UNIVERSITÄT DES SAARLANDES

Fachrichtung Informatik
Fakultät 6 – Mathematik und Informatik
Universität des Saarlandes

Modulhandbuch Cybersicherheit

Bachelor-Studiengang

11.07.2014

Modul **Grundlagen der Cybersicherheit**					Abk. **GdC**
Studiensem. **1.**	Regelstudiensem. **1.**	Turnus **Jährlich, WS**	Dauer **1 Semester**	SWS **2+2+2**	ECTS-Punkte **9**

Modulverantwortliche/r	Prof. Dr. Michael Backes
Dozent/inn/en	Prof. Dr. Michael Backes, Prof. Dr. Christian Hammer, Prof. Dr. Matteo Maffei, Prof. Dr. Dominique Schröder
Zuordnung zum Curriculum	Pflichtmodul im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	Keine
Leistungskontrollen / Prüfungen	Erfolgreiche Bearbeitung der Übungsaufgaben berechtigen zur Klausurteilnahme.
Lehrveranstaltungen / SWS	Vorlesung 2 SWS Übung 2 SWS Projekt 2 SWS
Arbeitsaufwand	Arbeitsaufwand: insgesamt 270 Stunden 40 Stunden Präsenzzeit Vorlesung, 230 Stunden Eigenstudium
Modulnote	Wird aus Leistungen in Klausuren, Übungen und praktischen Aufgaben ermittelt. Die genauen Modalitäten werden vom Modulverantwortlichen bekannt gegeben.

Lernziele/Kompetenzen
Die Studierenden kennen die Grundlagen der Kryptographie, Systemsicherheit, Netzwerksicherheit und der Abwehr von Cyberangriffen. Sie können für ausgewählte Probleme Schutzziele festlegen und sind mit den gängigen Angriffstechniken vertraut.

Inhalt	Grundlagen der Kryptographie; Grundlagen zum Schutz der Privatsphäre; Grundlagen der Systemsicherheit Grundlagen der benutzbaren Sicherheit Grundlagen der Netzwerksicherheit Grundlagen der Erkennung von Cyberangriffen Einführung in Verantwortlichkeit, Sicherheit für kritische Infrastrukturen und der frühzeitigen Erkennung von Risiken.

Weitere Informationen
Die Unterrichtssprache ist deutsch oder englisch und wird zu Beginn der Veranstaltung bekannt gegeben. Die Literatur zum Modul kann englisch- und/oder deutschsprachig sein und wird zu Beginn der Veranstaltung bekannt gegeben. Programmieraufgaben am Computer. Übungsaufgaben auf Papier und in Gruppen an der Tafel.

Modul **Mathematik für Informatiker 1**					Abk. **CS 110 / Mfl 1**
Studiensem. **1.**	Regelstudiensem. **1.**	Turnus **Jährlich, WS**	Dauer **1 Semester**	SWS **4+2**	ECTS-Punkte **9**

Modulverantwortliche/r	Prof. Dr. Joachim Weickert
Dozent/inn/en	Prof. Dr. Joachim Weickert, Prof. Dr. Frank-Olaf Schreyer
Zuordnung zum Curriculum	Pflichtmodul im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	keine
Leistungskontrollen / Prüfungen	Klausur und erfolgreiche Bearbeitung von Übungsblättern
Lehrveranstaltungen / SWS	Vorlesung *Mathematik für Informatiker 1* [CS 110 / Mfl 1], 6 SWS (9 CP)
Arbeitsaufwand	Arbeitsaufwand: insgesamt 270 Stunden 80 Stunden Präsenzzeit Vorlesung und Übung, 190 Stunden Selbststudium (Prüfungsvorbereitung)
Modulnote	Das Modul ist insgesamt bestanden, wenn die Prüfungsleistung bestanden wurde.

Lernziele/Kompetenzen

- Erarbeitung von mathematischem Grundlagenwissen, das im Rahmen eines Informatik- bzw. Cybersicherheitsstudiums benötigt wird
- Fähigkeit zur Formalisierung und Abstraktion
- Befähigung zur Aneignung weiteren mathematischen Wissens mit Hilfe von Lehrbüchern

Inhalt

Die Zahlen in den Klammern geben die Gesamtzahl der Doppelstunden an.

DISKRETE MATHEMATIK UND EINDIMENSIONALE ANALYSIS

A. Grundlagen der diskreten Mathematik (8)
   1. Mengen (1)
   2. Logik (1)
   3. Beweisprinzipien, inkl. vollständiger Induktion (1)
   4. Relationen (1)
   5. Abbildungen (2)
   6. injektiv, surjektiv, bijektiv
   7. Mächtigkeit, Abzählbarkeit
   8. Schubfachprinzip
   9. Primzahlen und Teiler (1)
   10. Modulare Arithmetik

B. Eindimensionale Analysis (22)

B.1 Zahlen, Folgen und Reihen (8)

11. Axiomatik der reellen Zahlen, sup, inf (1)
12. Komplexe Zahlen (1)
13. Folgen (1 ½)
14. Landau'sche Symbole (½)
15. Reihen: Konvergenzkriterien, absolute Konvergenz (2)
16. Potenzreihen (½)
17. Zahlendarstellungen (½)
18. Binomialkoeffizienten und Binomialreihe (1)

B.2 Eindimensionale Differentialrechnung (8)

19. Stetigkeit (1)
20. Elementare Funktionen (1)
21. Differenzierbarkeit (1 ½)
22. Mittelwertsätze und L'Hospital
23. Satz von Taylor
24. Lokale Extrema, Konvexität, Kurvendiskussion (2)
25. Numerische Differentiation (1)

B.3 Eindimensionale Integralrechnung (6)

25. Das bestimmte Integral (2)
26. Das unbestimmte Integral und die Stammfunktion (1)
27. Uneigentliche Integrale (1)
28. Numerische Verfahren zur Integration (1)
29. Kurven und Bogenlänge

Weitere Informationen

Die Unterrichtssprache ist deutsch. Die Literatur zum Modul kann englisch- und/oder deutschsprachig sein und wird zu Beginn der Veranstaltung bekannt gegeben.

