ganzen Universität zur Verfügung. Sie beherrschen entsprechend ihrer Auswahl verschiedene Schlüsselqualifikationen.

Inhalt: Bei der Auswahl geeigneter Lehrveranstaltungen kann das Vorlesungsverzeichnis der Ruhr-Universität verwendet werden. Dies schließt Veranstaltungen aller Fakultäten, des Optionalbereichs und des Zentrums für Fremdsprachenausbildung (Veranstaltungen aus Bachelor- oder Masterstudiengängen) mit ein, also auch die Angebote der nichttechnischen Veranstaltungen .

Zu beachten ist allerdings, dass bei Masterstudierenden in allen Fällen eine Anerkennung von Fächern aus dem zugehörigen Bachelorstudiengang nur sehr eingeschränkt möglich ist.

Weiterhin ist auch der Besuch von Lehrveranstaltungen anderer Univeristäten möglich - z.B. im Rahmen der Kooperationsvereinbarung mit der Fakultät für Elektrotechnik und Informationstechnik der TU Dortmund.

In der Fakultät wird speziell in diesem Bereich die Veranstaltung Methodik des wissenschaftlichen Publizierens angeboten. Im Rahmen der Kooperation mit der TU Dortmund wird folgende Veranstaltung angeboten: Musikdatenanalyse.

Voraussetzungen: entsprechend den Angaben zu der gewählten Veranstaltungen

Empfohlene Vorkenntnisse: entsprechend den Angaben zu der gewählten Veranstaltungen

exam: None, studienbegleitend

Beschreibung der Prüfungsleistung: Die Prüfung kann entsprechend der gewählten Veranstaltungen variieren.

2.16 141213: Fundamentals of Data Science

number:	141213
teaching methods:	lecture with tutorials
media:	rechnerbasierte Präsentation
responsible person:	Prof. Dr.-Ing. Aydin Sezgin
Lecturers:	Prof. Dr.-Ing. Aydin Sezgin
	M. Sc. Aya Ahmed
	M. Sc. Mohammadhossein Attar
	M. Sc. Sampath Thanthrige
language:	english
HWS:	4
Leistungspunkte:	5
angeboten im:	winter term

dates in winter term:

Beginn: Montag the 07.10.2019
Vorlesung Montags: from 12:15 to 13:45 o'clock in ID 04/401
Übung Freitags: from 14:15 to 15:45 o'clock in ID 04/401

goals: The students understand the concepts of pattern recognition, machine learning, and information theory and are able to apply it to data analysis. Equipped with tools and methods acquired during the lectures, problems arising regularly in engineering disciples can be investigated.

content: The view taken in the course is based on the ideas that data science is fundamentally rooted in information theory, as information theory is the pillar of most machine learning algorithms. Naturally, stochastic processes will also play a role, as sequences of events can be modeled nicely. The course has also a focus on Bayesian statistics and includes new developments in neural networks and deep learning.

The table of contents is as follows:

- Introduction
- Review: Linear Algebra
- Review: Probability Theory, Random variables and, Markov Chains, processes (Gaussian, Markov Decision)
- Least Mean Square Estimation
- Classification
- Bayesian Learning
- **Information theoretic learning**
  - Kullback-Leibler Divergence
  - ICA, Dictionary Learning,

  - k-SVD, Rate distortion theory,
  - entropy maximization, information bottleneck

- Neural networks and deep learning

As part of the exercise sessions, the students will implement various algorithms in Matlab:

- LMS, Kalman, Stochastic Gradient Descent,
- k-Means, KNN,
- Expectation Maximization, Backpropagation etc.

The focus of the course is on

- Discovery of regularities in data via Pattern recognition
- Development of algorithms via Machine learning (Classification, Clustering, Reinforcement Learning)
- Performance criteria via Information theory
- Hands-on experience

The main references for the course are:

- Sergios Theodoridis, Machine Learning- A Bayesian and optimization perspective.
- Simon Haykin, Neural Networks and Learning Machines
- Ian Goodfellow, Yoshua Bengio, Aaron Courville, Deep Learning

requirements: none

recommended knowledge: -Math I-IV -System theory I-III -Optimization

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 5 Stunden pro Woche, in Summe 70 Stunden, erforderlich. Etwa 24 Stunden sind für die Prüfungsvorbereitung vorgesehen.

exam: mündlich, 30 Minuten

literature:

[1] C. M., Bishop "Pattern Recognition and Machine Learning", Springer Verlag, 2006

2.17 141374: Fundamentals of GPU Programming

number: 141374
teaching methods: lecture with tutorials
media: Folien
responsible person: Prof. Dr. Ralf Peter Brinkmann
lecturer: Dr. Denis Eremin
language: english
HWS: 3
Leistungspunkte: 4
angeboten im: winter term

dates in winter term:

Beginn: Donnerstag the 10.10.2019
Vorlesung Donnerstags: from 14:15 to 15:45 o'clock in ID 03/471
Übung Donnerstags: from 16:15 to 17:00 o'clock in ID 03/471

goals: Die Studierenden erlernen das Programmieren auf Grafikprozessoren (GPUs)

content: Zu einem bestimmten Zeitpunkt um 2003 stieg die Rechenleistung nicht auf Kosten der Taktfrequenz des Prozessors, sondern durch Erhöhung der Anzahl der auf dem Prozessorchip zugewiesenen Rechenkerne. Grafikprozessoren (GPUs) sind die Meister dieser Computer-Hardware-Entwicklung und bieten bis zu Zehntausende einzelner Kerneinheiten. Gleichzeitig wird das GPU-Speichersystem nicht so sehr durch die Kompatibilitätsanforderungen mit älteren Generationen eingeschränkt wie CPU-Speichersysteme. Deswegen zeigen GPUs im Vergleich zu ihren älteren "Bruder" -Zentraleinheiten (CPUs) eine deutlich bessere Rohleistung der Recheneinheiten und des Speichersystems. Ursprünglich für Videobearbeitungsaufgaben entwickelt, wird die enorme Rechenleistung moderner GPUs üblicherweise zur Unterstützung von CPUs oder zur Lösung einer Vielzahl von Rechenproblemen mit (massiv) parallelisierbaren Teilen verwendet, wodurch Teraflops-hohe Rechenleistung kann schon auf Laptop- / Desktop-Computers erzielt werden. Der vorliegende Kurs zeigt, wie CUDA C (Erweiterung der C-Sprache für die GPU-Programmierung) und das entsprechende (sehr flexible!) CUDA-Laufzeit-API-Framework verwendet werden kann, um die Ausführung einiger typischer Programmiermuster um einen Faktor von 10 oder mehr zu beschleunigen das der CPU. Ausgehend vom CUDA-Programmiermodell geht man zum CUDA-Ausführungsmodell über und betrachtet grundlegende konzeptionelle, Software- und Hardwareprobleme, die zum Verständnis der Funktionsweise von GPUs beitragen. Fallstudien zu mehreren Problemen mit massiv parallelen Algorithmen, die in GPUs implementiert sind, werden ebenfalls weiter ausgeführt. Das theoretische Wissen, das in den Vorlesungen vermittelt wird, wird durch eine Vielzahl von praktischen Beispielen untermauert, an denen die Schüler zu Hause arbeiten können.

requirements: none

recommended knowledge: C (Programmiersprache)

Arbeitsaufwand: 120 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 3 SWS entsprechen in Summe 42 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 22 Stunden sind für die Prüfungsvorbereitung vorgesehen.

exam: mündlich, 30 Minuten

2.18 141044: Grundlagen der automatischen Spracherkennung

Nummer: 141044
Lehrform: Vorlesung und Praxisübungen
Medienform: Folien
Verantwortlicher: Prof. Dr.-Ing. Dorothea Kolossa
Dozent: Prof. Dr.-Ing. Dorothea Kolossa
Sprache: Deutsch
SWS: 4
Leistungspunkte: 6
angeboten im: Sommersemester

Termine im Sommersemester:

Beginn: Dienstag den 02.04.2019
Vorlesung Dienstags: ab 14:15 bis 15:45 Uhr im ID 04/445
Übung Mittwochs: ab 12:15 bis 13:45 Uhr im ID 2/201

Ziele: Die Teilnehmer verstehen die theoretischen und praktischen Grundlagen automatischer Spracherkennungssysteme. Sie sind in der Lage, die Kernalgorithmen eines einfachen Spracherkenners selbstständig zu implementieren und verstehen die Prinzipien von aktuellen Erkennungssystemen für kleines und großes Vokabular. Dabei wird auch ein Verständnis für die Entwicklung von automatischen Mustererkennungsverfahren für ein breites Anwendungsfeld entwickelt.

Inhalt: Die Vorlesung vermittelt Grundlagen und Algorithmen der maschinellen Spracherkennung in der Form, in der sie in aktuellen Systemen zur Erkennung fließender Sprache eingesetzt werden. Die folgenden Themen werden behandelt:

- Grundlagen: Phonetik, Sprachwahrnehmung
- Klassifikation mittels Deep Neural Networks und statistischer Methoden
- Merkmalsextraktion: Merkmale im Zeit- und Frequenzbereich, Cepstralanalyse
- Spracherkennung mit Hidden Markov Modellen: Algorithmen, Modellinitialisierung, Training und Einsatz von HMM/DNN-Systemen

Gleichzeitig werden in einem Python-Programmierpraktikum die Methoden angewandt. Die Übung ist projektorientiert; alle Übungsaufgaben zusammengenommen ergeben einen Verbundworterkenner für fließend gesprochene Ziffernketten. Dieser wird in Arbeitsgruppen von 2-3 Studenten erarbeitet.

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Grundkenntnisse der digitalen Signalverarbeitung
- Grundlegende Programmierkenntnisse

Arbeitsaufwand: 180 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 5 Stunden pro Woche, in Summe 70 Stunden, erforderlich. Etwa 54 Stunden sind für die Klausurvorbereitung vorgesehen.

exam: schriftlich, 120 Minuten

2.19 141145: Hardware / Software Codesign

Nummer:	141145
Lehrform:	Vorlesungen und Übungen
Verantwortlicher:	Prof. Dr.-Ing. Michael Hübner
Dozenten:	Prof. Dr.-Ing. Michael Hübner
	M. Sc. Florian Fricke
	M. Sc. Florian Kästner
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
angeboten im:	Sommersemester

Termine im Sommersemester:

Beginn: Mittwoch den 11.04.2018
Vorlesung Mittwochs: ab 08:15 bis 09:45 Uhr im ID 04/445
Übung Donnerstags: ab 10:15 bis 11:45 Uhr im ID 04/445

Ziele: Die Studierenden haben einen tiefen Einblick in modernste Entwurfsmethoden des HW / SW Codesigns. Sie haben einen gesamtheitlichen Überblick über eines der wichtigsten Gebiete für den Entwurf eingebetteter Systeme.

Inhalt: Der Inhalt dieser Vorlesung behandelt die Methoden des Hardware / Software Codesigns, d.h. der verzahnte Entwurf von digitaler Hardware und Software. Die Vorlesung erläutert mögliche Zielarchitekturen und führt dabei modernste Prozessortechnologien wie Superscalare Prozessoren, VLIW Prozessoren aber auch die traditionellen RISC und CISC Architekturen ein. Auch neuartige Multicore Prozessoren werden behandelt. Nachfolgend werden Methoden zur Abschätzung der Entwurfsqualität vertieft. Hierbei kommen Methoden wie z.B. Worst Case Execution Time Analysis, das Profiling und Tracing zur Sprache. Final werden partitionierungsverfahren wie Hierarchical Clustering, Fiduccia Mattheyses und auch genetische Algorithmen vertieft.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Inhalte der Vorlesungen

- Digitaltechnik
- Programmieren mit C

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 38 Stunden sind für die Klausurvorbereitung vorgesehen.

exam: schriftlich, 120 Minuten

Literatur:

[1] Bode, Arndt, Hennessy, John L., Patterson, David A. "Rechnerorganisation und -entwurf", Spektrum Akademischer Verlag, 2005

2.20 141144: Hardware Modeling and Simulation

Nummer:	141144
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien
Verantwortlicher:	Prof. Dr.-Ing. Michael Hübner
Dozenten:	Prof. Dr.-Ing. Michael Hübner
	M. Sc. Florian Fricke
	M. Sc. Florian Kästner
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
angeboten im:	

Termine im Sommersemester:

Beginn: Mittwoch den 11.04.2018
Vorlesung Mittwochs: ab 10:15 bis 11:45 Uhr im ID 04/459
Vorlesung Mittwochs: ab 10:15 bis 11:45 Uhr im ID 04/471
Übung Donnerstags: ab 08:15 bis 09:45 Uhr im ID 04/459
Übung Donnerstags: ab 08:15 bis 09:45 Uhr im ID 04/471

Ziele: Die Studierenden kennen die Hardwarebeschreibungssprache VHDL sowie die Methoden der Simulation, Evaluation und Verifikation für digitale elektronische Schaltungen.

Inhalt:

- Entwurfsprozesse für Integrierte Schaltungen und Printed Circuit Board
- Einführung in die Hardwarebeschreibungssprache VHDL
- Simulation, Evaluation und Verifikation digitaler Schaltungen
- SystemC

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Programmiererfahrung in C, C++, ggf. HDL (VHDL, Verilog)

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der

Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 38 Stunden sind für die Klausurvorbereitung vorgesehen.

exam: schriftlich, 120 Minuten

Literatur:

[1] Reichardt, Jürgen, Schwarz, Bernd "VHDL-Synthese: Entwurf digitaler Schaltungen und Systeme", Oldenbourg, 2009

2.21 141247: Introduction to System Safety Engineering and Management

number: 141247
teaching methods: lecture with integrated tutorials
media: rechnerbasierte Präsentation
responsible person: Prof. Dr.-Ing. Christof Paar
Lecturers: Prof. Dr.-Ing. Christof Paar
Dr. Oleg Lisagor
language: english
HWS: 2
Leistungspunkte: 3
angeboten im: summer term

dates in summer term:

Vorlesung: Dienstag the 11.06.2019 from 08:00 to 17:00 o'clock in ID 03/445
Vorlesung: Mittwoch the 12.06.2019 from 08:00 to 17:00 o'clock in ID 03/445
Vorlesung: Donnerstag the 13.06.2019 from 08:00 to 17:00 o'clock in ID 03/445
Vorlesung: Freitag the 14.06.2019 from 08:00 to 17:00 o'clock in ID 03/445
Übung: Dienstag the 11.06.2019 from 08:00 to 17:00 o'clock in ID 03/419
Übung: Mittwoch the 12.06.2019 from 08:00 to 17:00 o'clock in ID 03/419
Übung: Donnerstag the 13.06.2019 from 08:00 to 17:00 o'clock in ID 03/419
Übung: Freitag the 14.06.2019 from 08:00 to 17:00 o'clock in ID 03/419

goals: On completion of this block course, participants will:

- understand risk, and the factors influencing perception and acceptability of risk;
- be able to give definitions of safety-related terminology and discuss how the use of terminology varies between countries and industrial sectors;
- have an understanding of typical safety-critical systems lifecycles and the roles of the major groups of techniques within the lifecycle.

content: This block course provides an introduction to the basic concepts and principles of system safety, including risk, hazard, accidents, and failure, and techniques for safety analysis and assessment. It also provides a brief overview of related material, such as legal issues, management of safety critical projects, and human factors.

Topics include:

- Introduction to accidents, hazards and risk;
- Formal definitions of safety engineering terminology;
- Legal and moral context;

- System lifecycles view of safety activities;
- The concept of Safety Risk and making decisions about risk;
- Introduction to Safety Cases;
- Overview of safety analysis techniques;
- Safety-critical software;
- Introduction to Safety Cases;
- Introduction to Safety Management

In the end, participants have to complete an assessment approximately over the next six weeks which results in the final grade for this course.

Students can choose to only do a short assessment, which results in ungraded 2 CP for this course (only as a free elective course), instead of 3 graded CP (as a mandatory elective course).

requirements: none

Arbeitsaufwand: 90 Stunden

The workload is accumulated as follows: 4 days with 8 HWS each correspond to a total of 32 hours of physical presence. For the preparation of exercises and further reading accumulated 30 hours are required. About 28 hours are required in preparation for the examination.

exam: Projektarbeit, continual assessment

2.22 148219: Kryptanalytische Werkzeuge

Nummer:	148219
Lehrform:	Vorlesungen und Übungen
Verantwortlicher:	Prof. Dr.-Ing. Tim Güneysu
Dozenten:	Prof. Dr.-Ing. Tim Güneysu
	Dr.-Ing. Tobias Schneider
	Dr.-Ing. Alexander Wild
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
angeboten im:	

Ziele: Die Teilnehmer kennen wesentliche praktische Komponenten und Werkzeuge der Kryptanalyse. Sie haben einen umfangreichen Überblick über Algorithmen und Techniken, die heutzutage zur Analyse bestehender Systeme einge-setzt werden. Des Weiteren können sie nicht nur Kenntnisse über die neuesten Analyseverfahren, sondern auch die Grenzen bezüglich Rechen,- Speicher- und finanzieller Aufwand anwenden. Mit dem vermittelten Wissen, ist es den Teilnehmern zum Ende des Kurses möglich, unterschiedliche Methoden zur Analyse von bestehenden Systemen erfolgreich anzuwenden sowie die Limitierungen von Sicherheitsanalysen einschätzen zu können.

Inhalt: Diese Veranstaltung stellt Methoden und Werkzeuge zur Analyse von Sicherheits-mechanismen und kryptographischen Systemen vor. Der praktische Bezug der Methoden steht hierbei im Vordergrund, sodass die Ansätze insbesondere bezüglich verschiedener Rechnerplattformen verglichen werden. Hauptbestandteile der Veranstaltung sind dabei Möglichkeiten der effizienten Passwort- und Schlüsselsuche bzw. -extraktion für kryptographische Systeme. Hierbei werden Lösungen und Werkzeuge für Rechenplattformen wie PC-Clustern, Grafikkarten sowie Spezialhardware vorgestellt.

Im Rahmen der Vorlesung werden neben wöchentlichen vorlesungsbegleitenden Übungen drei integrierte praktische Workshops angeboten, um die vermittelten Lerninhalte mittels selbstentwickelten kryptanalytischen Werkzeugen weiter zu vertiefen.

Die Themen dieser Workshops sind:

1) Werkzeuge zur Geheimnisidentifikation: Entwicklung effizienter Passwortsuchstrategien

2) Werkzeuge zur symmetrische Kryptanalyse: Durchführung eines Time-Memory Trade-Off Angriffs auf Blockchiffren

3) Werkzeuge zur asymmetrische Kryptanalyse: Angriff auf ein Elliptisches Kurven Kryptosystem mittels des verteilten Pollard-Rho Algorithmus

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse der Kryptographie, über Rechnerarchitekturen und der Computerprogrammierung

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 2 Stunden pro Woche, in Summe 28 Stunden, erforderlich. Für drei begleitende Projekte sind je etwa 15 Stunden vorgesehen. Etwa 21 Stunden verblieben für die Klausurvorbereitung.

exam: schriftlich, 120 Minuten

2.23 148203: Kryptographie auf programmierbarer Hardware

Nummer:	148203
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Tim Güneysu
Dozent:	Prof. Dr.-Ing. Tim Güneysu
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
angeboten im:	

Ziele: 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 insbesondere 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 Unclonable 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 Blackboard-Kurs angeboten, der zusätzliche Inhalte sowie die praktischen Übungen bereithält.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Die Vorlesung baut auf Grundlagenstoff der folgenden Vorlesungen auf:

1) Grundlagen der Kryptographie und Datensicherheit

2) Computerarchitektur

3) Basiswissen Digitaltechnik

Empfehlenswert sind weiterhin Kenntnisse in folgenden Themenbereichen, die in der Vorlesung nur auszugsweise behandelt werden:

1) Schaltungsentwurf mit VHDL

2) Parallele Algorithmen und deren Programmierung

3) Implementierung kryptographischer Systeme

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Übungsaufgaben mit integrierten kleinen Programmieraufgaben und der Nachbereitung der Vorlesung sind etwa 70 Stunden (ca. 5 Stunden / Woche) vorgesehen. Da bei regelmäßiger Bearbeitung der Übungen der gesamte Lehrstoff vertieft wird, sind für die Prüfungsvorbereitung lediglich 24 Stunden angesetzt.

exam: schriftlich, 120 Minuten

2.24 150343: Kryptographische Protokolle

Nummer: 150343
Lehrform: Vorlesungen und Übungen
Verantwortlicher: Prof. Dr. Eike Kiltz
Dozent: Prof. Dr. Eike Kiltz
Sprache: Deutsch
SWS: 4
Leistungspunkte: 5
angeboten im: Sommersemester

Termine im Sommersemester:

Beginn: Donnerstag den 04.04.2019
Vorlesung Donnerstags: ab 10:00 bis 12:00 Uhr im NB 02/99
Übung Donnerstags: ab 08:00 bis 10:00 Uhr im IA 1/181

Ziele: Die Studierenden verstehen die erweiterten mathematischen Methoden und Verfahren, auf denen moderne kryptographische Protokolle beruhen. Die Teilnehmer sind zur Analyse und dem Design aktueller und zukünftiger kryptographischer Methoden befähigt.