Modul					Abk.
Programmierung 1					**CS 120 / P 1**
Studiensem.	Regelstudiensem.	Turnus	Dauer	SWS	ECTS-Punkte
1.	**1.**	**Jährlich, WS**	**1 Semester**	**4+2**	**9**

Modulverantwortliche/r	Prof. Dr. Gert Smolka
Dozent/inn/en	Prof. Dr. Gert Smolka, Prof. Dr.-Ing. Holger Hermanns
Zuordnung zum Curriculum	Pflichtmodul im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	keine
Leistungskontrollen / Prüfungen	• Die Leistungskontrolle setzt sich zusammen aus zwei Klausuren (Mitte und Ende der Vorlesungszeit) • Die Note wird aus den Klausuren gemittelt und kann durch Leistungen in den Übungen verbessert werden. • Eine Nachklausur findet innerhalb der letzten beiden Wochen vor Vorlesungsbeginn des Folgesemesters statt.
Lehrveranstaltungen / SWS	Vorlesung *Programmierung 1* [CS 120 / P 1], 6 SWS (9 CP)
Arbeitsaufwand	Arbeitsaufwand: insgesamt 270 Stunden 80 Stunden Präsenzzeit Vorlesung und Übung, 190 Stunden Selbststudium (Prüfungsvorbereitung)
Modulnote	Das Modul ist insgesamt bestanden, wenn die Prüfungsleistung bestanden wurde.

Lernziele/Kompetenzen

- höherstufige, getypte funktionale Programmierung anwenden können
- Verständnis rekursiver Datenstrukturen und Algorithmen, Zusammenhänge mit Mengenlehre
- Korrektheit beweisen und Laufzeit abschätzen
- Typabstraktion und Modularisierung verstehen
- Struktur von Programmiersprachen verstehen
- einfache Programmiersprachen formal beschreiben können
- einfache Programmiersprachen implementieren können
- anwendungsnahe Rechenmodelle mit maschinennahen Rechenmodellen realisieren können
- Praktische Programmiererfahrung, Routine im Umgang mit Interpretern und Übersetzern

Inhalt

- Funktionale Programmierung
- Algorithmen und Datenstrukturen (Listen, Bäume, Graphen; Korrektheitsbeweise; asymptotische Laufzeit)
- Typabstraktion und Module
- Programmieren mit Ausnahmen
- Datenstrukturen mit Zustand
- Struktur von Programmiersprachen (konkrete und abstrakte Syntax, statische und dynamische Syntax)
- Realisierung von Programmiersprachen (Interpreter, virtuelle Maschinen, Übersetzer)

Weitere Informationen

Die Unterrichtssprache ist deutsch. Die Literatur zum Modul kann englisch- und/oder deutschsprachig sein und wird zu Beginn der Veranstaltung bekannt gegeben. Übungen am Computer.

Modul **Mathematik für Informatiker 2**					Abk. **CS 210 / Mfl 2**
Studiensem. **2.**	Regelstudiensem. **2.**	Turnus **Jährlich, SS**	Dauer **1 Semester**	SWS **4+2**	ECTS-Punkte **9**

Modulverantwortliche/r	Prof. Dr. Joachim Weickert
Dozent/inn/en	Prof. Dr. Joachim Weickert, Prof. Dr. Frank-Olaf Schreyer
Zuordnung zum Curriculum	Pflichtmodul im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	Mathematik für Informatiker 1 (empfohlen)
Leistungskontrollen / Prüfungen	Klausur und erfolgreiche Bearbeitung von Übungsblättern
Lehrveranstaltungen / SWS	Vorlesung *Mathematik für Informatiker 2* [CS 210 / Mfl 2], 6 SWS (9 CP)
Arbeitsaufwand	Arbeitsaufwand: insgesamt 270 Stunden 80 Stunden Präsenzzeit Vorlesung und Übung, 190 Stunden Selbststudium (Prüfungsvorbereitung)
Modulnote	Das Modul ist insgesamt bestanden, wenn die Prüfungsleistung bestanden wurde.

Lernziele/Kompetenzen

- Erarbeitung von mathematischem Grundlagenwissen, das im Rahmen eines Informatik- bzw. Cybersicherheitsstudiums benötigt wird
- Fähigkeit zur Formalisierung und Abstraktion
- Befähigung zur Aneignung weiteren mathematischen Wissens mit Hilfe von Lehrbüchern

Inhalt

Die Zahlen in den Klammern geben die Gesamtzahl der Doppelstunden an.

ALGEBRAISCHE STRUKTUREN UND LINEARE ALGEBRA

C. Algebraische Strukturen (5)
   30. Gruppen (2)
   31. Ringe und Körper (1)
   32. Polynomringe über allgemeinen Körpern (½)
   33. Boole'sche Algebren (½)

D. Lineare Algebra (21)
   34. Vektorräume (2)
      - Def. Bsp.
      - lineare Abb.
      - Unterraum
      - Erzeugnis, lineare Abhängigkeit, Basis, Austauschsatz
   35. Lineare Abb. (Bild, Kern) (1)
   36. Matrixschreibweise für lineare Abbildungen (1 ½)
      - Interpretation als lineare Abbildungen
      - Multiplikation durch Hintereinanderausführung
      - Ringstruktur

- Inverses

37. Rang einer Matrix
38. Gauss-Algorithmus für lineare Gleichungssysteme (2)
    - Gausselimination (1)
    - Lösungstheorie (1)
39. Iterative Verfahren für lineare Gleichungssysteme (1)
40. Determinanten (1)
41. Euklidische Vektorräume, Skalarprodukt (1)
42. Funktionanalytische Verallgemeinerungen (1)
43. Orthogonalität (2)
44. Fourierreihen (1)
45. Orthogonale Matrizen (1)
46. Eigenwerte und Eigenvektoren (1)
47. Eigenwerte und Eigenvektoren symmetrischer Matrizen (1)
48. Quadritische Formen und passiv definite Matrizen (1)
49. Quadriken (1)
50. Matrixnormen und Eigenwertabschätzungen (1)
51. Numerische Berechnung von Eigenwerten und Eigenvektoren (1)

Weitere Informationen
Die Unterrichtssprache ist deutsch. Die Literatur zum Modul kann englisch- und/oder deutschsprachig sein und wird zu Beginn der Veranstaltung bekannt gegeben.