Inhalt: Die Vorlesung beschäftigt sich mit erweiterten kryptographischen Protokollen und deren Anwendungen. Hierbei wird insbesondere Wert auf eine formale Sicherheitsanalyse im Sinne von beweisbarer Sicherheit gelegt.

- Themenübersicht:
  - Identity-based Encryption
  - Digital Signatures
  - Secret sharing
  - Threshold Cryptography
  - Secure Multiparty Computation

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Inhalte des Moduls Kryptographie

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 38 Stunden sind für die Klausurvorbereitung vorgesehen.

exam: mündlich, 30 Minuten

2.25 310002: Künstliche Neuronale Netze

Nummer:	310002
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Priv.-Doz. Dr. Rolf P. Würtz
Dozent:	Priv.-Doz. Dr. Rolf P. Würtz
Sprache:	Deutsch
SWS:	2
Leistungspunkte:	5
angeboten im:	Wintersemester

Termine im Wintersemester:

Beginn: Freitag den 12.10.2018

Ziele: Die Studierenden beherrschen eine Reihe von Standardverfahren sowie neuerer Entwicklungen aus dem Bereich der künstlichen neuronalen Netze, die Funktionsweise und Anwendungsmöglichkeiten der behandelten Modelle sowie ihr Zusammenhang mit konventionellen mathematischen Methoden. Sie kennen Möglichkeiten und Grenzen der einzelnen Verfahren, sowohl für unüberwachtes als auch für überwachtes Lernen. Die Studierenden haben ein Verständnis der Technik künstlicher neuronaler Netzwerke zur Mustererkennung und Funktionsapproximation, sowie Stärken und Schwächen für praktische Anwendungen.

Inhalt:

- Problem Mustererkennung
- Problem Regression
- Kleinste Quadrate
- Lineare Diskriminanten
- Einschichtennetzwerke
- Limitierung von Einschichtennetzwerken
- Perzeptron Konvergenztheorem
- Mehrschichtennetzwerke
- Backpropagation
- Approximationstheorie für Zweischichtennetzwerke
- Perzeptron Konvergenztheorem

- RBF-Netzwerke
- Neuronale Karten

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Lineare Algebra
- Differentialrechnung
- Wahrscheinlichkeitsrechnung

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Kontaktzeit in der Vorlesung und der Übung entspricht 42 Stunden (28 Stunden Vorlesung und 14 Stunden Übung). Für die Vorbereitung der Übung - wozu implizit auch die Nachbereitung der Vorlesung gehört - und das Lösen der Übungsblätter mit je einer theoretischen und einer praktischen Aufgabe werden 108 Stunden (6 Übungsblätter * 18 Stunden) veranschlagt. Pro Übungsblatt werden ca. 12 Stunden für das Lösen der praktischen Aufgabe veranschlagt, was einem praktischen Anteil von ca. 6 * 12, also 72 Stunden entspricht.

exam: Projektarbeit, studienbegleitend

Literatur:

[1] C. M., Bishop "Pattern Recognition and Machine Learning", Springer Verlag, 2006

2.26 142061: Master-Forschungspraktikum Usable Security und Privacy

Nummer:	142061
Lehrform:	Praktikum
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Markus Dürmuth
Dozenten:	Prof. Dr. Markus Dürmuth M. Sc. Maximilian Golla Prof. Dr. Martina Angela Sasse
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Wintersemester und Sommersemester

Termine im Wintersemester:

Vorbesprechung: Donnerstag den 10.10.2019 ab 15:15 im ID 03/401
Praktikum Donnerstags: ab 15:15 bis 16:45 Uhr im ID 03/401

Termine im Sommersemester:

Vorbesprechung: Donnerstag den 11.04.2019 ab 15:15 im ID 04/401
Praktikum Donnerstags: ab 15:15 bis 16:45 Uhr im ID 04/401

Ziele: Die Veranstaltung wird im Sommersemester 2019 nicht angeboten.

Diese Veranstaltung vermittelt praktische Kenntnisse in den Forschungsgebieten Usabel Security und Privacy. Die Studierenden werden in die Lage versetzt, eigenständig Studien hinsichtlich der Usability von sicherheits- und privacyrelevanten Systemen durchzuführen, auszuwerten und kritisch zu hinterfragen.

Inhalt: Neben der notwendigen theoretischen Methodik, die in großen Teilen von der Vorlesung Usable Security and Privacy abgedeckt wird, werden in diesem Kurs vor allem die praktischen Aspekte der Usable Security und Privacy Forschung besprochen. Zunächst werden die Grundlagen über die Durchführung von Nutzerstudien aus der Vorlesung wiederholt und mit Hilfe von aktuellen Beispielen aus dem Bereich Usable Security und Privavcy Forschung vertieft. In Gruppen werden anschließend, unter Anleitung, eigene Nutzerstudien geplant, getestet, durchgeführt, ausgewertet, verschriftlicht und bewertet. Zum Abschluss des Praktikums werden die Ergebnisse in einer Präsentation vorgestellt und in einer kurzen wissenschaftlichen Arbeit verschriftlicht und diskutiert. Alle Studierenden durchlaufen in Ihrer Gruppe dabei die folgenden Schritte:

- Entwurf von Forschungsfragen, Interview-Protokollen, Fragebögen etc.

- Entwicklung von Prototypen
- Pilotversuch und anschließende Überarbeitung
- Kurzvortrag zum aktuellen Fortschritt
- Durchführung der Studie mit mindestens 10 Personen (oder mehr, falls online)
- Abschlussvortrag
- Schreiben einer englischsprachigen 4-seitigen wissenschaftlichen Arbeit
- Erstellen eines kritischen Reviews (500 Wörter)

Voraussetzungen: Keine

Empfohlene Vorkenntnisse:

- Usable Security and Privacy
- Allgemeine Kenntnisse der IT-Sicherheit

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Anwesenheit beträgt 3 SWS * 14 Wochen, also 42 Stunden. Zum Schreiben des geforderten Quelltextes werden weitere ca. 48 Stunden benötigt.

exam: Praktikum, studienbegleitend

2.27 142027: Master-Praktikum ARM Processors for Embedded Cryptography

Nummer:	142027
Lehrform:	Praktikum
Medienform:	Moodle
Verantwortlicher:	Prof. Dr.-Ing. Christof Paar
Dozenten:	Prof. Dr.-Ing. Christof Paar M. Sc. Max Hoffmann
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Wintersemester

Termine im Wintersemester:

Vorbesprechung: Mittwoch den 10.10.2018 ab 15:00 im ID 2/632
Praktikum Dienstags: ab 10:15 bis 11:45 Uhr im ID 04/445

Ziele: Absolventen des Praktikums kennen den Aufbau und die interne Funktion von Mikrocontrollern. Sie wissen wie ein Prozessor Maschinensprache verarbeitet und sind selbst in der Lage mittels Assembly maschinennah zu programmieren. Zudem sind sie in der Lage, hocheffiziente Implementierungen für die ARM Architektur zu erstellen, welche eine deutliche Geschwindigkeitsverbesserung im Vergleich zu C Implementierungen vorweisen. Da das Praktikum im besonderen ARM-Prozessoren behandelt und ARM eindeutiger Marktführer der Embedded-Branche ist, sind die Inhalte dieses Praktikums äußerst relevant. Das Praktikum setzt sich selbst das Ziel möglichst praxisnah zu arbeiten und die Aufgaben interessant zu gestalten, sodass die Teilnehmer einen Nutzen für spätere Arbeiten daraus ziehen können.

Inhalt: In diesem Praktikum wird der Umgang mit ARM Mikrocontrollern erarbeitet. Dazu erhält jeder Teilnehmer ein Board mit einem ARM Cortex-M4 basierten Mikrocontroller. Die Teilnehmer erlernen zunächst die Grundlagen über CISC und RISC Mikrocontroller. Sie erlernen, wie Code von Hardware ausgeführt wird und wie sie selbst maschinennahen Code schreiben können. Bereits nach den ersten beiden Praktikumsterminen sind die Teilnehmer in der Lage, kleine Programme in Assembly für die ARM Architektur zu entwickeln. Während der folgenden Termine werden die Kenntnisse bezüglich der ARM Architektur und des Boards vertieft. Die Teilnehmer lernen, wie Mikrocontroller untereinander und mit Peripheriegeräten kommunizieren. Die theoretischen Inhalte werden von praktischen Hausaufgaben begleitet. Die Teilnehmer implementieren nach und nach Programme in C und Assembly, um verschiedene Funktionalitäten des Boards zu verwenden. Nachdem die Teilnehmer mit ARM Assembly vertraut geworden sind, werden unterschiedliche kryptographische Anwendungen implementiert. Dabei liegt der Fokus besonders auf Effizienz und es muss stets eine C Implementierung

geschlagen werden. Die besten Teilnehmer erhalten ein Zertifikat sowie einen Preis.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse in Kryptographie (Einführung in die Kryptopgraphie I und II) und C

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 6 Termine zu je 3 Stunden entsprechen 18 Stunden Anwesenheit. Für die Vorbereitung werden 18 Stunden (3 Stunden je Termin für 6 Termine), für die Bearbeitung der Übungszettel 9 Stunden (3 Stunden je Übungszettel für drei Übungszettel), und für die Implementierungsaufgaben 45 Stunden veranschlagt.

exam: Praktikum, studienbegleitend

2.28 143143: Master-Praktikum Embedded Linux

Nummer: 143143
Lehrform: Praktikum
Verantwortlicher: Prof. Dr.-Ing. Michael Hübner
Dozent: Prof. Dr.-Ing. Michael Hübner
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
angeboten im:

Termine im Wintersemester:

Vorbesprechung: Dienstag den 10.10.2017 ab 16:15 im ID 1/103
Praktikum Dienstags: ab 16:00 bis 19:00 Uhr im ID 03/121

Ziele: Die Studierenden haben die Grundlagen von Embedded Linux kennen gelernt und können auch dieses Betriebssystem praktisch auf einen FPGA integrieren. Besonders der Umgang mit späteren Erweiterungen der Hardware und die Anbindung an den Prozessor bietet eine hervorragende Möglichkeit Kenntnisse dieser modernen Entwurfsmethodik zu erwerben.

Inhalt: Das Master-Praktikum Embedded Linux zeigt die Funktion und praktische Realisierung von embedded Linux auf einem FPGA Board. Hierbei werden alle Schritte durchlaufen, bis ein Kernel auf einem FPGA integriert ist und über ein Terminal angesprochen werden kann. Im Folgenden werden Hardwareerweiterungen für das Prozessorsystem entwickelt und Treiber für diese Erweiterungen programmiert.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Programmieren in C

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 8 Wochen zu je 3 SWS entsprechen 24 Stunden Anwesenheit. Für die Vorbereitung und Ausarbeitung werden jeweils 8 Stunden, insgesamt 64 Stunden veranschlagt. Es verbleiben 2 Stunden für die sonstige Organisation der Praktikumsdurchführung.

exam: Praktikum, studienbegleitend

2.29 142020: Master-Praktikum Embedded Smartcard Microcontrollers

Nummer:	142020
Lehrform:	Praktikum
Medienform:	Folien rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Christof Paar
Dozenten:	Prof. Dr.-Ing. Christof Paar M. Sc. Max Hoffmann
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	

Ziele: Dieses Praktikum verfolgt im Wesentlichen die folgenden drei Lernziele: Erstens kennen die Teilnehmer des Praktikums eine 8-Bit Mikrocontrollerarchitektur und deren Programmierung in Assembler. Zweitens wird der Umgang mit Smartcards, sowie Wissen über die entsprechenden Industriestandards beherrscht. Drittens sind die Implementierungsaspekte praktisch relevanter Blockchiffren (AES, 3DES, lightweight Chiffren etc.) bekannt. Dabei ist relevant, dass sowohl C, als auch Assembler die dominanten Programmiersprachen für Smartcards und viele andere eingebettete kryptographische Lösungen sind.

Inhalt: In diesem Praktikum werden zwei Themengebiete erarbeitet. Zunächst erlernen die Teilnehmer des Praktikums Grundlagen über CISC und RISC Mikrocontroller. Bereits nach dem ersten Praktikumstermin sind die Studenten in der Lage kleine Programme in Assembler für die Atmel RISC AVR Architektur zu entwickeln. Während der folgenden Termine werden die Kenntnisse bezüglich der AVR Architektur vertieft. Darüber hinaus müssen die Praktikumsteilnehmer immer komplexere Programme als Hausaufgaben schreiben. Im zweiten Teil des Praktikums erlernen die Studenten den Umgang mit Smartcards und den zugehörigen Industriestandards. Der Standard ISO 7816 und die zugehörigen T=0/T=1 Übertragungsprotokolle werden vorgestellt. Jeder Student erhält Zugriff auf eine Smartcard mit einem Atmel AVR Mikrocontroller, sowie einem Kartenschreib- bzw. -lesegerät. Dieser implementiert zwei vorgegebene Blockchiffren (die jährlich wechseln) in Assembler, und muss diese auf der Smartcard unter realistischen Bedingungen lauffähig bekommen. Beispiele für Algorithmen sind AES, 3DES und lightweight Chiffren. Um die Motivation der Praktikumsteilnehmer zu erhöhen, werden die effizientesten Implementierungen mit einer Urkunde und einem Buchpreis belohnt.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse Kryptographie, z.B. aus dem Modul Einführung in die Kryptographie und Datensicherheit.

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 6 Termine zu je 3 Stunden entsprechen 18 Stunden Anwesenheit. Für die Vorbereitung werden 18 Stunden (3 Stunden je Termin für 6 Termine), für die Bearbeitung der Übungszettel 9 Stunden (3 Stunden je Übungszettel für drei Übungszettel), für die Implementierung der Chiffre in Gruppenarbeit 40 Stunden und für die Vorbereitung auf das Prüfungsgespräch 5 Stunden veranschlagt.

exam: Praktikum, studienbegleitend

2.30 142181: Master-Praktikum Entwurf integrierter Digitalschaltungen mit VHDL

Nummer:	142181
Lehrform:	Praktikum
Verantwortlicher:	Prof. Dr.-Ing. Michael Hübner
Dozenten:	Prof. Dr.-Ing. Michael Hübner
	M. Sc. Keyvan Shahin
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	

Ziele: Die Studierenden sind zum Entwurf integrierter Digitalschaltungen unter Verwendung der Hardware-Beschreibungssprache VHDL befähigt. Sie können mit modernen Entwurfswerkzeugen der Mikroelektronik umgehen.

Inhalt: Der Entwurf von VLSI-Schaltungen ist aufgrund der großen Anzahl von Bauelementen nur zu beherrschen, wenn man Hardware-Beschreibungssprachen wie VHDL für den Entwurf einsetzt. Eine ganze Reihe von Eigenschaften macht VHDL für den Mikroelektronik-Entwurf so interessant. Dazu zählen: VHDL ist nicht technologiespezifisch, es ist das geeignete Medium zum Austausch zwischen Entwerfern untereinander und mit dem Chiphersteller, VHDL unterstützt Hierarchie und Top-down- und Bottom-up-Entwurfsmethoden, es unterstützt ferner Verhaltens-, Struktur- und Datenfluss-Beschreibung, es ist ein IEEE-Standard, Testmuster können mit derselben Sprache generiert werden u.a.m.

Das Praktikum findet basierend auf aktuellen FPGA-Architekturen und mit aktueller Synthesesoftware statt. Nach einem einführenden Tutorial in die Entwicklungsumgebung “Vivado” von Xilinx, werden Schaltwerke und Schaltnetze für unterschiedlichste Aufgaben erstellt, simuliert und auf echter Hardware getestet.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Wünschenswert sind Kenntnisse des Faches “Integrierte Digitalschaltungen”

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 12 Termine zu je 3 SWS entsprechen 36 Stunden Anwesenheit. Für die Vorbereitung werden 24 Stunden (2 Stunden je Praktikumstermin), für die Ausarbeitung der Dokumentation

24 Stunden (2 Stunden je Termin) und für die Zwischen- und Abschlussbesprechung inkl. Vorbereitung der Präsentationen 6 Stunden (jeweils 3 Stunden) veranschlagt.

exam: Praktikum, studienbegleitend

Literatur:

[1] Reichardt, Jürgen, Schwarz, Bernd "VHDL-Synthese: Entwurf digitaler Schaltungen und Systeme", Oldenbourg, 2009

2.31 142022: Master-Praktikum Java-Card

Nummer:	142022
Lehrform:	Praktikum
Verantwortlicher:	Prof. Dr.-Ing. Christof Paar
Dozenten:	Prof. Dr.-Ing. Christof Paar
	Dr.-Ing. Pawel Swierczynski
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Sommersemester

Termine im Sommersemester:

Vorbesprechung: Mittwoch den 11.04.2018 ab 15:15 im ID 2/632
Praktikum Mittwochs: ab 16:15 bis 17:45 Uhr im ID 2/632

Ziele: Nach dem erfolgreichen Abschluss des Praktikums versteht der Studierende folgende Zusammenhänge:

- Authentifizierung (Challenge/Response Protokoll) gegenüber dem Kartenmanager der Java Card zur Verwaltung des Systems
- Erstellen von kryptographischen Java Card Applets
- Aufruf der Funktionen des Hardware Co-Prozessors
- Übertragung und Installation von Java Card Applets
- Ansteuern von Java Card Applets
- Verarbeiten eingehender APDUs sowie Erstellen ausgehender APDUs, usw.
- Umgang mit dem Übertragungsprotokoll in C++

Inhalt: In diesem Praktikum erlernen die Teilnehmer den sicheren Umgang mit Java Cards. Diese Smart Cards können spezielle Java Applets auf einem Mikrocontroller ausführen. Die Programmiersprache Java kommt in Millionen von eingebetteten Geräten zum Einsatz, z.B. in SIM Karten, die den GSM Standard implementieren. Dabei stellen Java Cards die kleinste aller bekannten Java Plattformen dar. Diese führen einen reduzierten Satz von Java Code aus und bieten eine Schnittstelle zu sicheren kryptographischen Co-Prozessoren (DES, 3-DES, AES, usw.), welche den Ver- und Entschlüsselungsprozess erheblich beschleunigen. Der erste Teil des Praktikums erläutert Grundlagen über die Funktionsweise und den Aufbau von Java Cards. Anschließend wird den Teilnehmern vermittelt, wie die Authentifizierung (SCP01/SCP02) gegenüber einer Java Card funktioniert. In einem dritten Schritt erlernen die Teilnehmer das Erstellen von Java Card Applets, deren Konvertierung und Upload auf die Java Card selbst. Anschließend

wird den Teilnehmern vermittelt wie die eigenes erstellten Java Applikationen gemäß dem GlobalPlatform Standard selektiert und ausgefuehrt werden können. Ein Großteil der Programmierarbeiten erfolgt dabei in C++. In einem Abschlussprojekt werden einige sicherheitsrelevante Anwendungen - inklusive einer Blockchiffre - für die Java Card implementiert.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: keine

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 6 Termine zu je 3 Stunden entsprechen 18 Stunden Anwesenheit. Für die Vorbereitung werden 18 Stunden (3 Stunden je Termin für 6 Termine), für die Bearbeitung der Übungszettel 9 Stunden (3 Stunden je Übungszettel für drei Übungszettel), für die Implementierung der Chiffre in Gruppenarbeit 40 Stunden und für die Vorbereitung auf das Prüfungsgespräch 5 Stunden veranschlagt.

exam: Praktikum, studienbegleitend

2.32 142246: Master-Praktikum Programmanalyse

Nummer:	142246
Lehrform:	Praktikum
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozenten:	Prof. Dr. Thorsten Holz M. Sc. Andre Pawlowski
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Wintersemester

Termine im Wintersemester:

Vorbesprechung: Mittwoch den 09.10.2019 ab 12:00 bis 13:00 Uhr

Ziele: Die Studierenden haben ein tiefergehendes Verständnis der Funktionsweise aktueller Schadsoftware und kennen Techniken zur Analyse und zur Abwehr. Im Besonderen beherrschen die Teilnehmer entsprechende Techniken des Reverse-Engineerings unter Windows.