Modul **Programmierung 2**					Abk. **CS 220 / P 2**
Studiensem. **2.**	Regelstudiensem. **2.**	Turnus **Jährlich, SS**	Dauer **1 Semester**	SWS **4+2**	ECTS-Punkte **9**

Modulverantwortliche/r	Prof. Dr. Sebastian Hack
Dozent/inn/en	Prof. Dr. Andreas Zeller, Prof. Dr. Sebastian Hack
Zuordnung zum Curriculum	Pflichtmodul im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	Programmierung 1 (empfohlen)
Leistungskontrollen / Prüfungen	Prüfungsleistungen werden in zwei Teilen erbracht, die zu gleichen Teilen in die Endnote eingehen. Um die Gesamtveranstaltung zu bestehen, muss jeder Teil einzeln bestanden werden. Im **Praktikumsteil** müssen die Studierenden eine Reihe von Programmieraufgaben selbstständig implementieren. Diese Programmieraufgaben ermöglichen das Einüben der Sprachkonzepte und führen außerdem komplexere Algorithmen und Datenstrukturen ein. Automatische Tests prüfen die Qualität der Implementierungen. Die Note des Praktikumsteils wird maßgeblich durch die Testergebnisse bestimmt. Im **Vorlesungsteil** müssen die Studierenden Klausuren absolvieren und Übungsaufgaben bearbeiten. Die Aufgaben vertiefen dabei den Stoff der Vorlesung. Die Zulassung zu der Klausur hängt von der erfolgreichen Bearbeitung der Übungsaufgaben ab. Im Praktikumsteil kann eine Nachaufgabe angeboten werden
Lehrveranstaltungen / SWS	Vorlesung *Programmierung 2* [CS 220 / P 2], 6 SWS (9 CP)
Arbeitsaufwand	Arbeitsaufwand: insgesamt 270 Stunden 45 Stunden Präsenzzeit Vorlesung und Übung, 225 Stunden Selbststudium (Prüfungsvorbereitung)
Modulnote	Das Modul ist insgesamt bestanden, wenn die Prüfungsleistung bestanden wurde.

Lernziele/Kompetenzen

Die Studierenden lernen die Grundprinzipien der imperativen /objektorientierten Programmierung kennen. Dabei wird primär Java als Programmiersprache verwendet. Die Veranstaltung beinhaltet folgende Lernziele:

- mittelgroße objektorientierte Systeme in Java zu implementieren und zu testen
- kleinere, wohlstrukturierte Programme in C++ zu schreiben - im Wesentlichen als Umsetzung/Übersetzung der entsprechenden Java-Konzepte
- sich in wenigen Tagen eine neue imperative/objektorientierte Sprache anzueignen, um sich in ein bestehendes Projekt einzuarbeiten

Inhalt

- Objekte und Klassen
- Klassendefinitionen
- Objektinteraktion

- Objektsammlungen
- Objekte nutzen und testen
- Vererbung
- Dynamische Bindung
- Fehlerbehandlung
- Graphische Oberflächen
- Klassendesign und Modularität
- Objekte in C++
- Systemnahme Programmierung

Weitere Informationen
Die Unterrichtssprache ist deutsch. Die Literatur zum Modul kann englisch- und/oder deutschsprachig sein und wird zu Beginn der Veranstaltung bekannt gegeben. Programmieraufgaben am Computer. Übungsaufgaben auf Papier und in Gruppen an der Tafel.

Modul **Secure Software Engineering**					Abk. **XXX**
Studiensem. **2.**	Regelstudiensem. **2.**	Turnus **Jährlich, SS**	Dauer **1 Semester**	SWS **2+2**	ECTS-Punkte **6**

Modulverantwortliche/r	Prof. Dr. Matteo Maffei
Dozent/inn/en	Prof. Dr. Matteo Maffei, Prof. Dr. Christian Hammer
Zuordnung zum Curriculum	Pflichtmodul im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	keine
Leistungskontrollen / Prüfungen	Klausur und erfolgreiche Bearbeitung von Übungsblättern
Lehrveranstaltungen / SWS	Vorlesung *Secure Software Engineering* [XXX], 4 SWS (6 CP)
Arbeitsaufwand	Arbeitsaufwand: insgesamt 180 Stunden 60 Stunden Präsenzzeit Vorlesung und Übung, 60 Vor- und Nachbereitung, 60 Stunden Selbststudium (Prüfungsvorbereitung)
Modulnote	Das Modul ist insgesamt bestanden, wenn die Prüfungsleistung bestanden wurde.

Lernziele/Kompetenzen

Die Studierenden haben nach Ende der Veranstaltung ein profundes Verständnis von Methoden, Tools und besten Vorgehensweisen, um sicheren Programmcode zu schreiben.

Inhalt

- Threat-Modellierung und Schwachstellenanalyse
- Spezifikation und Management von Sicherheitsvoraussetzungen und –policies
- Sicherheitsarchitektur und Design von Software und Systemen
- Spezifikationsformalismen für Sicherheitsartefakte
- Verifikationstechniken für Sicherheitseigenschaften
- Systematische Unterstützung für beste Sicherheitspraktiken
- Sicherheitstesten
- Fälle von Sicherheitszusicherungen
- Programmiermuster, Modelle und DSL's für Sicherheit
- Techniken zur Programmrefaktorisierung
- Prozesse zur Entwicklung von sicherer Software und sicheren Systemen
- Sicherheitsorientierte Software-Rekonfiguration und –Evolution
- Sicherheitsbewertung
- Automatisierte Entwicklung
- Abwägen von Sicherheit und anderen nicht-funktionalen Voraussetzungen (insbesondere wirtschaftliche Überlegungen)
- Unterstützung für Zusicherung, Zertifizierung und Akkreditierung
- Empirisch sichere Softwareentwicklung
- Security by Design

Weitere Informationen

Die Unterrichtssprache ist deutsch oder englisch und wird zu Beginn der Veranstaltung bekannt gegeben. Die Literatur zum Modul kann englisch- und/oder deutschsprachig sein und wird zu Beginn der Veranstaltung bekannt gegeben.

Modul **Systemarchitektur**					Abk. **CS 230 / SysArch**
Studiensem.	Regelstudiensem.	Turnus	Dauer	SWS	ECTS-Punkte
2.	**2.**	**Jährlich, SS**	**1 Semester**	**4+2**	**9**

Modulverantwortliche/r	Prof. Dr. W.-J. Paul
Dozent/inn/en	Prof. Dr. W.-J. Paul
Zuordnung zum Curriculum	Pflichtmodul im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	Programmierung 1 und Mathematik für Informatiker 1 (empfohlen)
Leistungskontrollen / Prüfungen	Studienleistungen: die Vorlesungen hören, nach bearbeiten und gegebenenfalls verstehen; die Übungen allein oder in Gruppen bearbeiten; erfolgreich bearbeitete Übungen in der Übungsgruppe vortragen. Prüfungsleistungen: erfolgreiche Bearbeitung von 50 % der Übungsaufgaben berechtigt zur Teilnahme an den Klausuren. Bestehen von zwei aus drei Klausuren.
Lehrveranstaltungen / SWS	Vorlesung *Systemarchitektur* [CS 230 / SysArch], 6 SWS (9 CP) Übungsgruppen mit bis zu 20 Studierenden
Arbeitsaufwand	270 h = 80 h Präsenz- und 190 h Eigenstudium
Modulnote	Wird aus Leistungen in Klausuren, Übungen und praktischen Aufgaben ermittelt. Die genauen Modalitäten werden vom Modulverantwortlichen bekannt gegeben.

Lernziele / Kompetenzen

Die Studierenden sollen die Funktionsweise, die Eigenschaften und die Entwurfsprinzipien von Rechnerarchitekturen und Betriebssystemen kennen lernen.

Inhalt

1. Hardware
    a. Boole'sche Algebra und Schaltkreise
    b. Elementare Rechnerarithmetik
    c. ALU (Konstruktion und Korrektheit)
    d. Sequentieller vereinfachter DLX-Prozessor (Konstruktion und Korrektheit)
2. Betriebssystemkern
    a. Virtualisierung
    b. Ressourcen-Verwaltung, Speicher, Prozessor
    c. Scheduling
    d. Datei-System

Weitere Informationen

Die Unterrichtssprache ist deutsch. Die Literatur zum Modul kann englisch- und/oder deutschsprachig sein und wird zu Beginn der Veranstaltung bekannt gegeben.

Modul **Cryptography**					Abk. **CS 578 / CRY**
Studiensem. **3.**	Regelstudiensem. **3.**	Turnus **Jährlich, WS**	Dauer **1 Semester**	SWS **4+2**	ECTS-Punkte **9**

Modulverantwortliche/r	Prof. Dr. Michael Backes
Dozent/inn/en	Prof. Dr. Michael Backes, Prof. Dr. Dominique Schröder
Zuordnung zum Curriculum	Pflichtmodul im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	Grundzüge der Theoretischen Informatik, Mathematik für Informatiker 1 und 2 (empfohlen)
Leistungskontrollen / Prüfungen	Schriftliche oder mündliche Abschlussprüfung über das gesamte Themengebiet
Lehrveranstaltungen / SWS	Vorlesung *Cryptography* [CS 578 / CRY], 6 SWS (9 CP)
Arbeitsaufwand	Vorlesung 4 SWS Übung 2 SWS Übungsgruppen mit bis zu 20 Studierenden 270 h = 90 h Präsenz- und 180 h Prüfungsvorbereitung
Modulnote	Wird aus Leistungen in Klausuren, Übungen und praktischen Aufgaben ermittelt. Die genauen Modalitäten werden vom Modulverantwortlichen bekannt gegeben. Eigenstudium

Lernziele/Kompetenzen

Die Studierende verstehen die grundlegenden Konzepte der Kryptographie, sie verstehe formale Definitionen und können die Sicherheit von grundlegenden Verfahren beweisen.

Inhalt

- Symmetrische und asymmetrische Verschlüsselung
- Digital Unterschriften und Message Authentication Codes
- Informationstheoretische und Komplexitätstheoretische Sicherheitsdefinitionen, Kryptographische Reduktionsbeweise
- Kryptographische Modelle wie das Random Oracle Model
- Kryptographische Primitive wie z.B. Trapdoor-one-way Funktionen, Pseudozufallsgeneratoren, etc.
- Kryptographie in der Practice (Standards, Produkte)
- Ausgewählte Themen der aktuellen Forschung

Weitere Informationen

Die Unterrichtssprache ist englisch. Die Literatur zum Modul kann englisch- und/oder deutschsprachig sein und wird zu Beginn der Veranstaltung bekannt gegeben.