Inhalt: Das Praktikum ist eine Vertiefung der Inhalte, die in den Vorlesungen "Programmanalyse" und "Betriebssystemsicherheit" vorgestellt wurden. Die Teilnehmer sollen in Gruppen insgesamt sieben unterschiedliche Beispiele von realer Schadsoftware mit steigendem Schwierigkeitsgrad analysieren. Die zu analysierenden Schadsoftwarebeispiele werden jeweils zu einem eigenen Präsenztermin besprochen und entsprechende Analysemethoden vorgestellt. In vielen Fällen wird darüber hinaus Eigenrecherche und Autodidaktik zur Lösung der Aufgaben notwendig sein. Unter anderem werden die folgenden Themen behandelt:

- Entpacken/Entschleiern von Schadsoftware
- Statische und dynamische Analyse von Schadsoftware
- Entwicklung von Analyse-Tools
- Entwicklung von Kontrollstrukturen (C&C) für existierende Schadsoftware

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse im Bereich des Reverse-Engineerings sind wünschenswert, z.B. durch erfolgreichen Abschluss der Vorlesung "Programmanalyse" und Erfahrung mit x86-Assembler. Erfahrung in systemnaher Programmierung unter Windows (Assembler, C) ist hilfreich.

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Anwesenheit beträgt 3 SWS * 14 Wochen, also 42 Stunden. Zum Schreiben des geforderten Quelltextes werden weitere ca. 48 Stunden benötigt.

exam: Praktikum, studienbegleitend

2.33 142030: Master-Praktikum Reverse Engineering - The Key to Hacking Real-World Devices

number:	142030
teaching methods:	practical course
media:	Moodle
	rechnerbasierte Präsentation
responsible person:	Prof. Dr.-Ing. Christof Paar
Lecturers:	Prof. Dr.-Ing. Christof Paar
	M. Sc. Nils Albartus
	M. Sc. Steffen Becker
language:	english
HWS:	3
Leistungspunkte:	3
angeboten im:	winter term

dates in winter term:

Vorbesprechung: Freitag the 12.10.2018 from 10:00 in ID 04/413
Beginn: Freitag the 23.11.2018
Praktikum Freitags: from 10:00 to 12:00 o'clock in ID 04/413

goals: Den Studierenden bietet sich im Rahmen dieses innovativen Praktikums die einmalige Gelegenheit Wissen über Hardware Reverse Engineering aufzubauen und dieses praktisch anhand von Übungsaufgaben anzuwenden.

Dieses Praktikum vermittelt den Studierenden ein tiefgehendes Verständnis verschiedener Gate-level Netlist Reverse Engineering Methoden und bereitet sie ideal auf Abschlussarbeiten in diesem Bereich vor.

content: 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.

Schon heute sind schätzungsweise 20 Milliarden Geräte online - und dieses Internet der Dinge (IoT) wird mit Applikationen wie dem vernetzten Auto oder Smart Homes weiter rapide wachsen. Mit der fortschreitenden Vernetzung steigt aber auch der Bedarf an erfahrenen Reverse Engineers - sowohl in der Industrie, in der Wissenschaft als auch bei den Geheimdiensten.

Im Rahmen dieser Veranstaltung bearbeiten die Studierenden vier Projekte mithilfe mit dem Gate-level Netlist Reverse Engineering Framework HAL.

requirements: keine

recommended knowledge: Inhalte der Vorlesungen “Rechnerarchitektur” und “Einführung ins Hardware Reverse Engineering”.

Arbeitsaufwand: 90 Stunden

Für die Einarbeitung mit Betreuer werden 15 h angesetzt. Für die Bearbeitung des Projekts 50 h. Für die anschließende Ausarbeitung werden 25h angesetzt.

exam: Praktikum, continual assessment

2.34 150584: Master-Praktikum SAGE in der Kryptographie

Nummer: 150584
Lehrform: Praktikum
Verantwortlicher: Prof. Dr. Gregor Leander
Dozent: Prof. Dr. Gregor Leander
Sprache: Deutsch
SWS: 2
Leistungspunkte: 3
angeboten im: Wintersemester

Ziele: Die Studierenden lernen das open source Computeralgebrasystem "SAGE" kennen. Anhand von mehreren kleineren Projekten werden kryptographisch relevante Aufgaben gelöst.

Inhalt: Die Software "SAGE" bietet ein mächtiges Werkzeug um relativ einfach und schnell viele Probleme in der Kryptographie praktisch umzusetzen. Wir beschäftigen uns beispielhaft unter Anderem mit Algorithmen zum Faktoiriziden, dem Berechnen von diskreten Logarithmen und dem Lösen von Gleichungssystemen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse über Kryptographie, wie sie zum Beispiel in der "Einführung in die Kryptographie I und II" behandelt werden, sind hilfreich, aber nicht nötig.

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 12 Wochen zu je 3h entsprechen 36 Stunden Anwesenheit. Für die Vorbereitung und Ausarbeitung der Protokolle werden jeweils 4,5 Stunden, insgesamt 54 Stunden veranschlagt.

exam: Praktikum, studienbegleitend

2.35 142249: Master-Praktikum Schwachstellenanalyse

Nummer:	142249
Lehrform:	Praktikum
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozenten:	Prof. Dr. Thorsten Holz
	M. Sc. Moritz Contag
	M. Sc. Andre Pawlowski
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Sommersemester

Termine im Sommersemester:

Vorbesprechung: Mittwoch den 03.04.2019 ab 12:15 bis 13:00 Uhr im ID 03/419

Ziele: Die Studierenden haben ein tiefergehendes Verständnis der Funktionsweise aktueller Angriffsmethoden und Schutzmechanismen. Sie kennen verschiedene Techniken aus diesen beiden Bereichen und können diese umsetzen. Im Besonderen beherrschen die Teilnehmer entsprechende Techniken des Reverse-Engineerings und der Entwicklung von Exploits.

Inhalt: Das Praktikum ist eine Vertiefung der Inhalte, die in den Vorlesungen "Programmanalyse" und "Betriebssystemsicherheit" vorgestellt wurden. Im Rahmen des Praktikums werden verschiedene Arten von Schwachstellen vorgestellt und anhand realer Beispiele implementiert. Die zu analysierenden Schwachstellentypen werden jeweils zu einem eigenen Präsenztermin besprochen und entsprechende Analyse- und Exploitingmethoden vorgestellt. In vielen Fällen wird darüber hinaus Eigenrecherche und Autodidaktik zur Lösung der Aufgaben notwendig sein. Unter anderem werden die folgenden Themen behandelt:

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

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse im Bereich des Reverse-Engineerings sind wünschenswert, z.B. durch erfolgreichen Abschluss der Vorlesung "Programmanalyse" und Erfahrung mit x86-Assembler. Erfahrung in systemnaher Programmierung unter Windows (Assembler, C) ist hilfreich.

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Anwesenheit beträgt 3 SWS * 14 Wochen, also 42 Stunden. Zum Schreiben des geforderten Quelltextes werden weitere ca. 48 Stunden benötigt.

exam: Praktikum, studienbegleitend

2.36 142248: Master-Praktikum Security Appliances

Nummer:	142248
Lehrform:	Praktikum
Medienform:	e-learning Handouts rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk M. Sc. Dennis Felsch Dr.-Ing. Christian Mainka M. Sc. Paul Rösler
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	

Termine im Sommersemester:

Beginn: Montag den 09.04.2018
Praktikum Montags: ab 14:00 bis 16:00 Uhr im ID 04/445

Ziele: Die Studierenden haben einen umfassenden Einblick in die Welt der bargeldlosen Zahlung und Zahlungsabwicklung. Sie haben ein Verständnis für die verwendeten Datenformate, Prozesse und die notwendige Infrastruktur entwickelt und den Umgang, die Programmierung und den Betrieb von Hardware-Sicherheitsmodulen (HSM)erlernt. Sie bescherrschen die Einbindung und Verwendung einer HSM in Java unter Verwendung der Java Cryptographic Extension (JCE) sowie die Programmierung einer Firewall-Anwendung für Service-orientierte Architekturen (SOA).

Inhalt: Egal ob die neue App für das Handy, der schnelle Einkauf im Netz oder das Abendessen im Restaurant - täglich nutzen wir die Bequemlichkeit bargeldloser Zahlungssysteme ohne auch nur einen Gedanken an die notwendige Infrastruktur, die Prozesse und vor allem die Sicherheit hinter der Fassade zu verlieren.

Dieses Praktikum bietet eine Einführung in die Infrastruktur hinter bargeldlosem Zahlungsverkehr am Beispiel von Kreditkarten-basierter Zahlung. Inhalte sind die notwendigen Prozesse, Datenformate und deren Sicherheit.

Während des Praktikums werden notwendige Prozesse zur Abwicklung einer Zahlung nachimplementiert und in einer simulierten Point-of-Sales-Umgebung getestet. Hierbei steht besonders die notwendige Hardware zur sicheren Zahlungsabwicklung im Vordergrund. Die erarbeiteten Softwarekomponenten werden mit echten und simulierten Hardware-Sicherheitsmodulen (HSMs) interagieren.

Die Teilnehmer erwartet eine Schulung im Umgang mit HSMs direkt durch den Hersteller Utimaco. Des Weiteren wird auch ein tiefer Einblick in die Arbeitsweise von XML-Firewall-Hardware am Beispiel einer IBM DataPower-Appliance vermittelt.

Das Praktikum wird mit Unterstützung der Utimaco GmbH durchgeführt.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Programmierkenntnisse in C und Java

Studenten die bereits die Bachelorversion dieses Praktikums bestanden haben, dürfen leider nicht teilnehmen.

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 12 Wochen zu je 3h entsprechen 36 Stunden Anwesenheit. Für die Vorbereitung und Ausarbeitung der Protokolle werden jeweils 4,5 Stunden, insgesamt 54 Stunden veranschlagt.

exam: Praktikum, studienbegleitend

2.37 142023: Master-Praktikum Seitenkanalangriffe

Nummer:	142023
Lehrform:	Praktikum
Verantwortlicher:	Priv.-Doz. Dr. Amir Moradi
Dozenten:	Priv.-Doz. Dr. Amir Moradi M. Sc. Bastian Richter
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Wintersemester

Termine im Wintersemester:

Vorbesprechung: Mittwoch den 09.10.2019 ab 16:00 im ID 2/632

Ziele: Das Master-Praktikum Seitenkanalangriffe vermittelt die nötigen praktischen Fähigkeiten kryptographische Implementierungen auf ihre Seitenkanalsicherheit hin zu untersuchen und entsprechende Gegenmaßnahmen zu implementieren. Das Praktikum wurde vollständig überarbeitet und wird ab dem Wintersemester 18/19 auf einer aktuellen ARM M0-Platform durchgeführt. Die Studenten müssen selbständig Messungen durchführen und Gegenmaßnahmen auf dem Mikrocontroller implementieren.

Inhalt:

1. Einführung & Statistik
2. Pattern Matching & SPA
3. Messungen & CPA auf Software
4. Leakage Detection & CPA auf Hardware
5. CPA mit Alignment
6. Boolean Masking der AES S-Box
7. Abschlussprojekt

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Die Vorlesung "Implementierung kryptografischer Verfahren I" vermittelt nützliches Vorwissen, dieses wird jedoch nicht vorrausgesetzt.

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 6 Termine zu je 3 Stunden entsprechen 18 Stunden Anwesenheit. Für die Vorbereitung werden 18 Stunden (3 Stunden je Termin für 6 Termine), für die Bearbeitung der Übungszettel 9 Stunden (3 Stunden je Übungszettel für drei Übungszettel), für die Implementierung der Chiffre in Gruppenarbeit 40 Stunden und für die Vorbereitung auf das Prüfungsgespräch 5 Stunden veranschlagt.

exam: Praktikum, studienbegleitend

2.38 150562: Master-Praktikum Smart Contracts

Nummer:	150562
Lehrform:	Praktikum
Medienform:	Moodle rechnerbasierte Präsentation
Verantwortlicher:	Jun. Prof. Dr. Sebastian Faust
Dozent:	Jun. Prof. Dr. Sebastian Faust
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Sommersemester

Ziele: Die Studierenden erarbeiten den praktischen Umgang mit kryptographischen Währungen. Die Teilnehmer des Praktikums lernen die Funktionsweise der kryptographischen Währungen Bitcoin und Ethereum kennen und lernen wie man sicher mit diesen Währungen bezahlt. Dazu gehört neben dem Senden und Empfangen von Transaktionen vor allem die Programmierung von Smart Contracts.

Inhalt: Im Rahmen dieses Praktikums sollen die kryptographischen Währungen Bitcoin und Ethereum vorgestellt werden. Dabei werden zunächst die Grundlagen von Blockchain Technologie vermittelt um die zugrundeliegenden kryptographischen Bausteine zu verstehen. Darauf aufbauend sollen die Studierenden sich mit der Funktionsweise der dezentralen Netzwerke und des Minings vertraut machen. Anschließend wird die Programmierung von Smart Contracts und deren Integration in bestehende Software ausführlich betrachtet. Auch die Sicherheit von Smart Contract Programmierung soll dabei genauer untersucht werden. Die Programmierung dieser Contracts in Ethereum wird mit der Programmiersprache Solidity erfolgen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse im Bereich Blockchain Technologien wie z.B. aus der Vorlesung Financial Cryptography/Cryptocurrencies sind wünschenswert, aber nicht erforderlich. Erfahrungen in Programmierung mit JavaScript sind hilfreich.

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 6 Termine zu je 3 Stunden entsprechen 18 Stunden Anwesenheit. Für die Vorbereitung werden 18 Stunden (3 Stunden je Termin für 6 Termine), für die Bearbeitung der Übungszettel 9 Stunden (3 Stunden je Übungszettel für drei Übungszettel), und für die Implementierungsaufgaben 45 Stunden veranschlagt.

exam: Praktikum, studienbegleitend

2.39 142250: Master-Praktikum TLS Implementierung

Nummer:	142250
Lehrform:	Praktikum
Medienform:	Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Dr.-Ing. Juraj Somorovsky M. Sc. Robert Merget
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Wintersemester

Termine im Wintersemester:

Vorbesprechung: Dienstag den 15.10.2019 ab 12:00 im ID 04/653
Praktikum Dienstags: ab 12:00 bis 14:00 Uhr im ID 04/653

Ziele: Die Studierenden lernen ein modernes kryptographisches Protokoll detailliert kennen. Die Studierenden arbeiten mit Konzepten der modernen Softwareentwicklung. Ein Ausblick auf aktuelle Forschung in diesem Bereich wird gegeben.

Inhalt: Das TLS-Protokoll ist das wichtigste kryptographische Protokoll im Internet und wird beim Schutz von jeder wichtigen Webseite oder Webservices eingesetzt. In den letzten Jahren wurden viele Angriffe auf dieses Protokoll bekannt, wie z.B. POODLE, DROWN, Lucky 13 oder ROBOT. Deswegen wurde in den letzten Jahren in Zusammenarbeit von Industrie und Wissenschaft eine neue TLS Version entwickelt: TLS 1.3. Die neue Version sollte gegen alle bekannten Angriffe schützen und gleichzeitig die Performance von TLS erhöhen. TLS 1.3 verwendet nur die neuesten kryptographischen Mechanismen, so dass das Protokoll-Design für jeden Krypto-Entwickler und Designer von großem Interesse ist.

Im Rahmen des Praktikums implementieren die Studenten einen TLS 1.3 Server. Dabei wird diese Aufgabe in mehrere Teilaufgaben zerlegt und das Thema schrittweise an die Studenten herangeführt. Es werden weiterhin folgende Themen besprochen:

- Einführung in TLS, JUnit Tests und Git
- TLS 1.3
- Kryptographie mit Java
- Clean Code
- TLS-Attacker
- TLS Fuzzing

Empfohlene Vorkenntnisse:

- Erfolgreicher Abschluss der Lehrveranstaltung Netzsicherheit 2
- Programmierkenntnisse in Java

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 6 Termine zu je 3 Stunden entsprechen 18 Stunden Anwesenheit. Für die Vorbereitung werden 18 Stunden (3 Stunden je Termin für 6 Termine), für die Bearbeitung der Übungszettel 9 Stunden (3 Stunden je Übungszettel für drei Übungszettel), und für die Implementierungsaufgaben 45 Stunden veranschlagt.

exam: Praktikum, studienbegleitend

2.40 142026: Master-Praktikum Wireless Physical Layer Security

Nummer:	142026
Lehrform:	Praktikum
Medienform:	Folien rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Christof Paar
Dozenten:	Prof. Dr.-Ing. Christof Paar Dr.-Ing. Christian Zenger
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Wintersemester und Sommersemester

Termine im Wintersemester:

Vorbesprechung: Mittwoch den 09.10.2019 ab 16:00 im ID 04/445
Praktikum Mittwochs: ab 16:00 bis 18:00 Uhr im ID 04/445

Termine im Sommersemester:

Beginn: Mittwoch den 10.04.2019 ab 16:15 im ID 04/445
Praktikum Mittwochs: ab 16:00 bis 18:00 Uhr im ID 04/445

Ziele: Dieses Praktikum verfolgt im Wesentlichen die folgenden drei Lernziele: Erstens kennen die Teilnehmer des Praktikums eine Software Defined Radio (SDR) Architektur und deren Programmierung mit ‚GNU Radio'. Zweitens wird der Umgang mit SDRs, sowie Wissen über die entsprechenden Funkstandards und potenzielle Angriffe beherrscht. Drittens sind die Implementierungs- und Evaluierungsaspekte von modernen Funkkanal-basierten Sicherheitsarchitekturen bekannt. Python wird als Programmiersprachen verwendet. Über die technischen Ziele hinaus wird die Arbeitsfähigkeit in Gruppen erlernt, sowie Projektplanung und Zeitmanagement vermittelt.

Inhalt: In diesem Praktikum werden zwei Themengebiete erarbeitet. Zunächst erlernen die Teilnehmer des Praktikums Grundlagen über Software Defined Radios (SDRs). Bereits nach dem ersten Praktikumstermin sind die Studenten in der Lage passive Lauschangriffe mit GNU Radio für die RTL-SDR Architektur zu entwickeln. Während der folgenden Termine werden die Kenntnisse bezüglich der SDR Architektur und Funkstandards vertieft. Darüber hinaus müssen die Praktikumsteilnehmer immer komplexere Programme als Hausaufgaben schreiben. Im zweiten Teil des Praktikums erlernen die Studenten den Umgang mit Funkkanal-basierten Sicherheitsarchitekturen. Der Kanal-basierte Schlüsselgenerierung und Kanal-basiertes Fingerprinting werden vorgestellt. Die Studenten werden anschließend in Grup-

pen à drei Personen aufgeteilt. Jede Gruppe erhält ein Messsetup basierend aus drei Raspberry Pis, Funkmodulen und einer Messsoftware, sowie eine Virtuelle Maschine mit vorkonfiguriertem Evaluationsframework. Jede Gruppe implementiert eine vorgegebene Kanal-basierte Sicherheitsarchitektur (jährliche eine andere) in Python, und muss diese im Evaluationsframework unter realistischen Bedingungen lauffähig bekommen. Um die Motivation der Praktikumsteilnehmer zu erhöhen, werden die effizientesten Implementierungen mit Buchpreisen belohnt.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse Kryptographie, z.B. aus dem Modul Einführung in die Kryptographie und Datensicherheit

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 6 Termine zu je 3 Stunden entsprechen 18 Stunden Anwesenheit. Für die Vorbereitung werden 18 Stunden (3 Stunden je Termin für 6 Termine), für die Bearbeitung der Übungszettel 9 Stunden (3 Stunden je Übungszettel für drei Übungszettel), und für die Implementierungsaufgaben 45 Stunden veranschlagt.

exam: Praktikum, studienbegleitend

2.41 142243: Master-Praktikum zur Hackertechnik

Nummer:	142243
Lehrform:	Praktikum
Medienform:	Folien
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk
	Dr.-Ing. Marcus Niemietz
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Wintersemester und Sommersemester

Termine im Wintersemester:

Beginn: Mittwoch den 09.10.2019 ab 16:15 im ID 03/445
Praktikum Mittwochs: ab 16:15 bis 17:45 Uhr im ID 2/168

Termine im Sommersemester:

Vorbesprechung: Montag den 01.04.2019 ab 14:00 im ID 04/413
Praktikum Mittwochs: ab 16:15 bis 17:45 Uhr im ID 03/445

Ziele: Die teilnehmenden Studierenden haben ein weit gefächertes Wissen über die häufigsten Schwachstellen in Webapplikationen. Außerdem wissen sie, wie sie derartige Schwachstellen manuell finden können, ohne die Hilfe von automatisierten Webapplikations-Scannern in Anspruch zu nehmen. Darüber hinaus kennen die Studierenden entsprechende Schutzmaßnahmen sowie deren Wirksamkeit.

Inhalt: Webapplikationen sind im Zeitalter des Web-2.0 immer mehr zum Ziel von Angreifern geworden. So werden per SQL-Injektion fremde Datenbanken kompromittiert, per XSS-Schwachstelle Browsersessions gestohlen und per Cross-Site-Request-Forgery bekommt man von heute auf morgen unzählige neue Freunde in einem sozialen Netzwerk. Dazu wird nur ein einfacher Webbrowser benötigt.

Im Laufe dieses Praktikums sollen die Studierenden eine fiktive Online-Banking-Applikation angreifen und dabei die im Laufe der Veranstaltung erlernten Methoden und Techniken einsetzen. Dieses beinhaltet folgende Themengebiete:

- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Session Hijacking

- Session Fixation
- SQL Injection (SQLi)
- Local/Remote File Inclusion (LFI/RFI)
- Path Traversal
- Remote Code Execution (RCE)
- Logical Flaws
- Information Leakage
- Insufficient Authorization

Das Wissen der Studierenden wird zudem durch externe Experten aus der Industrie und IT-Sicherheits-Szene, die in Vorträgen über verschiedene Thematiken der Webapplikations-Sicherheit referieren werden, angereichert.

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Ausgeprägtes Interesse an IT-Sicherheit, speziell am Thema "Websicherheit"
- Grundlegende Kenntnisse über TCP/IP und HTTP(S)
- Grundlegende Kenntnisse über HTML / JavaScript
- Grundkenntnisse in PHP oder einer ähnlichen Scriptsprache
- Inhalte der Vorlesungen Netzsicherheit 1 und 2

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 12 Wochen zu je 3h entsprechen 36 Stunden Anwesenheit. Für die Vorbereitung und Ausarbeitung der Protokolle werden jeweils 4,5 Stunden, insgesamt 54 Stunden veranschlagt.

exam: Praktikum, studienbegleitend

2.42 142040: Master-Projekt DSP

Nummer:	142040
Lehrform:	Projekt
Medienform:	Folien
Verantwortlicher:	Prof. Dr.-Ing. Dorothea Kolossa
Dozenten:	Prof. Dr.-Ing. Dorothea Kolossa
	Dr.-Ing. Steffen Zeiler
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Sommersemester

Termine im Sommersemester:

Vorbesprechung: Freitag den 05.04.2019 ab 10:00 im ID 2/232

Ziele: Neben den Strategien und Methoden zur Bewältigung der technischen Herausforderungen beherrschen die Studierenden gleichzeitig die Organisation von größeren Projekten in Teams, Methoden der Projektplanung, strukturierte Softwareentwicklung incl. Spezifikation und Validierung.

Inhalt: In dieser Veranstaltung implementieren Master-Studierende in Teams von bis zu 10 Mitgliedern über den Verlauf eines Semesters hinweg ein größeres Projekt ihrer Wahl echtzeitfähig auf einer DSP-Plattform.

Semesterziel ist jeweils die vollständige Realisierung eines selbstgewählten Projekts aus der digitalen Signalverarbeitung, der automatischen Spracherkennung oder dem Bereich der kognitiven Modelle. Beispielhafte Themen, die sich realistisch in einem Semester umsetzen lassen, sind: Realisierung eines DAB-Radioempfängers, einer Sprachsteuerung für die Hausautomatisierung, oder einer automatischen Gesichtserkennung in Kamerabildern.

Es besteht Anwesenheitspflicht zu den Laborterminen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Grundkenntnisse der digitalen Signalverarbeitung
- sichere Beherrschung mindestens einer Programmiersprache
- idealerweise Erfahrungen mit der Programmierung in C

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 3 SWS ergeben 42 Stunden Anwesenheit. Es verbleiben 48 Stunden zur Vor- und Nachbereitung.

exam: Projektarbeit, studienbegleitend

2.43 142024: Master-Projekt Eingebettete Sicherheit

Nummer: 142024
Lehrform: Projekt
Verantwortlicher: Prof. Dr.-Ing. Christof Paar
Dozent: Prof. Dr.-Ing. Christof Paar
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
angeboten im: Wintersemester und Sommersemester

Termine im Wintersemester:

Vorbesprechung: nach Absprache

Termine im Sommersemester:

Vorbesprechung: nach Absprache

Ziele: Die Studierenden beherrschen verschiedene Techniken, die für die Forschung im Bereich der modernen eingebetten Sicherheit relevant sind.

Inhalt: Es wird eine Projektaufgabe unter Anleitung bearbeitet. Themen sind hierbei Fragestellungen bezüglich Implementierungstechniken, physikalischer Angriffe oder Sicherheits-Design.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse der angewandten Kryptographie, sowie Grundkenntniss der Software- oder Hardware-Implementierung

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berecnet sich wie folgt: 14 Wochen zu je 3 SWS ergeben 42 Stunden Anwesenheit. Es verbleiben 48 Stunden zur Vor- und Nachbereitung.

exam: Projektarbeit, studienbegleitend

2.44 142241: Master-Projekt Netz- und Datensicherheit

Nummer:	142241
Lehrform:	Projekt
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk M. Sc. Robert Merget
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Wintersemester und Sommersemester

Termine im Wintersemester:

Vorbesprechung: nach Absprache

Termine im Sommersemester:

Vorbesprechung: nach Absprache

Ziele: Die Studierenden analysieren die Sicherheit ausgewählter Protokolle und Implementierungen (z.B. TLS, IPsec, JSON Web Crypto), oder implementieren selber Tools für spezifische Sicherheitsanalysen (z.B. Plugins für Burp Suite).

Inhalt: Das Praktikum ist ein nicht angeleitetes Fortgeschrittenenpraktikum. Es umfasst nur ein Thema, das die Studierenden selbständig bearbeiten. Je nach Thema wird Ihnen der entsprechende Betreuer zugeordnet.

Zur Klarstellung: Es ist nicht vorgesehen, dass sie verschiedene Themenblöcke nacheinander abarbeiten (wie es bei den Grundlagenpraktika der Fall ist), sondern sie werden nur ein Thema im Praktikum vertiefen. Die Bearbeitung kann je nach Vereinbarung mit dem Betreuer semesterbegleitend (z.B. 3h die Woche), oder zusammengefasst als Block (insgesamt ca. 40h) erfolgen; je nach Verfügbarkeit des Betreuers ist auch eine Bearbeitung in den Semesterferien grundsätzlich möglich.

Die Themenliste stellt nur Themenstichworte dar; die detaillierte Besprechung, und endgültige Definition des Themas erfolgt zusammen mit dem jeweiligen Fachbetreuer.

Es wird eine Projektaufgabe unter Anleitung bearbeitet. Themen sind hierbei Fragestellungen der Netz- und Datensicherheit. Beispiele sind die Software-Implementierung XML-basierter Protokolle oder TLS.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundlagen der Kryptographie, Datensicherheit und Netzsicherheit, Programmierkenntnisse (nachweisbar z.B. durch eine erfolgreiche Teilnahme am Praktikum Security Appliances)

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Anwesenheit beträgt 3 SWS * 14 Wochen, also 42 Stunden. Zum Schreiben des geforderten Quelltextes werden weitere ca. 48 Stunden benötigt.

exam: Projektarbeit, studienbegleitend

2.45 142184: Master Project Virtual Prototyping of Embedded Systems

number: 142184
teaching methods: project
responsible person: Prof. Dr.-Ing. Michael Hübner
Lecturers: Prof. Dr.-Ing. Michael Hübner
M. Sc. Florian Fricke
M. Sc. Tomás Grimm
Prof. Dr.-Ing. Michael Hübner
language: english
HWS: 3
Leistungspunkte: 3
angeboten im:

dates in winter term:

Vorbesprechung: Mittwoch the 11.10.2017 from 16:15 in ID 1/103
Praktikum Montags: from 09:00 to 12:00 o'clock in ID 1/103

goals: The students master the design of "Embedded Systems" with the help of "Virtual Prototyping". Besides using tools for modeling, simulation and analysis of a virtual "Embedded System", the students will also be able to use SystemC, a hardware description language based on C++, and to model selected peripheral components. Furthermore they can implement applications in connection with the designed processor platform and a real-time operating system.

content: Within the project's scope, the methods of "Virtual Prototyping" are taught and reinforced with practical examples. The course's agenda is described below:

1. Introduction to Virtual Prototyping basic concepts, systems, tools, languages, etc.

2. SystemC basic course

This course is based on the IEEE SystemC TLM2.0 library, and aims to provide the basic understanding about the SystemC language and the Transaction-Level Modeling (TLM) standard.:

- Introduction to Transaction-Level Modeling
- Working with Loosely-Timed models
- Working with Approximately-Timed models
- Debugging methods

3. Tensilica Processor design framework

The objective is to provide hands-on knowledge about the Cadence Xtensa Xplorer framework to design custom processor architectures based on the Xtensa LX series processors:

- Tensilica Processor Architecture
- Programming Cores with Tensilica Instruction Extensions
- Developing Software for Xtensa Processors
- Xtensa Debug and Trace
- Support for Emulation

4. Virtual System Platform

This course uses the Cadence Virtual System Platform to integrate hardware and software platforms using fast processor models. The simulation platforms are based on SystemC/TLM2.0 models and allows for fast hardware emulation and early software development.

- Tool overview
- Selected examples
- Custom models design and analysis
- Fast processor models integration
- System-on-Chip ESL design

requirements: none

recommended knowledge: Basic programming knowledge in C/C++

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Das Praktikum findet als Blockveranstaltung statt mit 4 1/2 Tagen Dauer, entsprechend 36 Stunden Anwesenheit. Für die Vorbereitung werden 18 Stunden (9 Stunden je Abschnitt), für die Ausarbeitung des Praktikumsberichts 36 Stunden (18 Stunden je Abschnitt) veranschlagt.

exam: Projektarbeit, continual assessment

2.46 143242: Master-Seminar Aktuelle Themen der IT-Sicherheit

Nummer:	143242
Lehrform:	Seminar
Medienform:	Folien
	Handouts
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozent:	Prof. Dr. Thorsten Holz
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Wintersemester und Sommersemester

Termine im Wintersemester:

Vorbesprechung: Mittwoch den 09.10.2019 ab 10:15 bis 11:45 Uhr

Termine im Sommersemester:

Vorbesprechung: Mittwoch den 03.04.2019 ab 10:15 bis 11:45 Uhr im ID 03/471

Ziele: Die Studierenden haben Methoden des forschungsnahen Lernens kennen gelernt und sind in der Lage eigenständig ein eng umgrenztes Themengebiet anhand von wissenschaftlichen Papern zu erarbeiten. Durch die Ausarbeitung haben die Studierenden das Schreiben eigener Texte und die Zusammenfassung komplexer Themengebiete geübt. Darüber hinaus können die Studierenden einen Vortrag zur Präsentation von wissenschaftlichen Ergebnissen mit Bezug zu der aktuellen Forschung halten.

Inhalt: In jedem Semester bietet der Lehrstuhl ein Seminar zum Thema "Aktuelle Themen der IT-Sicherheit" an, der Fokus liegt auf den Bereichen Malware-Analyse, Systemsicherheit, Sicherheit im Internet und ähnlichen Themen aus dem Bereich der systemnahen IT-Sicherheit. Dazu sollen die Studierenden selbständig ein komplexes Themengebiet bearbeiten und eine Ausarbeitung sowie einen Vortrag zu diesem Thema verfassen. Die Ausarbeitung hat einen Umfang von etwa 20-25 Seiten und der Vortrag soll etwa 20 Minuten dauern. Daran schließt sich eine Diskussion von 5 Minuten an.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Vorkenntnisse über Systemsicherheit und Netzsicherheit z.B. aus den Vorlesungen Systemsicherheit 1/2 und Netzsicherheit 1/2

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Seminarvorträge finden als Blockveranstaltung statt. Es besteht Anwesenheitspflicht. Dafür sind durchschnittlich (je nach Teilnehmerzahl) 20 Stunden anzusetzen. Die Erarbeitung des Seminarthemas findet eigenverantwortlich mit Unterstützung der betreuenden Mitarbeiter statt. Eine schriftliche Ausarbeitung von ca. 20 Seiten ist zu erstellen. Die Themen sind so gewählt, dass hierfür eine Arbeitszeit von 70 Stunden anzusetzen ist.

exam: Seminarbeitrag, studienbegleitend

2.47 143245: Master-Seminar Digitale Signaturen

Nummer: 143245
Lehrform: Seminar
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr. Jörg Schwenk
Dozent: M. Sc. Sebastian Lauer
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
angeboten im: Wintersemester

Ziele: Die Teilnehmer können mit technischer und wissenschaftlicher Literatur für Forschung und Entwicklung umgehen und die Ergebnisse wissenschaftlich präsentieren.

Inhalt: Im Rahmen dieses Seminars wird ein solides Grundverständnis für die Konstruktion von sicheren digitalen Signaturverfahren vermittelt. Folgende Themen werden behandelt und vertieft:

- Einmalsignaturverfahren
- Chamäleon-Hashfunktionen
- RSA-basierte Signaturverfahren
- Pairing-basierte Signaturverfahren
- Blind-Signatures
- Verifiable Random Functions
- Group-Signatures
- Identity-based Signatures

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Grundlegende Kenntnisse der Kryptographie
- Vorlesung “Kryptographie” von Prof. Dr. Alexander May

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Seminarvorträge finden als Blockveranstaltung statt. Es besteht Anwesenheitspflicht. Dafür sind durchschnittlich (je nach Teilnehmerzahl) 20 Stunden anzusetzen. Die Erarbeitung des Seminarthemas findet eigenverantwortlich mit Unterstützung der betreuenden Mitarbeiter statt. Eine schriftliche Ausarbeitung von ca. 20 Seiten ist zu erstellen. Die Themen sind so gewählt, dass hierfür eine Arbeitszeit von 70 Stunden anzusetzen ist.

exam: Seminarbeitrag, studienbegleitend

2.48 143021: Master Seminar Embedded Security

number: 143021
teaching methods: seminar
media: rechnerbasierte Präsentation
responsible person: Priv.-Doz. Dr. Amir Moradi
Lecturers: Priv.-Doz. Dr. Amir Moradi
M. Sc. Anita Aghaie
language: english
HWS: 3
Leistungspunkte: 3
angeboten im: winter term and summer term

dates in winter term:

Vorbesprechung: Dienstag the 09.10.2018 from 14:00 in ID 03/445

dates in summer term:

Vorbesprechung: Mittwoch the 03.04.2019 from 14:00 in ID 03/419

goals: Die Teilnehmer bescherrschen den akademischen Umgang mit technischer und wissenschaftlicher Literatur. Sie kennen Stand der Forschung.

content: Fortgeschrittene Themen der IT-Sicherheit werden von den Studierenden eigenständig erarbeitet. Das Spektrum möglicher Themen reicht von der Sicherheitsanalyse eingebetteter Systeme, über kryptografische Algorithmen für leistungsbeschränkte Geräte bis hin zu verschiedenen Aspekten der mobilen Sicherheit. Im Gegensatz zu dem Seminar im Bachelorstudiengang werden hier in der Regel Themen mit Bezug zu der aktuellen Forschung aufgegriffen.

requirements: keine

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Seminarvorträge finden als Blockveranstaltung statt. Es besteht Anwesenheitspflicht. Dafür sind durchschnittlich (je nach Teilnehmerzahl) 20 Stunden anzusetzen. Die Erarbeitung des Seminarthemas findet eigenverantwortlich mit Unterstützung der betreuenden Mitarbeiter statt. Eine schriftliche Ausarbeitung von ca. 20 Seiten ist zu erstellen. Die Themen sind so gewählt, dass hierfür eine Arbeitszeit von 70 Stunden anzusetzen ist. Eine Klausurvorbereitung entfällt, da der Vortrag und die Ausarbeitung beurteilt werden.

exam: Seminarbeitrag, continual assessment

2.49 143248: Master-Seminar Human Centered Security and Privacy

Nummer:	143248
Lehrform:	Seminar
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Markus Dürmuth
Dozenten:	Prof. Dr. Markus Dürmuth
	M. Sc. Philipp Markert
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Wintersemester und Sommersemester

Termine im Wintersemester:

Vorbesprechung: Freitag den 11.10.2019 ab 12:15 im ID 03/445

Termine im Sommersemester:

Vorbesprechung: Dienstag den 16.04.2019 ab 09:00 bis 10:00 Uhr im ID 04/401

Ziele: Die Studierenden haben einen Einblick in aktuelle Forschungsthemen und können eigenständig Fachliteratur zu einem bestimmten Themengebiet verstehen. Sie sind in der Lage eigene Texte und die Zusammenfassung komplexer Themengebiete zu verfassen. Darüber hinaus können sie einen Vortrag zur Präsentation von wissenschaftlichen Ergebnissen halten.

Inhalt: Es wird eine Auswahl an aktuellen Forschungsarbeiten im Bereich der nutzerorientierten Sicherheit und Privatheit bereitgestellt. Thematische Schwerpunkte sind u.a. die Sicherheit von Authentifizierungsverfahren und Digitales Vergessen, die jeweils sowohl von technischer Seite als auch aus Anwendersicht beleuchtet werden. Dazu sollen die Studierenden anhand von Forschungsarbeiten selbständig ein Themengebiet erarbeiten und eine Zusammenfassung erstellen. Im Anschluss wird jeder Student drei andere Zusammenfassung begutachten und zu jeder ein Review verfassen. Zum Abschluss des Seminars hält jeder Student einen Vortrag über seine Zusammenfassung.

Voraussetzungen: Keine

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Seminarvorträge finden als Blockveranstaltung statt. Es besteht Anwesenheitspflicht. Dafür sind

durchschnittlich (je nach Teilnehmerzahl) 20 Stunden anzusetzen. Die Erarbeitung des Seminarthemas findet eigenverantwortlich mit Unterstützung der betreuenden Mitarbeiter statt. Eine schriftliche Ausarbeitung von ca. 20 Seiten ist zu erstellen. Die Themen sind so gewählt, dass hierfür eine Arbeitszeit von 70 Stunden anzusetzen ist.

exam: Seminarbeitrag, studienbegleitend

2.50 150538: Master-Seminar Kryptographie

Nummer: 150538
Lehrform: Seminar
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr. Eike Kiltz
Dozent: Prof. Dr. Eike Kiltz
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
angeboten im:

Ziele: Die Studierenden können sich selbständig Originalarbeiten aus dem Bereich Kryptograhie aneigenen, und wissenschaftliche Ergebnisse präsentieren.

Inhalt: Aktuelle Forschungsarbeiten der wichtigsten Kryptographie-Konferenzen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Inhalte des Moduls “Kryptographie”

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Seminarvorträge finden wöchentlich statt. Es besteht Anwesenheitspflicht. Dafür sind durchschnittlich (je nach Teilnehmerzahl) 20 Stunden anzusetzen. Die Erarbeitung des Seminarthemas findet eigenverantwortlich mit Unterstützung der betreuenden Mitarbeiter statt. Eine schriftliche Ausarbeitung von ca. 20 Seiten ist zu erstellen. Die Themen sind so gewählt, dass hierfür eine Arbeitszeit von 70 Stunden anzusetzen ist.

exam: Seminarbeitrag, studienbegleitend

2.51 150999: Master-Seminar Kryptologie

Nummer: 150999
Lehrform: Seminar
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr. Gregor Leander
Dozent: Prof. Dr. Gregor Leander
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
angeboten im:

Ziele: Die Studierenden können sich selbständig Originalarbeiten aus dem Bereich Kryptograhie aneigenen, und wissenschaftliche Ergebnisse präsentieren.