Modul **Softwaredesignpraktikum**					Abk. **CS 320 / SoDePra**
Studiensem. **3.**	Regelstudiensem. **3.**	Turnus **Jährlich, WS**	Dauer **1 Semester**	SWS **1+1+4**	ECTS-Punkte **9**

Modulverantwortliche/r	Prof. Dr. Andreas Zeller
Dozent/inn/en	Prof. Dr. Andreas Zeller, Prof. Dr. Philipp Slusallek, Prof. Dr. Holger Hermanns
Zuordnung zum Curriculum	Pflichtmodul im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	Programmierung 1 +2 (empfohlen)
Leistungskontrollen / Prüfungen	Erfolgreiches Erstellen eines komplexen Software-Produkts im Team, insbesondere • Einreichen der erforderlichen Dokumente • Abnahme des Endprodukts durch den Kunden • Einhaltung der Termin- und Qualitätsstandards
Lehrveranstaltungen / SWS	Praktikum *Softwaredesignpraktikum* [CS 320 / SoDePra], 6 SWS (9 CP)
Arbeitsaufwand	Arbeitsaufwand: insgesamt 270 Stunden 20 Stunden Präsenzzeit Vorlesung, 250 Stunden Selbststudium (Übungen und Prüfungsvorbereitung)
Modulnote	Das Modul ist insgesamt bestanden, wenn die Prüfungsleistung bestanden wurde.

Lernziele/Kompetenzen

Die Studierenden erwerben die Fähigkeit, im Team zu arbeiten und Probleme der Informatik zu lösen.
Die Studierenden wissen, welche Probleme beim Durchführen eines Software-Projekts auftreten können, und wie man damit umgeht.
Sie können eine komplexe Aufgabenstellung eigenständig in ein Software-Produkt umsetzen, das den Anforderungen des Kunden entspricht. Hierfür wählen sie einen passenden Entwicklungsprozess, der Risiken früher erkannt und minimiert, und wenden diesen an.
Sie sind vertraut mit Grundzügen des Software-Entwurfs wie schwache Kopplung, hohe Kohäsion, Geheimnisprinzip sowie Entwurfs- und Architekturmustern und sind in der Lage, einen Entwurf anhand dieser Kriterien zu erstellen, zu beurteilen und zu verbessern.
Sie beherrschen Techniken der Qualitätssicherung wie Testen und Gegenlesen und wenden diese an.

Inhalt

Software-Entwurf (objektorientierter Entwurf mit UML)
Software-Prozesse (Wasserfall, inkrementelles Modell, agile Modelle)
Projektplanung und -durchführung
Qualitätssicherung
Programmierwerkzeuge (Versionskontrolle, Konstruktion, Test, Fehlersuche)

Weitere Informationen

Die Unterrichtssprache ist deutsch. Die Literatur zum Modul kann englisch- und/oder deutschsprachig sein und wird zu Beginn der Veranstaltung bekannt gegeben. Die Veranstaltung findet in der vorlesungsfreien Zeit statt.

Modul **Grundzüge der Theoretischen Informatik**					Abk. **CS 420 / TheoInf**
Studiensem. **3.**	Regelstudiensem. **3.**	Turnus **Jährlich, WS**	Dauer **1 Semester**	SWS **4+2**	ECTS-Punkte **9**

Modulverantwortliche/r	Prof. Dr. Raimund Seidel
Dozent/inn/en	Prof. Dr. Bernd Finkbeiner, Prof. Dr. Kurt Mehlhorn, Prof. Dr. W.J. Paul, Prof. Dr. Raimund Seidel, Prof. Dr. Reinhard Wilhelm, Prof. Dr. Markus Bläser
Zuordnung zum Curriculum	Pflichtmodul im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	Programmierung 1 und 2, Mathematik für Informatiker 1 und 2 (empfohlen)
Leistungskontrollen / Prüfungen	Erfolgreiche Bearbeitung der Übungsaufgaben berechtigt zur Klausurteilnahme.
Lehrveranstaltungen / SWS	Vorlesung 4 SWS Übung 2 SWS Übungsgruppen mit bis zu 20 Studierenden
Arbeitsaufwand	270 h = 80 h Präsenz- und 190 h Eigenstudium
Modulnote	Wird aus Leistungen in Klausuren, Übungen und praktischen Aufgaben ermittelt. Die genauen Modalitäten werden vom Modulverantwortlichen bekannt gegeben.

Lernziele / Kompetenzen

Die Studierenden kennen verschiedene Rechenmodelle und ihre relativen Stärken und Mächtigkeiten. Sie können für ausgewählte Probleme zeigen, ob diese in bestimmten Rechenmodellen lösbar sind oder nicht.
Sie verstehen den formalen Begriff der Berechenbarkeit wie auch der Nicht-Berechenbarkeit.
Sie können Probleme aufeinander reduzieren.
Sie sind vertraut mit den Grundzügen der Ressourcenbeschränkung (Zeit, Platz) für Berechnungen und der sich daraus ergebenden Komplexitätstheorie.

Inhalt	Die Sprachen der Chomsky Hierarchie und ihre verschiedenen Definitionen über Grammatiken und Automaten; Abschlusseigenschaften; Klassifikation von bestimmten Sprachen („Pumping lemmas“); Determinismus und Nicht-Determinismus; Turing Maschinen und äquivalente Modelle von allgemeiner Berechenbarkeit (z.B. µ-rekursive Funktionen, Random Access Machines) Reduzierbarkeit, Entscheidbarkeit, Nicht-Entscheidbarkeit; Die Komplexitätsmaße Zeit und Platz; die Komplexitätsklassen P und NP; Grundzüge der Theorie der NP-Vollständigkeit

Weitere Informationen

Die Unterrichtssprache ist deutsch. Die Literatur zum Modul kann englisch- und/oder deutschsprachig sein und wird zu Beginn der Veranstaltung bekannt gegeben.