Inhalt: Aktuelle Forschungsarbeiten der wichtigsten Kryptographie-Konferenzen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Inhalte des Moduls “Kryptographie”

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Seminarvorträge finden wöchentlich statt. Es besteht Anwesenheitspflicht. Dafür sind durchschnittlich (je nach Teilnehmerzahl) 20 Stunden anzusetzen. Die Erarbeitung des Seminarthemas findet eigenverantwortlich mit Unterstützung der betreuenden Mitarbeiter statt. Eine schriftliche Ausarbeitung von ca. 20 Seiten ist zu erstellen. Die Themen sind so gewählt, dass hierfür eine Arbeitszeit von 70 Stunden anzusetzen ist.

exam: Seminarbeitrag, studienbegleitend

2.52 143240: Master-Seminar Netz- und Datensicherheit

Nummer:	143240
Lehrform:	Seminar
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk Dr.-Ing. Marcus Niemietz M. Sc. Dominik Noß
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Wintersemester und Sommersemester

Termine im Wintersemester:

Vorbesprechung: Dienstag den 08.10.2019 ab 14:15 im ID 04/413
Seminar Dienstags: ab 14:15 bis 16:45 Uhr im ID 04/413

Termine im Sommersemester:

Vorbesprechung: Dienstag den 02.04.2019 ab 15:00 im ID 03/471
Seminar Dienstags: ab 15:00 bis 16:45 Uhr im ID 03/471

Ziele: Die Teilnehmer können mit technischer und wissenschaftlicher Literatur für Forschung und Entwicklung umgehen und die Ergebnisse wissenschaftlich präsentieren.

Inhalt: Hinweis: Die Seminarthemen wurden für das SS 2019 vollständig vergeben.

Ausgewählte Themen der IT-Sicherheit mit Bezug zur Netz- und Datensicherheit werden von den Studierenden eigenständig erarbeitet.

Vorläufige Termine/Meilensteine

- 26.03.19 - 01.04.19: Zeitraum der zentralen Themenvergabe
- 03.04.19, 13:00: Einführungsveranstaltung in ID 2/168 (Präsenztermin, Anwesenheitpflicht - nicht der 02.04.19)
- 29.04.19, 23:59: Abgabe Exposé
- 27.05.19: Abgabe Vorabversion
- 24.06.19: Abgabe Endversion
- 01.07.19: Abschlusspräsentation in ID 2/168 (Präsenztermin, Anwesenheitpflicht)

Hinweis: Es werden keine Teilnahme-/Leistungsscheine ausgestellt. Die Ergebnisse werden direkt an das Prüfungsamt gemeldet.

Bei Fragen zu eurem Thema bitte den Betreuer direkt kontaktieren.

Ausarbeitungen: Vorlage: http://nds.rub.de/teaching/theses/seminar/

Anmerkungen:

Ziel des Seminars ist die Vorstellung einer wissenschaftlichen Veröffentlichung. Hierzu werden bereits veröffentliche Artikel zur Auswahl angeboten.

Die Seminarteilnehmer sollen die Veröffentlichung im Rahmen des Seminars verständlich erarbeiten und evtl. benötigte Grundlagen kurz und präzise einführen.

Die Zuteilung von Seminar-Themen geschieht über die zentrale Seminarverteilung https://seminar.hgi.rub.de/. Nach der Zuteilung des vorausgewählten Seminarthemas ist von allen Teilnehmern für das Seminarthema ein zweiseitiges Exposee beim jeweiligen Betreuer einzureichen.

Die Ausarbeitung sollte folgenden Umfang haben:

- 12 Seiten für Bachelorstudierende
- 15 Seiten für Masterstudierende
- 30 Seiten für Themen, die von zwei Personen bearbeitet werden

[system-message] [system-message]system-message
WARNING/2 in <string>, line 34
Definition list ends without a blank line; unexpected unindent. backrefs:

Ausnahmen oder Abweichungen sind mit dem jeweiligen Betreuer abzustimmen. Vor dem Präsentationstermin muss dem Betreuer eine Preversion der schriftlichen Ausarbeitung vorliegen. Diese wird durch den jeweiligen Betreuer einmalig korrigiert. Die Korrekturen sind in die finale Version der Ausarbeitung einzuarbeiten.

Ein Seminarvortrag umfasst üblicherweise 20-30 Minuten, einschließlich einer anschließenden Fragerunde. Das Foliendesign sowie die Vortragssprache (deutsch, englisch) sind freigestellt. Bitte reichen Sie Ihre Ausarbeitung und Präsentation im PDF Format ein. Powerpoint-Formate sind nicht erlaubt. Fragen und Korrekturen durch die Betreuer sind während des Vortrags möglich.

Anwesenheitspflicht:

- Zur Einführungsveranstaltung besteht Anwesenheitspflicht.
- Am Ende des Semesters werden die Vorträge innerhalb eine Blocktermins abgehalten (KEINE WÖCHENTLICHEN TERMINE!). An diesem Termin besteht Anwesenheitspflicht

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundlegende Kenntnisse der Kryptographie und / oder Netzwerktechnik

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Seminarvorträge finden als Blockveranstaltung statt. Es besteht Anwesenheitspflicht. Dafür sind durchschnittlich (je nach Teilnehmerzahl) 20 Stunden anzusetzen. Die Erarbeitung des Seminarthemas findet eigenverantwortlich mit Unterstützung der betreuenden Mitarbeiter statt. Eine schriftliche Ausarbeitung von ca. 20 Seiten ist zu erstellen. Die Themen sind so gewählt, dass hierfür eine Arbeitszeit von 70 Stunden anzusetzen ist.

exam: Seminarbeitrag, studienbegleitend

2.53 150534: Master-Seminar on Secure Multiparty Computation

Nummer:	150534
Lehrform:	Seminar
Verantwortlicher:	Jun. Prof. Dr. Sebastian Faust
Dozent:	Jun. Prof. Dr. Sebastian Faust
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Wintersemester

Ziele: Die Studierenden können sich selbständig Originalarbeiten aus dem Bereich Kryptograhie aneigenen, und wissenschaftliche Ergebnisse präsentieren.

Inhalt: ichere Multiparty Computation (MPC) Protokolle sind ein faszinierender Baustein der modernen Kryptographie. Ein MPC Protokoll erlaubt es Parteien sicher und verteilt beliebige Funktionen zu berechnen selbst wenn die Teilnehmer des Protokolls beliebig von den Vorschriften des Protokolls abweichen können. In dem Seminar werden wir grundsätzliche Konzepte und Protokolle aus dem Gebiet der MPC durchnehmen. Das Seminar orientiert sich dazu unter anderem an folgendem Buch:

Secure Multiparty Computation and Secret Sharing, Ronald Cramer, Ivan Bjerre Damgård, Jesper Buus Nielsen

Voraussichtliche Themen sind:

- Verifiable secret sharing
- Definition von MPC Protokollen (passiv/aktiv)
- OT Protokolle
- Informationstheoretisch sichere MPC Protokolle
- Effizientere MPC Protokolle gegen PPT Angreifer
- Sichere 2-Parteien Protokolle mit Yao Garbled Circuits

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Kenntnisse aus der Vorlesung Kryptographie notwendig. Kenntnisse aus Spezialvorlesungen aus der Kryptographie sind von Vorteil.

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Seminarvorträge finden wöchentlich statt. Es besteht Anwesenheitspflicht. Dafür sind durchschnittlich (je nach Teilnehmerzahl) 20 Stunden anzusetzen. Die Erarbeitung des Seminarthemas findet eigenverantwortlich mit Unterstützung der betreuenden Mitarbeiter statt. Eine schriftliche Ausarbeitung von ca. 20 Seiten ist zu erstellen. Die Themen sind so gewählt, dass hierfür eine Arbeitszeit von 70 Stunden anzusetzen ist.

exam: Seminarbeitrag, studienbegleitend

2.54 141211: Master Seminar Physical Layer Security Journal Club

number: 141211
teaching methods: seminar
media: rechnerbasierte Präsentation
Tafelanschrieb
responsible person: Prof. Dr.-Ing. Aydin Sezgin
lecturer: Prof. Dr.-Ing. Aydin Sezgin
language: english
HWS: 2
angeboten im: summer term

dates in summer term:

Vorbesprechung: Dienstag the 09.04.2019 from 14:15 to 15:45 o'clock in ID 2/340

goals: The stuu00addents unu00adderu00adstand the conu00adcepts of phyu00adsiu00adcal-layu00ader meu00adau00adsuu00adres to achieu00adve secrecy. They know how to extract the core concept and contribution from a scientific manuscript. They are able to present and introduce in an oral talk the tools and meu00adthods utilized in the respective manuscript.

content: The students are exposed to scientific manuscript within the area of physcical-layer security, which includes but is not limited to

- private information retrieval
- secure distributed computation
- wiretapping
- key generation
- authentification
- oblivious transfer
- instance hiding

They study and review the corresponding scientific paper, extract the

- essense of the problem
- importance of the problem studied
- the methodology on how the problem is tackled
- the solution
- and the insights.

Finally, they preu00adpau00adre a short sciu00adenu00adtiu00adfic talk and give a presentation to fellow stuu00addents.

requirements: Keine

recommended knowledge:

- Sysu00adtem Theou00adry
- Comu00admuu00adniu00adcau00adtiu00adons Enu00adgiu00adneeu00adring
- Stou00adchasu00adtic Siu00adgnals

exam: Seminarbeitrag, continual assessment

2.55 150540: Master-Seminar Research oriented Cryptography

Nummer: 150540
Lehrform: Seminar
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Jun. Prof. Dr. Sebastian Faust
Dozent: Jun. Prof. Dr. Sebastian Faust
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
angeboten im:

Ziele: Die Studierenden können sich selbständig Originalarbeiten aus dem Bereich Kryptograhie aneigenen, und wissenschaftliche Ergebnisse präsentieren.

Inhalt: Wissenschaftliches Arbeiten in der Kryptographie

In einer kleinen Gruppe (max. 5 Teilnehmer) wird gemeinsam unter Anleitung des Dozenten eine aktuelle wissenschaftliche Arbeit/en aus dem Gebiet der Kryptographie zunächst betrachtet. Aufbauend auf den Erkenntnissen der Betrachtung werden Verbesserungen erarbeitet, die in Form einer neuen Arbeit aufgeschrieben werden. Das genaue Thema wird in der Vorbesprechung festgelegt.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: mindestens „Kryptographie I+II“, vorteilhaft aber nicht notwendig: Besuch von Spezialvorlesungen der Kryptographie (Kryptographische Protokolle, Randomness in Cryptography, Digitale Signaturen, etc.). Inhaltlich sollen grundlegende wissenschaftliche Arbeitsweisen (Stichworte: Definitionen, Beweise, etc.) bekannt sein.

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Seminarvorträge finden wöchentlich statt. Es besteht Anwesenheitspflicht. Dafür sind durchschnittlich (je nach Teilnehmerzahl) 20 Stunden anzusetzen. Die Erarbeitung des Seminarthemas findet eigenverantwortlich mit Unterstützung der betreuenden Mitarbeiter statt. Eine schriftliche Ausarbeitung von ca. 20 Seiten ist zu erstellen. Die Themen sind so gewählt, dass hierfür eine Arbeitszeit von 70 Stunden anzusetzen ist.

exam: Seminarbeitrag, studienbegleitend

2.56 143244: Master-Seminar Security and Privacy of Wireless Networks and Mobile Devices

Nummer:	143244
Lehrform:	Seminar
Medienform:	Folien language skills training rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr. Markus Dürmuth
Dozent:	Prof. Dr. Markus Dürmuth
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	

Ziele: Die Studierenden haben einen Einblick in aktuelle Forschungsthemen und können eigenständig Fachliteratur zu einem bestimmten Themengebiet verstehen. Sie sind in der Lage eigene Texte und die Zusammenfassung komplexer Themengebiete zu verfassen. Darüber hinaus können sie einen Vortrag zur Präsentation von wissenschaftlichen Ergebnissen halten.

Inhalt: Es wird eine Auswahl an aktuellen Forschungsarbeiten im Bereich der Sicherheit in existierenden und entstehenden Funknetzwerken ebenso wie zur Sicherheit mobiler Geräte bereitgestellt. Thematische Schwerpunkte sind u.a. Sicherheitsaspekte in Ad-hoc Netzen, Location Privacy und Tracking, Authentifizierung auf mobilen Geräten etc. Dazu sollen die Studierenden anhand von Forschungsarbeiten selbständig ein Themengebiet erarbeiten und eine Ausarbeitung sowie einen Vortrag zu diesem Thema verfassen. Die Ausarbeitung hat einen Umfang von etwa 18 Seiten. Der Vortrag soll etwa 20 Minuten dauern, anschließend erfolgt eine Diskussion.

Voraussetzungen: keine

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Seminarvorträge finden als Blockveranstaltung statt. Es besteht Anwesenheitspflicht. Dafür sind durchschnittlich (je nach Teilnehmerzahl) 20 Stunden anzusetzen. Die Erarbeitung des Seminarthemas findet eigenverantwortlich mit Unterstützung der betreuenden Mitarbeiter statt. Eine schriftliche Ausarbeitung von ca. 20 Seiten ist zu erstellen. Die Themen sind so gewählt, dass hierfür eine Arbeitszeit von 70 Stunden anzusetzen ist.

exam: Praktikum, studienbegleitend

2.57 148212: Master-Seminar Sichere Hardware

Nummer:	148212
Lehrform:	Seminar
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Tim Güneysu
Dozent:	Prof. Dr.-Ing. Tim Güneysu
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	

Ziele: Die Teilnehmer können technische und wissenschafltiche Literatur finden, beschaffen verstehen und auswerten. Sie können diese wissenschaftlich präsentieren.

Inhalt: Ausgewählte Themen der IT-Sicherheit werden von den Studierenden eigenständig erarbeitet. Das Spektrum möglicher Themen reicht von der Sicherheitsanalyse eingebetteter Systeme über kryptographische Algorithmen für leistungsbeschränkte Geräte bis hin zu verschiedenen Aspekten der hardwarenahen Sicherheit. Soweit möglich werden Themen in Anlehnung an eine gerade laufende Wahlpflichtveranstaltung gewählt, um didaktische Synergieeffekte zu nutzen.

Wie auch im letzten Semester werden die Seminarthemen des Lehrstuhls über die Webseite der zentralen Seminarvergabe vergeben. Dort befinden sich ebenfalls weitere Informationen zur Bedienung und zum Auswahlverfahren.

Der Anmeldezeitraum liegt in der Regel am Ende des vorangehenden Semesters. Der genaue Zeitraum wird über die RUB-Mailingliste its-announce bekannt gegeben.

Wichtig: Die Nutzung der zentralen Seminarvergabe ist Voraussetzung für die Vergabe eines Themas sowie für die erfolgreiche Teilnahme am Seminar.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundlegende Kenntnisse in Elektrotechnik und IT-Sicherheit.

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Seminarvorträge finden als Blockveranstaltung statt. Es besteht Anwesenheitspflicht. Dafür sind durchschnittlich (je nach Teilnehmerzahl) 20 Stunden anzusetzen. Die Erarbeitung des Seminarthemas findet eigenverantwortlich mit Unterstützung der betreuenden Mitarbeiter statt. Eine schriftliche Ausarbeitung von ca. 20

Seiten ist zu erstellen. Die Themen sind so gewählt, dass hierfür eine Arbeitszeit von 70 Stunden anzusetzen ist. Eine Klausurvorbereitung entfällt, da der Vortrag und die Ausarbeitung beurteilt werden.

exam: Seminarbeitrag, studienbegleitend

2.58 143022: Master-Seminar Smart Technologies for the Internet of Things

Nummer:	143022
Lehrform:	Seminar
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Michael Hübner
Dozenten:	Prof. Dr.-Ing. Michael Hübner
	Prof. Dr. Thorsten Holz
	Prof. Dr.-Ing. Dorothea Kolossa
	Prof. Dr.-Ing. Rainer Martin
	Prof. Dr.-Ing. Aydin Sezgin
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Sommersemester

Termine im Sommersemester:

Vorbesprechung: Montag den 16.04.2018 ab 16:15 im ID 04/401

Ziele: Im Seminar werden nicht nur fachliche Kenntnisse vermittelt, sondern auch die Grundsätze und Regeln der Präsentation von Vorträgen im Allgemeinen besprochen und eingeübt. Jeder Teilnehmer ist in der Lage, einen Vortrag so zu entwerfen und zu halten, dass er als wohlgegliedert, verständlich und interessant empfunden wird. Ferner können sie über fachliche Themen angemessen diskutieren.

Inhalt: Im Sommersemester 2018 werden in diesem Seminar lehrstuhlübergreifend Aspekte des modernen "Internet der Dinge" beleuchtet. Unter anderem befassen sich die Themen mit den Bereichen: Protokolle und Systemanforderungen bezüglich Geschwindigkeit, Stromverbrauch und Sicherheit. Die Themen werden am Vorbesprechungstermin an die Teilnehmer vergeben.

Jeder Studierende hält einen englischsprachigen Vortrag über ein spezielles Thema aus dem gestellten Problemkreis und erstellt einen ca. 20-seitigen Bericht (wahlweise deutsch oder englisch). Zu allen Vorträgen gehört eine eingehende Diskussion, an der sich alle Teilnehmer beteiligen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundlegende Kenntnisse in Elektrotechnik und IT-Sicherheit.

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Seminarvorträge finden als Blockveranstaltung statt. Es besteht Anwesenheitspflicht. Dafür sind durchschnittlich (je nach Teilnehmerzahl) 20 Stunden anzusetzen. Die Erarbeitung des Seminarthemas findet eigenverantwortlich mit Unterstützung der betreuenden Mitarbeiter statt. Eine schriftliche Ausarbeitung von ca. 20 Seiten ist zu erstellen. Die Themen sind so gewählt, dass hierfür eine Arbeitszeit von 70 Stunden anzusetzen ist. Eine Klausurvorbereitung entfällt, da der Vortrag und die Ausarbeitung beurteilt werden.

exam: Seminarbeitrag, studienbegleitend

2.59 143163: Master-Seminar Sprach- und Mustererkennung

Nummer:	143163
Lehrform:	Seminar
Verantwortlicher:	Prof. Dr.-Ing. Dorothea Kolossa
Dozenten:	Prof. Dr.-Ing. Dorothea Kolossa
	Dr.-Ing. Steffen Zeiler
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Sommersemester

Termine im Sommersemester:

Vorbesprechung: Freitag den 05.04.2019 ab 10:00 im ID 2/232

Ziele: Im Seminar werden nicht nur fachliche Kenntnisse vermittelt, sondern auch die Grundsätze und Regeln der Präsentation von Vorträgen im Allgemeinen besprochen und eingeübt. Jeder Teilnehmer ist in der Lage, einen Vortrag so zu entwerfen und zu halten, dass er als gut gegliedert, verständlich und interessant empfunden wird. Ferner können die Teilnehmer über fachliche Themen angemessen diskutieren.

Inhalt: In dieser Veranstaltung werden aktuelle Forschungsthemen aus der Sprach- und Mustererkennung tiefergehend betrachtet und in studentischen Vorträgen vorgestellt. Die Studenten erarbeiten im Lauf eines Semesters einen halbstündigen Vortrag zu einem jeweils aktuellen Zeitschriften- oder Konferenzartikel und stellen diesen im Seminar vor. Mögliche Themen liegen beispielsweise im Bereich der robusten und audiovisuellen Spracherkennung, der EEG-Analyse und der multimodalen Biometrie.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Kenntnisse der digitalen Signalverarbeitung und statistische Grundlagenkenntnisse

Arbeitsaufwand: 90 Stunden

Die Arbeitsbelastung berechnet sich wie folgt: 14 Wochen zu je 3 SWS entsprechen in Summe 42 Stunden Anwesenheit. 48 Stunden werden für die Vorbereitung des eigenen Seminarvortrages angesetzt.

exam: Seminarbeitrag, studienbegleitend

Literatur:

[1] C. M., Bishop "Pattern Recognition and Machine Learning", Springer Verlag, 2006

2.60 150539: Master-Seminar Symmetrische Kryptographie

Nummer: 150539
Lehrform: Seminar
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr. Gregor Leander
Dozent: Prof. Dr. Gregor Leander
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
angeboten im: Sommersemester

Ziele: Die Studierenden können sich selbständig Originalarbeiten aus dem Bereich Kryptograhie aneigenen, und wissenschaftliche Ergebnisse präsentieren.

Inhalt: Aktuelle Forschungsarbeiten der wichtigsten Kryptographie-Konferenzen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Inhalte des Moduls “Kryptographie”

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Seminarvorträge finden wöchentlich statt. Es besteht Anwesenheitspflicht. Dafür sind durchschnittlich (je nach Teilnehmerzahl) 20 Stunden anzusetzen. Die Erarbeitung des Seminarthemas findet eigenverantwortlich mit Unterstützung der betreuenden Mitarbeiter statt. Eine schriftliche Ausarbeitung von ca. 20 Seiten ist zu erstellen. Die Themen sind so gewählt, dass hierfür eine Arbeitszeit von 70 Stunden anzusetzen ist.

exam: Seminarbeitrag, studienbegleitend

2.61 143291: Master-Seminar Usable Security and Privacy Research

Nummer: 143291
Lehrform: Seminar
Medienform: Folien
Verantwortlicher: Prof. Dr. rer. nat. Sascha Fahl
Dozent: Prof. Dr. rer. nat. Sascha Fahl
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
angeboten im:

Ziele: Das Seminar behandelt insbesondere folgende Themen:

Einführung Überblick Motivation Themen und Forschungsmethoden

Wissenschaftliche Praxis Reviews für Paper Rebuttals und Meta-Reviews PC Meeting Konferenztag

Zentrale Themen Zentrale Fragestellungen und angewandte Methoden der benutzbaren IT-Sicherheit. Wissenschaftliche Publikationspraxis: Von der Einreichung, über die Auswahl von Beiträgen bis zur Vorstellung auf einer Konferenz

Inhalt: Die Studierenden lernen den aktuellen Forschungsstand des Feldes "Usable Security and Privacy" kennen. Sie bekommen Erfahrung im kritischen Umgang mit wissenschaftlicher Literatur und erlangen einen Überblick über Themen und Forschungsmethoden. Zusätzlich dazu erlangen die Studierenden einen Einblick in die Publikationspraxis im Forschungsgebiet. Dazu wird der Begutachtungsprozess einer hochwertigen wissenschaftlichen Konferenz simuliert. Studierende schreiben Gutachten für Publikationen, setzen sich damit in einer Dikussionsrunde kritische auseinander und werden abschließend Vorträge zu ausgewählten Publikationen halten.

Voraussetzungen: Keine

Empfohlene Vorkenntnisse: Keine

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Seminarvorträge finden als Blockveranstaltung statt. Es besteht Anwesenheitspflicht. Dafür sind durchschnittlich (je nach Teilnehmerzahl) 20 Stunden anzusetzen. Die Erarbeitung des Seminarthemas findet eigenverantwortlich mit Unterstützung der betreuenden Mitarbeiter statt. Eine schriftliche Ausarbeitung von ca. 20 Seiten ist zu erstellen. Die Themen sind so gewählt, dass hierfür eine Arbeitszeit von 70 Stunden anzusetzen ist.

exam: Seminarbeitrag, studienbegleitend

2.62 140002: Master-Startup ITS

Nummer:	140002
Lehrform:	Beliebig
Verantwortlicher:	Prof. Dr.-Ing. Tim Güneysu
Dozenten:	Prof. Dr.-Ing. Tim Güneysu M. Sc. Tobias Oder
Sprache:	Deutsch
SWS:	2
Leistungspunkte:	1
angeboten im:	Wintersemester und Sommersemester

Termine im Wintersemester:

Beginn: Mittwoch den 09.10.2019 ab 16:00 im ID 03/463
Tutorium Mittwochs: ab 16:00 bis 18:00 Uhr im ID 03/463

Termine im Sommersemester:

Beginn: Mittwoch den 03.04.2019 ab 16:00 im ID 03/455
Tutorium Mittwochs: ab 16:00 bis 18:00 Uhr im ID 03/455

Ziele: Erleichterung des Einstiegs in das Studium; Vernetzung der Studierenden untereinander; Einsicht in Berufsbilder, Karrieremöglichkeiten etc.

Inhalt: Studienbegleitende Informationen, Exkursionen, Vorträge etc.
Programm Sommersemester 2018

- 11.04.2018 Kickoff
- 18.04.2018 Lehrstuhl NDS
- 25.04.2018 Entfaellt
- 02.05.2018 Lehrstuhl Systemsicherheit
- 09.05.2018 Lehrstuhl EmSec
- 16.05.2018 PHYSEC
- 30.05.2018 RIPS Tech
- 06.06.2018 Context Information Security
- 13.06.2018 Rohde und Schwarz Cybersecurity
- 15.06.2018 ITS Connect(Abweichend zum 20.06)
- 27.06.2018 TBA
- 04.07.2018 VMRay

- 11.07.2018 Ange Albertini (Google) @Hackpra

Programm WS 2017/2018

- 11.10.2017 Kick-Off: Info-Veranstaltung zum Studium/Master-Startup
- 18.10.2017 Florian Rüchel
- 25.10.2017 FluxFingers
- 01.11.2017 Feiertag
- 08.11.2017 EmSec Lehrstuhl
- 15.11.2017 PHYSEC
- 22.11.2017 RIPS
- 29.11.2017 VMRay
- 06.12.2017 David Holing (eDiscovery) und Johannes Moritz (SEC Consult)
- 13.12.2017 SysSec Lehrstuhl
- 20.12.2017 NDS Lehrstuhl
- 10.01.2018 Rhode & Schwarz Cybersecurity
- 17.01.2018 HackPra Gastvortrag 1&1 Security
- 24.01.2018
- 31.01.2018

Arbeitsaufwand: 30 Stunden

Es handelt sich um eine freiwillige Zusatzveranstaltung. Es kann 1 LP (Anerkennung als freies Wahlfach) erworben werden.

exam: None, studienbegleitend

2.63 144102: Masterarbeit ITS

Nummer: 144102
Lehrform: Masterarbeit
Verantwortlicher: Studiendekan ITS
Dozent: Hochschullehrer der Fakultät ET/IT
Sprache: Deutsch
Leistungspunkte: 30
angeboten im: Wintersemester und Sommersemester

Termine im Wintersemester:

Abschlussarbeit: nach Absprache

Termine im Sommersemester:

Abschlussarbeit: nach Absprache

Ziele: Die Teilnehmer sind mit Arbeitsmethoden der wissenschafltichen Forschung und der Projektorganisation vertraut. Ihre fortgeschrittenen Kenntisse und Arbeitsergebnisse können sie verständlich präsentieren.

Inhalt: Weitgehend eigenständige Lösung einer wissenschaftlichen Aufgabe unter Anleitung. Präsentation der eigenen Ergebnisse der Masterarbeit.

Abschlussarbeiten können grundsätzlich bei allen Hochschullehrern der Fakultät und bei den am Studiengang beteiligten Hochschullehrern der Fakultät für Mathematik angefertigt werden.

Eine Übersicht der Hochschullehrer der **Fakultät für Elektrotechnik und Informationstechnik** befindet sich unter: https://www.ei.rub.de/fakultaet/professuren/

In der Fakultät für Mathematik sind dies:

- **Lehrstuhl für Kryptologie und IT-Sicherheit - Prof. May**
  http://www.cits.rub.de
- **Lehrstuhl für Kryptographie - Prof. Kiltz**
  http://www.foc.rub.de/
- **Arbeitsgruppe für Symmetrische Kryptographie - Prof. Leander**
  http://www.cits.rub.de/personen/index.html

Voraussetzungen: siehe Prüfungsordnung

Empfohlene Vorkenntnisse: Vorkenntnisse entsprechend dem gewählten Thema erforderlich

Arbeitsaufwand: 900 Stunden

6 Monate Vollzeittätigkeit

exam: Abschlussarbeit, studienbegleitend

2.64 141252: Message-Level Security

Nummer:	141252
Lehrform:	Vorlesungen und Übungen
Medienform:	Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Dr.-Ing. Christian Mainka Dr.-Ing. Vladislav Mladenov
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
angeboten im:	Wintersemester

Termine im Wintersemester:

Beginn: Freitag den 11.10.2019
Vorlesung Freitags: ab 09:15 bis 10:45 Uhr im ID 03/411
Übung Freitags: ab 11:15 bis 12:45 Uhr im ID 03/411

Ziele: Die Studierenden haben ein Verstädnis über den Nutzen, die Verwendung und damit verbundenen Probleme von Nachrichtensicherheit.

Inhalt: Die Vorlesung behandelt das Thema *Message-Level Security*. Anders als bei SSL/TLS, welches einen sicheren Transportkanal aufbaut, geht es bei Message-Level Security darum, Nachrichten - wie beispielsweise HTTP Requests – auf Nachrichtenebene zu schützen. Hierbei kommt es auf die korrekte Verwendung von kryptographischen Verfahren als auch eine sichere Bereitstellung von API-Schnittstellen an.

Im Rahmen der Vorlesung werden verschiedene Verfahren von Message-Level Security beleuchtet.

Die Vorlesung behandelt dabei verschiedene Verfahren von Message-Level Security:

- **JSON** ist eine universelle Datenbeschreibungssprache, die unter anderem von jedem modernen Browser unterstützt wird. Mithilfe von JSON-Signature und JSON-Encryption JSON Nachrichten direkt geschützt werden. Doch reicht das aus oder können diese Sicherheitsmechanismen umgangen werden?

- **OAuth** ist eine sehr weit verbreitete Technologie zum Delegieren von Berechtigungen und wird heutzutage von allen großen Webseiten wie Facebook, Google, Twitter, Github, uvm. eingesetzt. Die Vorlesung erklärt tief-gehende Details und gängige Fehler/Angriffe, die bei der Verwendung von OAuth entstehen können.

- **OpenID Connect** ist eine Erweiterung für OAuth, um Benutzer auf Webseiten mithilfe eines Drittanbietes zu authentifizieren (Single Sign-On, z.B. Google Login). OpenID Connect hat sich in den letzten Jahren

zum defacto Standard für Web-Logins über Drittanbieter etabliert. In der Vorlesung wird detailliert erklärt, was die Unterschiede zu OAuth sind und welche Angriffe auf OpenID Connect möglich sind.

- **SAML** steht für *Security Assertion Markup Language* und ist ein Single Sign-On Standard, der weitere Verbreitung in Business-Szenerien findet. Allerdings existieren zahlreiche Angriffe von Identitätsdiebstahl bis hin zu *Remote Code Execution*.

- **PDF** ist das vermutlich am weitesten verbreitetste universelle Dokumentenaustauschformat. In der Vorlesung werden die Sicherheitseigenschaften von PDFs beleuchtet. Insbesondere werden hierbei digitale Signaturen untersucht, welche z.B. bei Verträgen zum Einsatz kommen. Wird es uns gelingen, signierte Dokumente zu fälschen?

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

Empfohlene Vorkenntnisse:

- Grundkenntnisse HTTP, HTML und Kryptographie

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 38 Stunden sind für die Klausurvorbereitung vorgesehen.

exam: schriftlich, 120 Minuten

2.65 141032: Methoden der Benutzer-Authentisierung

Nummer:	141032
Lehrform:	Vorlesungen und Übungen
Medienform:	Moodle rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr. Markus Dürmuth
Dozenten:	Prof. Dr. Markus Dürmuth M. Sc. Maximilian Golla M. Sc. Philipp Markert
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	4
angeboten im:	Wintersemester

Termine im Wintersemester:

Beginn: Freitag den 11.10.2019
Vorlesung Freitags: ab 10:15 bis 11:45 Uhr im ID 03/445
Übung Freitags: ab 12:15 bis 13:00 Uhr im ID 03/445

Ziele: Die Studierenden haben einen umfassenden Überblick über die verschiedenen Möglichkeiten zur Benutzerauthentifizierung.

Inhalt: Diese Vorlesung behandelt verschiedene Formen der Benutzerauthentisierung. Ausgehend von Passwörtern, die wir wohl alle täglich benutzen, wollen wir untersuchen wie genau Passwörter eingesetzt werden, warum sie nicht besonders sicher sind, und wie wir ihre Sicherheit erhöhen können. Weiter betrachten wir zahlreiche Alternativen, wie Einmal-Passwörter, grafische Passwörter (z. B. Android-Entsperrmuster oder Windows 10), Sicherheitstokens (z. B. YubiKey oder RSA SecurID), oder biometrische Verfahren (z. B. Gesichtserkennung oder basierend auf Gehirnaktivitat), und lernen deren Funktionsweise sowie Vor- und Nachteile kennen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Solide Programmierkenntnisse

Arbeitsaufwand: 120 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 3 SWS entsprechen in Summe 42 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 22 Stunden sind für die Klausurvorbereitung vorgesehen.

exam: schriftlich, 120 Minuten

2.66 141150: Multi-Core Architekturen und deren Programmierung

Nummer:	141150
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Michael Hübner
Dozenten:	Prof. Dr.-Ing. Michael Hübner
	M. Sc. Jens Rettkowski
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
angeboten im:	

Ziele: Die Studierenden haben einen Überblick über verschiedene Multi-Core Architekturen und deren Programmiermodelle. Anhand praktischer Rechnerübungen sind die Teilnehmer befähigt eigene eingebettete Multi-Core Architekturen anhand von FPGA Technologie zu entwickeln, sowie aktuelle Grafikkarten mittels CUDA C/C++ zu programmieren.

The students have an overview of multi-core architectures and parallel programming models. Using computer exercises the attendees can develop own embedded multi-core architectures based on FPGA technology and program state-of-the-art graphic cards using CUDA C/C++.

Inhalt: Im Rahmen der Vorlesung werden zunächst Multi-Core Architekturen und deren Komponenten (z.B. Prozessoren, Speicher, Kommunikationsinfrastrukturen) vorgestellt. Anschließend werden verschiedene Programmiermodelle (OpenMP, MPI, CUDA C/C++, OpenCL) erläutert. In den Laborübungen werden die theoretischen Kenntnisse unter Verwendung von Multi-Core Architekturen und Grafikkarten erweitert und vertieft.

First multi-core architectures and their hardware components (e.g. processors, memories, and communication infrastructures) will be introduced. Afterwards parallel programming models (e.g. OpenMP, MPI, CUDA C/C++, and OpenCL) will be explained. The theoretical contents are supplemented using computer exercises for developing own multi-core architectures based on FPGA technology and for programming state-of-the-art graphic cards using CUDA C/C++.

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Programmierkenntnisse in C/C++ oder einer ähnlichen Programmiersprache
- Knowledge of C/C++ or a similar programming language is required

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 38 Stunden sind für die Klausurvorbereitung vorgesehen.

exam: schriftlich, 120 Minuten

2.67 310509: Nebenläufige Programmierung

Nummer:	310509
Lehrform:	Vorlesungen und Übungen
Medienform:	e-learning rechnerbasierte Präsentation
Verantwortlicher:	Dr.-Ing. Doga Arinir
Dozent:	Dr.-Ing. Doga Arinir
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	4
angeboten im:	Sommersemester

Termine im Sommersemester:

Vorlesung m. int. Übung Freitags: ab 08:00 bis 11:00 Uhr im IA 02/481

Ziele: Die Studierenden haben grundlegende Fähigkeiten und Techniken, um nebenläufige Programme sicher entwickeln zu können. Es kennen softwaretechnische Entwurfsmuster, welche bekannte Probleme bei nebenläufigen Programmen wie zum Beispiel die Verklemmung vermeiden lassen. Die Teilnehmer können

- die Performanz von Programmen durch den Einsatz der nebenläufigen Programmierung verbessern,
- bestehende Programme analysieren und mögliche Fehler erkennen und
- die Sprachmerkmale und Schnittstellen von JAVA für die nebenläufige Programmierung sicher anwenden.

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

- Nebenläufigkeit: Schnelleinstieg
  - Anwendungen vs. Prozesse
  - Programme und ihre Ausführung
  - Vorteile & Probleme von nebenläufigen Programmen
    - Verbesserung der Performanz
    - Synchronisation
    - Realisierung kritischer Abschnitte

    - Monitore
    - Lebendigkeit
    - Verklemmungen
- Threads in Java
- UML-Modellierung von Nebenläufigkeit
- Neues zur Nebenläufigkeit in Java 5 und Java 6
- Realisierung von Nebenläufigkeit
- Fortgeschrittene Java-Konzepte für Nebenläufigkeit

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Inhalte der Vorlesungen:

- Informatik 1
- Informatik 2
- Web-Engineering
- Softwaretechnik 1

Arbeitsaufwand: 120 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 3 SWS entsprechen in Summe 42 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 22 Stunden sind für die Klausurvorbereitung vorgesehen.

exam: schriftlich, 90 Minuten

Literatur:

[1] Arinir, Doga, Ziesche, Peter "Java: Nebenläufige und verteilte Programmierung, 2. Auflage", W3l, 2010

2.68 141105: Nichttechnische Veranstaltungen

Nummer: 141105
Lehrform: Beliebig
Verantwortlicher: Dekan
Dozent: Dozenten der RUB
Sprache: Deutsch
angeboten im: Wintersemester und Sommersemester

Ziele: Innerhalb des Moduls setzen die Studierenden entsprechend ihrer Interessen verschiedene Schwerpunkte. Dafür steht Ihnen das breite Angebot der ganzen Universität zur Verfügung. Sie beherrschen entsprechend ihrer Auswahl verschiedene Schlüsselqualifikationen.

Inhalt: Neben den in der Studiengangsübersicht angegebenen Lehrveranstaltungen können die Studierenden aus dem Angebot der Ruhr-Universität weitere Veranstaltungen auswählen. Es muss sich dabei um nichttechnische Fächer handeln. Ausgenommen sind somit die Fächer der Ingenieurwissenschaften sowie der Physik und Mathematik. Möglich Inhalte sind dagegen Sprachen, BWL, Jura, Chemie etc.

Beispielsweise gibt es verschiedene spezielle **Englischkurse**: Es wird ein Kurs Technisches Englisch für Bachelorstudierende der Fakultät angeboten. Außerdem wird ein weiterführender Englischkurs Projects and management in technical contexts für Masterstudierende angeboten. Schließlich richtet sich der allgemeine Kurs Engineer your careers an Bachelor- und Masterstudierende.

Aus anderen Bereichen gibt es folgende Kurse:

Der Ingenieur als Manager

Angewandte Methoden zur Trendforschung und Ideenfindung .

Methods and Instruments of Technology Management

Scientific Working

Im Zusammenhang mit dem Thema “Existenzgründung” gibt es folgenden Kurs:

Coaching für Existenzgründer

Unsicherheitserfahrung und Bewältigungsstrategien im unternehmerischen Kontext – Simulationsbasierte Lernansätze

Bei der Auswahl kann außerdem das Vorlesungsverzeichnis der Ruhr-Universität verwendet werden, eine Beispiele sind:

0em

BWL: https://www.wiwi.ruhr-uni-bochum.de/zfoeb

Sprachen: http://www.ruhr-uni-bochum.de/zfa/

Recht: https://zrsweb.zrs.rub.de/institut/qzr/

Schreibzentrum: https://www.zfw.rub.de/sz/ (z.B. Vorbereitung auf die Abschlussarbeit)

Bitte beachten Sie, dass die Vorlesungen "BWL für Ingenieure" und "BWL für Nichtökonomen" identischen Inhalt haben und deshalb nur eine von beiden Veranstaltungen anerkannt werden kann. Gleiches gilt für die Veranstaltungen "Kostenrechnung" und "Einführung in das Rechnungswesen/Controlling".

Voraussetzungen: entsprechend den Angaben zu der gewählten Veranstaltungen

Empfohlene Vorkenntnisse: entsprechend den Angaben zu der gewählten Veranstaltungen

exam: None, studienbegleitend

Beschreibung der Prüfungsleistung: Die Prüfung kann entsprechend der gewählten Veranstaltungen variieren.