Modul **Grundzüge von Algorithmen und Datenstrukturen**					Abk. **CS 340 / GrADS**
Studiensem. **3.**	Regelstudiensem. **3.**	Turnus **Jährlich, WS**	Dauer **1 Semester**	SWS **2+2**	ECTS-Punkte **6**

Modulverantwortliche/r	Prof. Dr. Raimund Seidel
Dozent/inn/en	Prof. Dr. Markus Bläser, Prof. Dr. Kurt Mehlhorn, Prof. Dr. Raimund Seidel
Zuordnung zum Curriculum	Pflichtmodul im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	Programmierung 1 +2 u. Mathematik für Informatiker 1 +2 (empfohlen)
Leistungskontrollen / Prüfungen	Klausur und erfolgreiche Bearbeitung von Übungsblättern
Lehrveranstaltungen / SWS	Vorlesung *Algorithmen und Datenstrukturen* [CS 340 / GrADS], 4 SWS (6 CP)
Arbeitsaufwand	Arbeitsaufwand: insgesamt 180 Stunden 60 Stunden Präsenzzeit Vorlesung und Übung, 120 Stunden Selbststudium (Prüfungsvorbereitung)
Modulnote	Das Modul ist insgesamt bestanden, wenn die Prüfungsleistung bestanden wurde. [benotet]

Lernziele/Kompetenzen

Die Studierenden lernen die wichtigsten Methoden des Entwurfs von Algorithmen und Datenstrukturen kennen: Teile-und-Herrsche, Dynamische Programmierung, inkrementelle Konstruktion, „Greedy“, Dezimierung, Hierarchisierung, Randomisierung. Sie lernen Algorithmen und Datenstrukturen bzgl. Zeit- und Platzverbrauch für das übliche RAM Maschinenmodell zu analysieren und auf Basis dieser Analysen zu vergleichen. Sie lernen verschiedene Arten der Analyse (schlechtester Fall, amortisiert, erwartet) einzusetzen.
Die Studierenden lernen wichtige effiziente Datenstrukturen und Algorithmen kennen. Sie sollen die Fähigkeit erwerben, vorhandene Methoden durch theoretische Analysen und Abwägungen für ihre Verwendbarkeit in tatsächlich auftretenden Szenarien zu prüfen. Ferner sollen die Studierenden die Fähigkeit trainieren, Algorithmen und Datenstrukturen unter dem Aspekt von Performanzgarantien zu entwickeln oder anzupassen.

Inhalt

siehe Lernziele/Kompetenzen.

Weitere Informationen

Die Unterrichtssprache ist deutsch. Die Literatur zum Modul kann englisch- und/oder deutschsprachig sein und wird zu Beginn der Veranstaltung bekannt gegeben.

Modul **Proseminar**					Abk. **CS 300**
Studiensem. **4.**	Regelstudiensem. **4.**	Turnus **Jährlich, SS+WS**	Dauer **1 Semester**	SWS **2**	ECTS-Punkte **5**

Modulverantwortliche/r	Studiendekan der Fakultät Mathematik und Informatik bzw. Studienbeauftragter der Informatik
Dozent/inn/en	Professoren der Fachrichtung
Zuordnung zum Curriculum	Wahlpflichtmodul im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	keine
Leistungskontrollen / Prüfungen	• Diskussion in der Gruppe • thematischer Vortrag • kurze schriftliche Ausarbeitung
Lehrveranstaltungen / SWS	Seminar *Proseminar* [CS 300], 2 SWS (5 CP)
Arbeitsaufwand	Arbeitsaufwand: insgesamt 150 Stunden 40 Stunden Präsenzzeit, 110 Stunden Selbststudium
Modulnote	Das Modul ist insgesamt bestanden, wenn die Prüfungsleistung bestanden wurde.

Lernziele/Kompetenzen

Die Studierenden haben am Ende der Veranstaltung ein profundes Verständnis aktueller oder fundamentaler Aspekte eines spezifischen Teilbereiches der Informatik erlangt.
Sie haben Kompetenz im Verstehen einfacher wissenschaftlicher Aufsätze und im Präsentieren von wissenschaftlichen Erkenntnissen erworben.

Inhalt

Praktisches Einüben unter Anleitung von

- Lesen und Verstehen wissenschaftlicher Aufsätze
- Diskutieren der Aufsätze in der Gruppe
- Analysieren, Zusammenfassen und Wiedergeben des spezifischen Themas
- Präsentationstechnik

Spezifische Vertiefung in Bezug auf das individuelle Thema des Seminars.

Weitere Informationen

Die Unterrichtssprache ist deutsch. Die Literatur zum Modul kann englisch- und/oder deutschsprachig sein und wird zu Beginn der Veranstaltung bekannt gegeben. Wechselnde Titel je nach Thema.

Modul **Security**					Abk. **CS 559 / SEC**
Studiensem. **4.**	Regelstudiensem. **4.**	Turnus **Jährlich, SS**	Dauer **1 Semester**	SWS **4+2**	ECTS-Punkte **9**

Modulverantwortliche/r	Prof. Dr. Matteo Maffei
Dozent/inn/en	Prof. Dr. Michael Backes, Prof. Dr. Christian Hammer, Prof. Dr. Matteo Maffei
Zuordnung zum Curriculum	Pflichtmodul im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	Programmierung 1 und 2 (empfohlen)
Leistungskontrollen / Prüfungen	Regelmäßige Teilnahme an den Vorlesungen und Übungen. Abschließende Klausur.
Lehrveranstaltungen / SWS	Vorlesung 4 SWS Übung 2 SWS Übungsgruppen mit bis zu 20 Studierenden
Arbeitsaufwand	270 h = 90 h Präsenz- und 180 h Prüfungsvorbereitung
Modulnote	Wird aus Leistungen in Klausuren, Übungen und praktischen Aufgaben ermittelt. Die genauen Modalitäten werden vom Modulverantwortlichen bekannt gegeben.

Lernziele / Kompetenzen

The students will acquire a deep understanding and hands-on experience on a broad spectrum of attack and defense techniques for IT systems.