2.69 141028: Physical Attacks and Countermeasures

number: 141028
teaching methods: lecture with tutorials
responsible person: Priv.-Doz. Dr. Amir Moradi
Lecturers: Priv.-Doz. Dr. Amir Moradi
M. Sc. Thorben Moos
M. Sc. Felix Wegener
language: english
HWS: 4
Leistungspunkte: 5
angeboten im: summer term

dates in summer term:

Beginn: Montag the 01.04.2019
Vorlesung Montags: from 14:15 to 15:45 o'clock in ID 03/471
Übung Montags: from 16:00 to 16:45 o'clock in ID 03/471
Praxisübung Montags: from 17:00 to 17:45 o'clock in ID 2/632

goals: Die Studierenden

- haben ein Gefühl für die Gefährlichkeit von kryptanalytischen Angriffen für Implementierungen von kryptographischen Algorithmen.
- verstehen wie und warum physikalische Angriffe funktionieren.
- kennen mögliche Gegenmaßnahmen und wissen wie diese eingesetzt werden, um ein System gegen physikalische Angriffe zu schützen.

content: Moderne kryptographische Algorithmen bieten ausreichend Schutz gegen die bekannten mathematischen Angriffe. In der Praxis werden diese Algorithmen für sicherheits-kritische Anwendungen auf verschiedenen Plattformen implementiert. Dies geschieht sowohl als Programmcode (Software) als auch mit logischen Elementen (Hardware). Der physikalische Zugang zu kryptographischen Implementierungen (z.B., eine Smartcard oder ein Smartphone, welche zum Bezahlen benutzt werden), in welchen der geheime Schlüssel eingebettet ist, hat zur Entwicklung einer neuen Klasse von Angriffen, genannt physikalische Angriffe, geführt. Diese Angriffe zielen darauf ab den geheimen Schlüssel, der vom kryptographischen Algorithmus benutzt wird, zu extrahieren. Dabei verlassen sich diese Art von Angriffen nicht auf Schwächen im Algorithmus sondern nutzen Schwachstellen der Implementierung aus. Daher müssen diese Angriffe bereits in der Entwicklungsphase von kryptographischen Implementierungen berücksichtigt werden. Das Ziel dieser Lehrveranstaltung ist es einen Überblick über bekannte physikalische Angriffe und deren Gegenmaßnahmen zu geben. Im ersten Teil der Vorlesung

werden die verschiedenen Angriffstypen eingeführt, während im zweiten Teil der Fokus auf Gegenmaßnahmen liegt.

requirements: none

recommended knowledge: Grundkenntnisse der Datensicherheit und Kryptographie, eine Programmiersprache (C++), Computerarchitektur

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 38 Stunden sind für die Prüfungsvorbereitung vorgesehen.

exam: schriftlich, 120 Minuten

2.70 141212: Physical-Layer Security

Nummer: 141212
Lehrform: Vorlesungen und Übungen
Verantwortlicher: Prof. Dr.-Ing. Aydin Sezgin
Dozent: Prof. Dr.-Ing. Aydin Sezgin
Sprache: Deutsch
SWS: 4
Leistungspunkte: 5
angeboten im:

Termine im Sommersemester:

Beginn: Donnerstag den 20.04.2017
Vorlesung Donnerstags: ab 14:15 bis 15:45 Uhr im ID 03/471
Übung Donnerstags: ab 16:15 bis 17:45 Uhr im ID 03/471

Ziele: The students understand the concepts of physical-layer measures to achieve secrecy. Equipped with tools and methods acquired during the lectures, new setups can be investigated.

Inhalt: The broadcast nature of wireless systems makes it more vulnerable to eavesdroppers to extract data from the received signals. The conventional way to achieve confidentiality is by using cryptographic encryption based on keys. The idea behind is that the eavesdropper is assumed to have limited time or computational resources. While this approach has both it advantages and disadvantages, the physical-layer approach can be regarded as a powerful alternative or as an additional level of protection to achieve security in wireless networks. A distinct feature of the physical-layer approach is that the eavesdropper is assumed to have unlimited time and resources available. Furthermore, this approach guarantees both reliability and security, which the other approach can not. In this lecture, we will cover the following aspects and setups

- Part I: Review

[system-message] [system-message]system-message
WARNING/2 in `<string>`, line 6
Bullet list ends without a blank line; unexpected unindent. backrefs:

  - Entropy, Mutual Information, Differential Entropy
  - Fading channels
  - Capacity of Gaussian channels
  - Medium Access (Centralized and Distributed)
  - Coding on Dirty Paper
  - Beamforming and zero-forcing

- Deterministic models
- Interference Alignment

[system-message] [system-message]system-message
WARNING/2 in <string>, line 14
Block quote ends without a blank line; unexpected unindent. backrefs:

- Part II: Basics

[system-message] [system-message]system-message
WARNING/2 in <string>, line 15
Bullet list ends without a blank line; unexpected unindent. backrefs:

- Confidentiality and Encryption
- Basic Wyner Wiretap Channel
- Multiple-Antenna Wiretap Channel

[system-message] [system-message]system-message
WARNING/2 in <string>, line 18
Block quote ends without a blank line; unexpected unindent. backrefs:

- Part III: Advanced Topics

[system-message] [system-message]system-message
WARNING/2 in <string>, line 19
Bullet list ends without a blank line; unexpected unindent. backrefs:

- Broadcast channel with side information
- Secret-Key Agreement: Half-Duplex vs. Full-Duplex
- Specific Multiuser Wiretap Channels
- Caching in D2D networks with secure delivery
- Retrospective Alignment and Jamming
- Network Coding, Source Coding
- Cross-Layer Design

[system-message] [system-message]system-message
WARNING/2 in <string>, line 26
Block quote ends without a blank line; unexpected unindent. backrefs:

- Practical Projects

[system-message] [system-message]system-message
WARNING/2 in <string>, line 27
Bullet list ends without a blank line; unexpected unindent. backrefs:

- Medium Access
- Antenna design and beamforming
- Jamming
- Software defined radio based implementations of physical-layer security methods

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- System Theory
- Communications Engineering
- Stochastic Signals

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 5 Stunden pro Woche, in Summe 70 Stunden, erforderlich. Etwa 24 Stunden sind für die Prüfungsvorbereitung vorgesehen.

exam: mündlich, 30 Minuten

2.71 148215: Private and Anonymous Communication

number: 148215
teaching methods: lecture with tutorials
media: rechnerbasierte Präsentation
responsible person: Prof. Dr. Christina Pöpper
lecturer: Prof. Dr. Christina Pöpper
language: english
HWS: 4
Leistungspunkte: 5
angeboten im:

goals: The students are able to describe, classify, and assess techniques for private and anonymous communication. They are able to reason about the motivation for using these techniques and can describe different scenarios and applications. They are able to describe, classify, and (to a certain extent) counter attacks on privacy and anonymity. The students understand the architectures of different tools, approaches, and techniques that have been proposed and developed in this context. They are able to reason about the achieved levels of protection and also gain practical experience with different tools.

content: The focus of this course are privacy-enhancing technologies and anonymity techniques. Central elements are privacy metrics and techniques, vulnerabilities and attack mechanisms as well as detection, protection, and prevention techniques. The course will cover techniques for anonymous communication and browsing (e.g., Tor), anonymity in electronic payment systems (e.g., E-Cash, Bitcoin), steganographic and censorship circumvention techniques, communication hiding, and location privacy. The course may also cover special topics such as electronic voting or privacy in social networks.

requirements: none

recommended knowledge: Knowledge of the contents of Netzsicherheit and Computernetze as well as expertise in programming will be beneficial.

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 38 Stunden sind für die Klausurvorbereitung vorgesehen.

exam: schriftlich, 120 Minuten

2.72 150353: Privatheit und Authentizität

Nummer:	150353
Lehrform:	Vorlesung
Medienform:	rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Dr.-Ing. Sven Schäge
Dozent:	Dr.-Ing. Sven Schäge
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	4.5
angeboten im:	Wintersemester

Ziele: Die Studierenden sind befähigt, kryptographische Verfahren zu verifizieren, ihre Effizienz zu bewerten und in Anwendungen zielgerichtet - insbesondere anstelle klassischer Authentikationsverfahren - einzusetzen.

Inhalt: Die Studierenden erlernen kryptographische Ansätze um die widerstrebenden Sicherheitsziele Privatheit und Authentizität zu vereinbaren. Zunächst wird eine Einführung und Diskussion von unterschiedlichen Formalisierungen von Privatheit und Authentizität in der Kryptographie gegeben. Anschließend werden mehrere kryptographische Lösungskonzepte vorgestellt.

Hierunter zählen: - Ringsignaturen - Gruppensignaturen - (Nicht-interaktive) Zero-knowledge Beweise - Anonymous Credential Systems

Zu jedem dieser Bausteine werden konkrete Realisierungen vorgestellt.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Kenntnisse aus der Vorlesung Kryptographie

Arbeitsaufwand: 135 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 3 SWS ergeben 42 Stunden Anwesenheit. Zum Lösen der Übungsaufgaben sind zwei Stunden je Woche vorgesehen. Es verbleiben 65 Stunden zur Vor- und Nachbereitung und zur Prüfungsvorbereitung.

exam: mündlich, 30 Minuten

2.73 150355: Probabilistische Algorithmen

Nummer: 150355
Lehrform: Vorlesungen und Übungen
Verantwortlicher: Prof. Dr. Alexander May
Dozent: Prof. Dr. Alexander May
Sprache: Deutsch
SWS: 4
Leistungspunkte: 5
angeboten im: Wintersemester und Sommersemester

Termine im Wintersemester:

Beginn:

Ziele: In der Vorlesung Probabilistische Algorithmen werden probabilistische Methoden zur Analyse von Algorithmen verwendet.

Inhalt:

- Diskrete Zufallsvariablen und Momente
- Chernoff Schranken
- Bälle, Urnen und zufällige Graphen
- Probabilistische Methode
- Markovketten und Random Walks
- Entropie
- Monte Carlo Methode
- Universelle Hashfunktionen

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Diskrete Mathematik

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 38 Stunden sind für die Klausurvorbereitung vorgesehen.

exam: mündlich, 30 Minuten

2.74 141241: Programmanalyse

Nummer:	141241
Lehrform:	Vorlesungen und Übungen
Medienform:	e-learning rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozenten:	Prof. Dr. Thorsten Holz M. Sc. Tim Blazytko M. Sc. Emre Güler M. Sc. Sergej Schumilo
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
angeboten im:	Sommersemester

Termine im Sommersemester:

Beginn: Dienstag den 02.04.2019
Vorlesung Dienstags: ab 14:15 bis 15:45 Uhr im ID 04/471
Vorlesung Dienstags: ab 14:15 bis 15:45 Uhr im ID 04/459
Übung Donnerstags: ab 12:15 bis 13:45 Uhr im ID 04/471
Übung Donnerstags: ab 12:15 bis 13:45 Uhr im ID 04/459

Ziele: 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.

Inhalt: In der Vorlesung werden unter anderem die folgenden Themen und Techniken aus dem Bereich der Programmanalyse behandelt:

- Statische und dynamische Analyse von Programmen
- Analyse von Kontroll- und Datenfluss
- Symbolische Ausführung
- Taint Tracking
- Virtual Machine Introspektion
- 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.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Erfahrung in systemnaher Programmierung, Assembler sowie Programmieren in C sind hilfreich für das Verständnis der vermittelten Themen. Vorkenntnisse aus den Vorlesungen Eingebettete Prozessoren (insbesondere Assembler-Programmierung) sowie Systemsicherheit/Betriebssystemsicherheit sind hilfreich aber nicht notwendig zum Verständnis der Themen.

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 38 Stunden sind für die Klausurvorbereitung vorgesehen.

exam: schriftlich + studienbegleitend, 120 Minuten

2.75 150277: Public Key Verschlüsselung

Nummer:	150277
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Jun. Prof. Dr. Nils Fleischhacker
Dozent:	Jun. Prof. Dr. Nils Fleischhacker
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
angeboten im:	Wintersemester

Ziele: x

Inhalt: Die Vorlesung gibt einen Einblick in theoretische und praktische Aspekten der Public Key Verschlüsselung. Dies umfasst Grundlagen und formalen Definitionen von Sicherheit (CPA, CCA1, CCA2), die beweisbare Sicherheit verschiedener theoretischer und praktischer Konstruktionen, sowie die Verbindungen von Public Key Verschlüsselung zu anderen Aspekten der Krytographie.

Voraussetzungen: Als Voraussetzung für die Vorlesung sind Vorkenntnisse in Kryptographie und beweisbarer Sicherheit, insbesondere von Reduktionsbeweisen, hilfreich aber nicht zwingend erforderlich.

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 15 Wochen zu je 4 SWS ergeben 60 Stunden Anwesenheit. Zum Lösen der Übungsaufgaben sind zwei Stunden je Woche vorgesehen. Es verbleiben 60 Stunden zur Vor- und Nachbereitung und zur Prüfungsvorbereitung.

exam: mündlich, 30 Minuten

2.76 150318: Quantenalgorithmen

Nummer: 150318
Lehrform: Vorlesungen und Übungen
Verantwortlicher: Prof. Dr. Alexander May
Dozent: Prof. Dr. Alexander May
Sprache: Deutsch
SWS: 4
Leistungspunkte: 5
angeboten im: Wintersemester

Termine im Wintersemester:

Beginn:

Ziele: Die Studierenden beherrschen die Grundlagen für Quantenalgorithmen.

Inhalt: Die Vorlesung gibt einen Einblick in die Konstruktion von Algorithmen für Quantenrechner.

- Themenübersicht:
  - Quantenbits und Quantengatter
  - Separabilität und Verschränkung
  - Teleportation
  - Quantenschlüsselaustausch
  - Quantenkomplexität
  - Simons Problem
  - Shors Faktorisierungsalgorithmus
  - Grovers Suchalgorithmus

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Lineare Algebra, Algorithmen

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 15 Wochen zu je 3 SWS ergeben 45 Stunden Anwesenheit. Zum Lösen der Übungsaufgaben sind zwei Stunden je Woche vorgesehen. Es verbleiben 75 Stunden zur Vor- und Nachbereitung und zur Prüfungsvorbereitung.

exam: schriftlich, 120 Minuten

2.77 150345: Randomness in Cryptography

Nummer:	150345
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Jun. Prof. Dr. Sebastian Faust
Dozent:	Jun. Prof. Dr. Sebastian Faust
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	4.5
angeboten im:	

Ziele: Gute Zufälligkeit ist eine fundamentale Voraussetzung für sichere kryptographische Algorithmen. Zufälligkeit wird benötigt um gute Schlüssel zu erzeugen und findet Einsatz bei vielen kryptographischen Algorithmen (wie z.B. beim Verschlüsseln). Leider ist es in der Praxis aufwendig gute Zufallswerte zu erzeugen. Die Vorlesung beschäftigt sich mit praktischen und theoretischen Techniken der Erzeugung von guten Zufallswerten und zeigt auf wie schlechte Zufallswerte in der Praxis zum Verlust von Sicherheit führen können.

Inhalt: Voraussichtliche Themen sind: - Praktische Angriffe auf Systeme mit schlechtem Zufall - Einführung in relevante Konzepte der Informationstheorie - Extraktoren und Kondensers zur Erzeugen von Zufälligkeit - Pseudozufälligkeit - Erzeugen von Zufälligkeit in der Praxis (dev/random und Fortuna in Windows und deren Sicherheitsanalyse) - Kryptographie mit ungenügender Zufälligkeit

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Kryptographie I+II, Interesse an praktischen und theoretischen Fragestellungen in der Kryptographie.

Arbeitsaufwand: 135 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 3 SWS ergeben 42 Stunden Anwesenheit. Zum Lösen der Übungsaufgaben sind zwei Stunden je Woche vorgesehen. Es verbleiben 65 Stunden zur Vor- und Nachbereitung und zur Prüfungsvorbereitung.

exam: mündlich, 30 Minuten

2.78 150537: Seminar zur Kryptographie

Nummer: 150537
Lehrform: Seminar
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr. Gregor Leander
Dozent: Prof. Dr. Gregor Leander
Sprache: Deutsch
SWS: 2
Leistungspunkte: 3
angeboten im: Sommersemester

Ziele: Die Studierenden können sich selbständig Originalarbeiten aus dem Bereich Kryptograhie aneigenen, und wissenschaftliche Ergebnisse präsentieren.

Inhalt: Aktuelle Forschungsarbeiten der wichtigsten Kryptographie-Konferenzen.

Voraussetzungen: Keine

Empfohlene Vorkenntnisse: Inhalte des Moduls “Kryptographie”

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Seminarvorträge finden wöchentlich statt. Es besteht Anwesenheitspflicht. Dafür sind durchschnittlich (je nach Teilnehmerzahl) 20 Stunden anzusetzen. Die Erarbeitung des Seminarthemas findet eigenverantwortlich mit Unterstützung der betreuenden Mitarbeiter statt. Eine schriftliche Ausarbeitung von ca. 20 Seiten ist zu erstellen. Die Themen sind so gewählt, dass hierfür eine Arbeitszeit von 70 Stunden anzusetzen ist.

exam: Seminarbeitrag, studienbegleitend

2.79 150560: Seminar zur Real World Cryptoanalysis

Nummer: 150560
Lehrform: Seminar
Medienform: Folien
Verantwortlicher: Prof. Dr. Alexander May
Dozent: Prof. Dr. Alexander May
Sprache: Deutsch
SWS: 2
Leistungspunkte: 4
angeboten im: Wintersemester

Termine im Sommersemester:

Seminar Dienstags: ab 14:00 bis 16:00 Uhr

Ziele: Ziel des Seminares ist es, sich selbstständig in eine wissenschaftliche Veröffentlichung einzuarbeiten, diese aufzubereiten und im Rahmen eines Vortrages den Teilnehmern zu präsentieren.

Inhalt: Das Seminar befasst sich mit praxisrelevanten Themen der Kryptographie und Kryptanalyse.

Empfohlene Vorkenntnisse: Ein allgemeines Verständnis von IT-Sicherheit ist hilfreich. Weiterhin sind, je nach Thema, Inhalte nützlich, wie sie etwa in den Vorlesungen Kryptgraphie I + II und Kryptanaylse vermittelt werden. In der Regel lassen sich aber Themen abhängig von bereits besuchten Veranstaltungen finden.

Arbeitsaufwand: 120 Stunden

XXX

exam: Seminarbeitrag, studienbegleitend

2.80 150359: Sicherheit und Privatheit für Big Data

Nummer:	150359
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Dr.-Ing. Sven Schäge
Dozent:	Dr.-Ing. Sven Schäge
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	4.5
angeboten im:	Wintersemester

Ziele: Die Studierenden sind befähigt, kryptographische Verfahren für Big-Data Anwendungen zu verifizieren, ihre Effizienz zu bewerten und in Anwendungen zielgerichtet einzusetzen.

Inhalt: Die Vorlesung behandelt Ansätze um Sicherheitsverfahren zu designen, zu analysieren oder zu vergleichen, die in Anwendungsszenarien mit großen Nutzerzahlen oder Datenmengen eingesetzt werden (können). Insbesondere sollen Verfahren betrachtet werden, mit Hilfe derer die zweckmäßige Anwendbarkeit klassischer Sicherheitssysteme in diesen Szenarien untersucht werden können.

Die Vorlesung ist inhaltlich in zwei Themenblöcke organisiert.

1) Der erste Themenblock behandelt realistische Modellierungen von Sicherheit in Mehrparteienmodellen und effiziente Sicherheitsreduktionen (tightness in multi-user cryptography). Hier geht es insbesondere um Anwendungen mit hohen Nutzerzahlen.

   - Effiziente Sicherheitsreduktionen (tightness) und ihre Auswirkung auf Systemparameter
   - Selbstreduzierbarkeit von kryptografischen Problemen und ihre Anwendung in Mehrparteienanwendungen
   - Nachweis untere Tightness
   - Schranken und optimal effiziente Sicherheitsreduktionen

2) Im zweiten Themenblock werden wichtige und praktische Verfahren vorgestellt, die effizient auf großen Datenmengen arbeiten. Wichtige Themen sind:

   - Searchable Encryption
   - Order-Preserving Encryption

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Empfohlen wird der Besuch der Vorlesung Kryptographie.

Arbeitsaufwand: 135 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 3 SWS ergeben 42 Stunden Anwesenheit. Zum Lösen der Übungsaufgaben sind zwei Stunden je Woche vorgesehen. Es verbleiben 65 Stunden zur Vor- und Nachbereitung und zur Prüfungsvorbereitung.

exam: mündlich, 30 Minuten

2.81 141030: Software-Implementierung kryptographischer Verfahren

Nummer: 141030
Lehrform: Vorlesungen und Übungen
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr.-Ing. Christof Paar
Dozent: M. Sc. Max Hoffmann
Sprache: Deutsch
SWS: 4
Leistungspunkte: 5
angeboten im: Sommersemester

Termine im Sommersemester:

Beginn: Mittwoch den 03.04.2019
Vorlesung m. int. Übung Mittwochs: ab 14:15 bis 16:45 Uhr im ID 04/653

Ziele: Die Studierenden haben ein Verständnis für Methoden für die schnelle Software-Realisierung ausgewählter Krypto-Verfahren und diese selbst implementiert.

Inhalt: Es werden ausgewählte fortgeschrittene Implementierungstechniken der modernen Kryptographie behandelt.

Inhalte:

- Effiziente Implementierung von Blockchiffren
- Bitslicing
- Effiziente Arithmetik in GF(2^m)
- Effiziente Arithmetik auf elliptischen Kurven
- Spezielle Primzahlen zur schnellen modularen Reduktion
- Primzahltests
- Post-Quantum Kryptographie
- Secure Coding

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse der Programmiersprache C bzw. C++, Vorlesung “Einführung in die Kryptographie I”

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 38 Stunden sind für die Klausurvorbereitung vorgesehen.

exam: schriftlich, 120 Minuten

2.82 148171: Sprachimplementierung

Nummer:	148171
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr. Eberhard Bertsch
Dozent:	Prof. Dr. Eberhard Bertsch
Sprache:	Deutsch
SWS:	6
Leistungspunkte:	9
angeboten im:	

Ziele: Die Studierenden haben Kenntnisse und Verständnis von Übersetzungsverfahren, speziell auch für prozedurale Programmiersprachen (wie C++, Java).

Inhalt: Die effiziente Implementierung von Programmiersprachen wie PASCAL, C oder JAVA gehört zu den wichtigsten und zugleich anspruchsvollsten Aufgaben der Praktischen Informatik. Im Laufe mehrerer Jahrzehnte wurde eine Reihe von Methoden entwickelt, die heute zum Kernbestand dieses Gebiets gehören, und die sich sinngemäß auch auf die Realisierung einfacherer Benutzer-Schnittstellen anwenden lassen. Hierzu gehören unter anderem: Lexikalische Analyse (Scanner); Syntax-Analyse, insbesondere mit LL(1)- und LR(1)-Grammatiken; statische Semantik; Laufzeitbehandlung von imperativen Konstrukten; dynamische Datentypen; Optimierung zur Compile-Zeit. Je nach Interesse seitens der Studierenden können methodisch verwandte Algorithmen zur Analyse von Zeichenketten einbezogen werden, die in der molekularen Biologie eine zunehmende Rolle spielen (beim Mustervergleich in DNA-Sequenzen und Proteinen).

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundlagen der Informatik

Arbeitsaufwand: 270 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 6 SWS ergeben 84 Stunden Anwesenheit. Zur Vor-und Nachbereitung sind 126 Stunden sowie für die Prüfungsvorbereitung 60 Stunden vorgesehen.

exam: schriftlich, 90 Minuten

Literatur:

[1] Aho, Alfred V., Lam, Monica S., Sethi, Ravi "Compilers Principles, Techniques, & Tools", Addison Wesley Longman Publishing Co, 2005
[2] Maurer, Dieter, Wilhelm, Reinhard "Übersetzerbau. Theorie, Konstruktion, Generierung", Springer, 1996

2.83 150351: Symmetrische Kryptanalyse

Nummer: 150351
Lehrform: Vorlesungen und Übungen
Verantwortlicher: Prof. Dr. Gregor Leander
Dozent: Prof. Dr. Gregor Leander
Sprache: Deutsch
SWS: 4
Leistungspunkte: 5
angeboten im: Wintersemester

Termine im Wintersemester:

Beginn: Dienstag den 09.10.2018
Vorlesung Dienstags: ab 08:30 bis 10:00 Uhr im NA 3/99

Ziele: Die Studierenden haben ein vertieftes Verständnis für die Sicherheit symmetrischer Chiffren.

Inhalt: Wir behandeln die wichtigsten Themen in der symmetrischen Kryptanalyse. Nach einer ausführlichen Vorstellung von linearer und differentieller Kryptanalyse werden weitere Angriffe auf symmetrische Primitive, insbesondere Block-Chiffren behandelt. Hierzu zählen insbesondere Integral (auch Square) Attacken, Impossible Differentials, Boomerang-Angriffe und Slide-Attacken. Neben den Angriffen selbst werden auch immer die daraus resultierenden Design-Kriterien beschrieben, um neue Algorithmen sicher gegen die Angriffe zu machen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Einführung in die Kryptographie 1

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 38 Stunden sind für die Klausurvorbereitung vorgesehen.

exam: mündlich, 30 Minuten

Literatur:

[1] Knudsen, Lars, Robshaw, Matthew "The Block Cipher Companion", Springer, 2012

2.84 150240: Theoretische Informatik

Nummer:	150240
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien
	Tafelanschrieb
Verantwortlicher:	Prof. Dr. Hans Ulrich Simon
Dozent:	Prof. Dr. Hans Ulrich Simon
Sprache:	Deutsch
SWS:	6
Leistungspunkte:	9
angeboten im:	Wintersemester

Termine im Wintersemester:

Beginn: Mittwoch den 10.10.2018
Vorlesung Montags: ab 10:00 bis 12:00 Uhr im HZO 70
Vorlesung Mittwochs: ab 10:00 bis 12:00 Uhr im HNC 20
Übung (alternativ) Dienstags: ab 14:00 bis 16:00 Uhr im IA 1/63
Übung (alternativ) Dienstags: ab 14:00 bis 16:00 Uhr im NB 5/99
Übung (alternativ) Mittwochs: ab 08:00 bis 10:00 Uhr im IA 1/181
Übung (alternativ) Mittwochs: ab 14:00 bis 16:00 Uhr im IA 1/63

Ziele: Die studierenden haben fundamentale Einsichten zum Verhältnis zwischen Automaten und Grammatiken und zum Verhältnis von Determinismus und Nicht-Determinismus. Durch Einüben von Beweistechniken wie wechselseitige Simulation oder (polynomiell) berechenbare Reduktionen ist die Einsicht gereift, dass an der Oberfläche verschieden aussehende Konzepte im Kern identisch sein können. Zudem wurde ein tieferes Verständnis von Komplexität erreicht. Auf den unteren Ebenen der Chomsky-Hierarchie finden sich effizient lösbare Anwendungsprobleme der Textmanipulation und Textanalyse. Auf den oberen Ebenen der Hierarchie haben die Studierenden Bekanntschaft mit dem Phänomen der inhärenten Härte (oder gar Unentscheidbarkeit) eines Problems gemacht.

Inhalt:

- Grammatiken (mit Schwerpunkt auf kontextfreien Grammatiken)
- Automaten
- endliche Automaten
- Kellerautomaten
- Turing-Maschinen
- Berechenbarkeitstheorie
- NP-Vollständigkeitstheorie

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Nützlich (aber nicht zwingend erforderlich) sind elementare Grundkenntnisse in Informatik und Diskreter Mathematik sowie Vertrautheit mit mindestens einer Programmiersprache.

Arbeitsaufwand: 270 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Kontaktzeit in der Veranstaltung entspricht 84 Stunden (14 Wochen * 6 Stunden). Zur Vor- und Nachbereitung sind 126 Stunden, sowie für die Prüfungsvorbereitung 60 Stunden vorgesehen.

exam: schriftlich, 180 Minuten

Literatur:

[1] Hopcroft, John E., Motwani, Rajeev, Ullman, Jeffrey D. "Introduction to Automata Theory, Languages, and Computation", Addison Wesley Longman Publishing Co, 2001
[2] Sipser, Michael "Introduction to the Theory of Computation", Brooks Cole, 2005
[3] Schöning, Uwe "Theoretische Informatik - kurzgefasst", Spektrum Akademischer Verlag, 2001

2.85 141033: Usable Security and Privacy

number: 141033
teaching methods: lecture with integrated tutorials
media: Moodle
rechnerbasierte Präsentation
responsible person: Prof. Dr. Markus Dürmuth
lecturer: Prof. Dr. Markus Dürmuth
language: english
HWS: 3
Leistungspunkte: 4
angeboten im: summer term

dates in summer term:

Beginn: Freitag the 05.04.2019
Vorlesung Freitags: from 12:15 to 13:45 o'clock in ID 04/401
Übung Freitags: from 14:00 to 14:45 o'clock in ID 04/401

goals: 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.

content: Diese Veranstaltung vermitttelt Kenntnisse der Usable Security und Privacy. Die Themen umfassen insbesondere:

- Benutzbare Authentifizierung
- Nutzer und Phishing
- Vertrauen/ Trust, PKI, PGP
- Privatheit und Tor
- Privacy policies
- Design und Auswertung von Benutzerstudien

requirements: none

recommended knowledge: Allgemeine Kenntnisse der IT-Sicherheit

Arbeitsaufwand: 120 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 3 SWS entsprechen in Summe 42 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 22 Stunden sind für die Klausurvorbereitung vorgesehen.

exam: schriftlich, 120 Minuten

2.86 310502: Vision in Man and Machine

Nummer: 310502
Lehrform: Vorlesungen und Übungen
Medienform: Folien
Tafelanschrieb
Verantwortlicher: Priv.-Doz. Dr. Rolf P. Würtz
Dozent: Priv.-Doz. Dr. Rolf P. Würtz
Sprache: Deutsch
SWS: 3
Leistungspunkte: 5
angeboten im:

Ziele: Die Studierenden haben umfassende Kenntnisse über die Probleme, Ansätze und modernen Methoden des Computersehens, und über die Verbindungen zum menschlichen Sehen.

Inhalt: Die Vorlesung behandelt das Phänomen des Sehens aus der Sicht der Informatik, Psychophysik und Neurobiologie. Nach einer Phänomenologie des menschlichen Sehens werden die Grundlagen der Bildverarbeitung behandelt, einschließlich moderner Ansätze wie Mehrskalenverarbeitung. Dabei liegt der Schwerpunkt auf Ähnlichkeiten und Unterschieden zwischen natürlichen und künstlichen Systemen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Fouriertransformation
- Differential- und Integralrechnung

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: Die Kontaktzeit in der Veranstaltung entspricht 42 Stunden (14 Wochen * 3 Stunden). Für die Nachbereitung der Vorlesung sind etwa 2 Stunden pro Woche, in Summe 28 Stunden, erforderlich. 80 Stunden sind für die Lösung der praktischen Übungsaufgaben vorgesehen.

exam: Projektarbeit, studienbegleitend

2.87 148202: Web-Engineering

Nummer:	148202
Lehrform:	Vorlesungen und Übungen
Medienform:	e-learning rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Helmut Balzert
Dozent:	Prof. Dr.-Ing. Helmut Balzert
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	4
angeboten im:	

Ziele: Die Studierenden sind in der Lage, durchgehende Web-Anwendungen - beginnend mit HTML über JSPs, die Einbindung von Java Beans und den Anschluss an eine relationale Datenbank - zu erstellen.

Inhalt: Diese Veranstaltung gibt einen vertieften Einblick in die Programmierung von Web-Anwendungen. Ausgehend von einer Vertiefung von HTML und CSS, wird anschließend die Programmierung von JSPs und die Anbindung einer SQL-Datenbank vermittelt. Damit ist der Studierende dann in der Lage, durchgehende Web-Anwendungen - beginnend mit HTML über JSPs, die Einbindung von Java Beans und den Anschluss an eine relationale Datenbank - zu erstellen. Er lernt verschiedene Werkzeuge, Techniken, Konzepte und Programmiersprachen in Kombination einzusetzen. Zusätzlich lernt der Studierende, wie mit Hilfe der UML Web-Anwendungen modelliert werden können. Am Beispiel einer Fallstudie Web-Anzeigenmarkt lernt er statische Websites und dynamische Websites kennen. Parallel zu dieser Fallstudie soll er selbst eine Website für einen (virtuellen) Verein entwickeln. Inhaltsübersicht:

HTML, XHTML & CSS

- Von HTML zu XHTML
- CSS
- XHTML-Bilder
- XHTML-Image Maps
- XHTML-Medien
- Listen: XHTML & CSS
- CSS-Klassen
- CSS: kontextabhängige Stilregeln
- CSS: ID-Attribut
- CSS: Umrandungen
- CSS: Füllungen & Abstände
- CSS: Pseudo-Klassen & -Elemente

- XHTML: Tabellen
- XHTML: Frames
- XHTML: Formulare
- Websites: Entscheidungen

JSPs

- JSPs: Java auf dem Server
- Servlets: Basis von JSPs
- JSPs: Fehlersuche
- Zugriff auf relationale Datenbanken
- JSPs: Aufruf & Parameter
- Fallstudie Web-Anzeigenmarkt
- JSP: Implizite Objekte
- Sitzungsverfolgung
- JSP-Aktionen
- Entwurfsmuster
- JSPs: Ausblick

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Es werden grundlegende Kenntnisse in der objektorientierten Programmierung, insbesondere in der Programmiersprache Java vorausgesetzt. Diese Inhalte werden in den Vorlesungen Grundlagen der Informatik I und II vermittelt.

Arbeitsaufwand: 120 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 3 SWS ergeben 42 Stunden Anwesenheit. Parallel zur Vorlesung können wöchentlich praktische Programmieraufgaben (ca. 3 Stunden wöchentlich entsprechen 42 Stunden) abgegeben werden, die in der nachfolgenden Übung besprochen werden. Es verbleiben 36 Stunden zur Prüfungsvorbereitung.

exam: schriftlich, 120 Minuten

Literatur:

[1] Balzert, Helmut, Krüger, Sandra "HTML, XHTML & CSS, 2. Auflage", W3l, 2011
[2] Wißmann, Dieter "JavaServer Pages, 3. Auflage", W3l, 2012
[3] Balzert, Helmut "JSP JavaServer Pages. Quick Reference Map", W3l, 2003

2.88 128968: Web-Engineering

Nummer: 128968
Lehrform: Vorlesungen und Übungen
Verantwortlicher: Prof. Dr.-Ing. Markus König
Dozent: Prof. Dr.-Ing. Markus König
Sprache: Deutsch
SWS: 4
Leistungspunkte: 5
angeboten im: Sommersemester

Termine im Sommersemester:

Vorlesung Montags: ab 12:00 bis 14:00 Uhr im HGA 30
Übung Montags: ab 14:15 bis 15:45 Uhr im IC 04/630

Ziele: Link:
https://moodle.ruhr-uni-bochum.de/m/enrol/index.php?id=20278

Inhalt: Im Rahmen des Modules werden den Studierenden aktuelle Techniken und Kenntnisse im Bereich der Webentwicklung aufgezeigt. Thematisch wird der Bereich der server- und clientseitigen Entwicklung abgedeckt. JavaScript stellt dabei eine zentrale Rolle dar.
Lehrinhalte:

- HTML / CSS
- JavaScript
- jQuery
- REST
- Node.js (+Express)
- HTML5

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand errechnet sich wie folgt: 14 Wochen zu je 4 SWS ergeben 56 Stunden Anwesenheit. Es verbleiben 94 Stunden zur Vor- und Nachbereitung, sowie zur Prüfungsvorbereitung.

exam: schriftlich, 120 Minuten

2.89 148216: Wireless Security

number: 148216
teaching methods: lecture with tutorials
media: rechnerbasierte Präsentation
responsible person: Prof. Dr. Christina Pöpper
lecturer: Prof. Dr. Christina Pöpper
language: english
HWS: 4
Leistungspunkte: 5
angeboten im:

goals: Communication services and applications are increasingly leveraging the wireless medium. Given this development, the importance of information and network security in the wireless domain grows. Providing secure communication and network services in wireless environments creates challenges that often differ considerably from traditional wired systems.

The students are able to describe, classify, and assess security goals and attacks on wireless communication and in wireless networks. The students are able to describe the security architectures of different wireless systems and networks, in particular 802.11, GSM/UMTS, RFID, ad hoc and sensor networks. They will are able to reason about security protocols for wireless networks and can implement certain mechanisms to secure them.

content: The focus of this course are wireless environments such as wireless ad hoc, mesh, and sensor networks. Central elements of the course are the wireless communication channel, wireless network architectures and protocols. We will focus on the vulnerabilities, attack mechanisms as well as detection, protection and prevention techniques in wireless networks.

The course starts with wireless fundamentals and wireless channel basics. This includes jamming and modification attacks and respective countermeasures. It will then cover basic security protocols and protection mechanisms in cellular, WiFi and multi-hop networks. This will be followed by recent advances in the security of multi-hop networks. The considered techniques include security in off-the-shelf wireless technologies (such as WiFi, WiMAX, Mobile Telecommunication, RFID, Bluetooth) and in emerging wireless technologies (security in ad-hoc networks, key management, sensor networks).

requirements: none

recommended knowledge: Knowledge of the course contents of Systemsicherheit, Netzsicherheit, and Computernetze can be beneficial.

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der

Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 38 Stunden sind für die Klausurvorbereitung vorgesehen.

exam: mündlich, 30 Minuten

2.90 150232: Zahlentheorie

Nummer:	150232
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation
	Tafelanschrieb
Verantwortlicher:	Dr. Viktoriya Ozornova
Dozent:	Dr. Viktoriya Ozornova
Sprache:	Deutsch
SWS:	6
Leistungspunkte:	9
angeboten im:	Sommersemester

Termine im Sommersemester:

Vorlesung Montags: ab 12:00 bis 14:00 Uhr im HZO 70
Vorlesung Mittwochs: ab 10:00 bis 12:00 Uhr im HZO 60
Übung (alternativ) Montags: ab 14:00 bis 16:00 Uhr im IA 1/91
Übung (alternativ) Montags: ab 16:00 bis 18:00 Uhr im IA 1/135
Übung (alternativ) Dienstags: ab 08:00 bis 10:00 Uhr im IA 1/177
Übung (alternativ) Dienstags: ab 08:00 bis 10:00 Uhr im IA 1/91
Übung (alternativ) Dienstags: ab 14:00 bis 17:00 Uhr im IA 01/481
Übung (alternativ) Mittwochs: ab 14:00 bis 16:00 Uhr im IA 01/481

Ziele: Die Studierenden haben ein umfassendes Verständnis der zahlentheoretischen Grundlagen, die für die moderne Kryptologie essentiell sind.

Inhalt: Das Ziel dieser Vorlesung ist es, eine Einführung in die Zahlentheorie zu geben. Die notwendigen Hilfsmittel aus Algebra und Analysis, die nicht aus den oben zitierten Vorlesungen bekannt sind, werden in der Vorlesung bereitgestellt. Die elementare Zahlentheorie ist ein geeignetes Thema für künftige Lehrerinnen und Lehrer, da Schüler und Laien typischerweise Spass an den einfach zu formulierenden (aber nicht immer einfach zu lösenden) Fragestellungen der Zahlentheorie haben. Ausserdem ist die Zahlentheorie ein grundlegendes Werkzeug in der Kryptographie, und im Rahmen der arithmetischen Geometrie eng verwandt mit der algebraischen Geometrie. Behandelt werden insbesondere: Primfaktorzerlegung, Kongruenzen, Chinesischer Restsatz und Anwendungen, Zahlentheoretische Funktionen (z.B. die Riemannsche Zeta-Funktion), Quadratische Reste und Quadratsummen, Diophantische Gleichungen (z.B. die Pell'sche Gleichung), Kettenbrüche, Primzahlsatz.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundlegende Mathematikkenntnisse

Arbeitsaufwand: 270 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 6 SWS ergeben 84 Stunden Anwesenheit. Zur Vor- und Nachbereitung sind 126 Stunden, sowie für die Prüfungsvorbereitung 60 Stunden vorgesehen.

exam: schriftlich, 120 Minuten