Inhalt

- Security principles
- Authentication and access control
- Network security
- Operating system security
- Web application security
- Malware
- Risk management
- Logging and log analysis
- Cryptographic protocols
- Security of information flow

Weitere Informationen

The teaching language is English. The teaching material will be in English and it will consist of slides as well as book chapters.

Modul **Informationssysteme**					Abk. **CS 330 / InfoSys**
Studiensem. **4.**	Regelstudiensem. **4.**	Turnus **Jährlich, SS**	Dauer **1 Semester**	SWS **2+2**	ECTS-Punkte **6**

Modulverantwortliche/r	Prof. Dr. Jens Dittrich
Dozent/inn/en	Prof. Dr. Jens Dittrich
Zuordnung zum Curriculum	Pflichtmodul im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	keine
Leistungskontrollen / Prüfungen	Erfolgreiche Teilnahme an den Übungen berechtigt zur Teilnahme an der Abschlußklausur (bzw. Studienarbeit).
Lehrveranstaltungen / SWS	Vorlesung *Informationssysteme* [CS 330 / InfoSys], 4 SWS (6 CP)
Arbeitsaufwand	Arbeitsaufwand: insgesamt 180 Stunden 80 Stunden Präsenzzeit Vorlesung und Übung, 100 Stunden Selbststudium (Prüfungsvorbereitung)
Modulnote	Das Modul ist insgesamt bestanden, wenn die Prüfungsleistung bestanden wurde.

Lernziele/Kompetenzen

Die Vorlesung vermittelt grundlegende Kenntnisse über Konzepte und Schnittstellen von Datenbanksystemen und anderen Arten von Informationsdienstsoftware sowie der Anwendungsentwicklungswerkzeuge zur Realisierung von Informationssystemen. Besonderes Augenmerk wird auf die logische Ebene des ANSI 3-Schichtenmodells gelegt.

Inhalt

Schwerpunktthemen sind:

- Datenmodelle (relational, hierarchisch, graphisch)
- Alternative Datenrepräsentationen (XML, RDF, JSON)
- Datenbankarchitekturen (2-tier, 3-tier, 4-tier, Parallel, P2P, Cloud)
- Datenbankentwurf (der Weg vom realen Problem zur Datenbank)
- Entity Relationship-Modellierung (die Welt abbilden auf ER-Diagramme)
- Relationales Modell (ER-Diagramme abbilden auf Relationen)
- Relationale Algebra (Mengenorientierte Operationen auf dem Relationen Modell)
- Tabellen (Relationen abbilden auf Tabellen in einem DBMS)
- SQL (Mengenorientierte Operationen auf Tabellen)
- Integritätsbedingungen (Zusätzliche Verbesserung der Konsistenz von Daten)
- Relationale Entwurfstheorie (Vermeidung der Redundanz von Daten)
- Transaktionsverwaltung (Zusammenfassen von Operationen)
- Synchronisation (Nebenläufigkeit von Transaktionen)
- Übersicht über physische Organisation eines DBMS (Implementierung und Effizienz eines DBMS)
- Alternative Systeme zur Datenverarbeitung (Suchmaschinen, NoSQL, MapReduce, etc.)
- Datenbankkonnektivität zu Programmiersprachen (JDBC)
- Applikationsserver
- Datenbanken und Clouds

Die notwendigen Grundlagen werden in der Vorlesung eingeführt.

Weitere Informationen
Die Unterrichtssprache ist deutsch. Die Literatur zum Modul kann englisch- und/oder deutschsprachig sein und wird zu Beginn der Veranstaltung bekannt gegeben.

Modul **Nebenläufige Programmierung**					Abk. **CS 430**
Studiensem. **4.**	Regelstudiensem. **4.**	Turnus **Jährlich, SS**	Dauer **1 Semester**	SWS **2+2**	ECTS-Punkte **6**

Modulverantwortliche/r	Prof. Dr. Holger Hermanns
Dozent/inn/en	Prof. Dr. Holger Hermanns Prof. Dr. Gert Smolka Prof. Bernd Finkbeiner, PhD
Zuordnung zum Curriculum	Pflichtmodul im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	Programmierung 1 [CS 120 / P 1] & Programmierung 2 [CS 220 / P 2], Softwaredesignpraktikum [CS 320 / SoDePra], Theoretische Informatik [CS 420 / TheoInf] (empfohlen)
Leistungskontrollen / Prüfungen	Zwei Klausuren (Mitte und Ende der Vorlesungszeit), praktisches Projekt.
Lehrveranstaltungen / SWS	Vorlesung *Nebenläufige Programmierung* [CS 430], 4 SWS (6 CP)
Arbeitsaufwand	Arbeitsaufwand: insgesamt 180 Stunden 80 Stunden Präsenzzeit Vorlesung und Übung, 100 Stunden Selbststudium (Prüfungsvorbereitung)
Modulnote	Das Modul ist insgesamt bestanden, wenn die Prüfungsleistung bestanden wurde.

Lernziele/Kompetenzen

Die Teilnehmer lernen die Nebenläufigkeit von Prozessen als ein weitreichendes, grundlegendes Prinzip in der Theorie und Praxis der modernen Informatik kennen. Durch die Untersuchung und Verwendung unterschiedlicher formaler Modelle gewinnen die Teilnehmer ein vertieftes Verständnis von Nebenläufigkeit. Dabei lernen die Teilnehmer wichtige formale Konzepte der Informatik korrekt anzuwenden. Das im ersten Teil der Veranstaltung erworbene theoretische Wissen wird in der zweiten Hälfte in der (Programmier-) Praxis angewendet. Dabei lernen die Teilnehmer verschiedene Phänomene des nebenläufigenden Programmierens in den formalen Modellen zu beschreiben und mit deren Hilfe konkrete Lösungen für die Praxis abzuleiten. Des Weiteren werden die Teilnehmer in der Praxis existierende Konzepte auf diese Art auf ihre Verlässlichkeit hin untersuchen.

Inhalt

Nebenläufigkeit als Konzept

- Potentieller Parallelismus
- Tatsächlicher Parallelismus
- Konzeptioneller Parallelismus

Nebenläufigkeit in der Praxis

- Objektorientierung
- Betriebssysteme
- Multi-core Prozessoren, Coprozessoren
- Programmierte Parallelität
- Verteilte Systeme (client-server, peer-2-peer, Datenbanken, Internet)

Die Schwierigkeit von Nebenläufigkeit
- Ressourcenkonflikte
- Fairness
- Gegenseitiger Auschluss
- Verklemmung (Deadlock)
- gegenseitige Blockaden (Livelock)
- Verhungern (Starvation)

Grundlagen der Nebenläufigkeit
- Sequentielle Prozesse
- Zustaende, Ereignisse und Transitionen
- Transitionssysteme
- Beobachtbares Verhalten
- Determinismus vs. Nicht-Determinismus
- Algebren und Operatoren

CCS: Der Kalkül kommunizierender Prozesse
- Konstruktion von Prozessen: Sequenz, Auswahl, Rekursion
- Nebenläufigkeit
- Interaktion
- Strukturelle operationelle Semantik
- Gleichheit von Beobachtungen
- Implementierungsrelationen
- CCS mit Datentransfer

Programmieren von Nebenläufigkeit
Java vs. C++
- Objekte in Java
- Sockets, Protokolle, Datenstroeme in Java
- Shared Objects und Threads in Java
- Shared Objects und Threads als Transitionssysteme
- Monitore und Semaphoren

Analyse und Programmierunterstützung
- Erkennung von Verklemmungen
- Zusicherung von Sicherheit und Lebendigkeit
- Model-Basiertes Design von Nebenläufigkeit
- Software Architekturen für Nebenläufigkeit

Weitere Informationen
Die Unterrichtssprache ist deutsch oder englisch. Die Literatur zum Modul kann englisch- und/oder deutschsprachig sein und wird zu Beginn der Veranstaltung bekannt gegeben.

Modul **Cybersicherheitsprojekt**					Abk. **XXX**
Studiensem.	Regelstudiensem.	Turnus	Dauer **1 Semester**	SWS **1+1+4**	ECTS-Punkte **9**

Modulverantwortliche/r	Prof. Dr. Michael Backes
Dozent/inn/en	Prof. Dr. Michael Backes, Prof. Dr. Christian Hammer, Prof. Dr. Matteo Maffei, Prof. Dr. Dominique Schröder
Zuordnung zum Curriculum	Wahlpflichtmodul im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	Grundlegende Kenntnisse im jeweiligen Teilbereich der Informatik.
Leistungskontrollen / Prüfungen	Projektarbeit, Projektdokumentation, Projektpräsentation
Lehrveranstaltungen / SWS	Vorlesung 2 SWS Praktikum 4 SWS (Teams in Gruppe bis zu 6 Studierenden)
Arbeitsaufwand	Arbeitsaufwand: insgesamt 270 Stunden 20 Stunden Präsenzzeit, 250 Stunden Selbststudium
Modulnote	Das Modul ist insgesamt bestanden, wenn die Prüfungsleistung bestanden wurde.

Lernziele/Kompetenzen

Die Studierenden erwerben die Fähigkeit, im Team zu arbeiten und Probleme der Cybersicherheit zu lösen.

Die Studierenden wissen, welche sicherheitskritischen Probleme auftreten können, und wie man damit umgeht.

Sie sind vertraut mit Grundzügen der Cybersicherheit wie den grundlegenden kryptographischen Primitiven, der Schutz der Privatsphäre und der Systemsicherheit, sie können Cyberangriffe erkennen und entsprechende Maßnahmen treffen.

Inhalt

Siehe Lernziele/Kompetenzen

Weitere Informationen

Die Unterrichtssprache ist deutsch oder englisch und wird zu Beginn der Veranstaltung bekannt gegeben. Die Literatur zum Modul kann englisch- und/oder deutschsprachig sein und wird zu Beginn der Veranstaltung bekannt gegeben.

Modul **Seminar**					Abk. **CS 500**
Studiensem. **5.**	Regelstudiensem. **5.**	Turnus **Jährlich, WS+SS**	Dauer **1 Semester**	SWS **3**	ECTS-Punkte **7**

Modulverantwortliche/r	Studiendekan der Fakultät Mathematik und Informatik bzw. Studienbeauftragter der Informatik
Dozent/inn/en	Professoren der Fachrichtung
Zuordnung zum Curriculum	Wahlpflichtmodul im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	Grundlegende Kenntnisse im jeweiligen Teilbereich der Informatik.
Leistungskontrollen / Prüfungen	• Beiträge zur Diskussion • Thematischer Vortrag • Schriftliche Ausarbeitung • Mündliche Abschlussprüfung über das gesamte Themengebiet
Lehrveranstaltungen / SWS	*Seminar* [CS 500], 3 SWS (7 CP)
Arbeitsaufwand	Arbeitsaufwand: insgesamt 210 Stunden 60 Stunden Präsenzzeit, 150 Stunden Selbststudium
Modulnote	Das Modul ist insgesamt bestanden, wenn die Prüfungsleistung bestanden wurde.

Lernziele/Kompetenzen

Die Studierenden haben am Ende der Veranstaltung ein tiefes Verständnis aktueller oder fundamentaler Aspekte eines spezifischen Teilbereiches der Informatik erlangt.
Sie haben Kompetenz im eigenständigen wissenschaftlichen Recherchieren, Einordnen, Zusammenfassen, Diskutieren, Kritisieren und Präsentieren von wissenschaftlichen Erkenntnissen gewonnen.

Inhalt

Praktisches Einüben von

- reflektierender wissenschaftlicher Arbeit,
- Analyse und Bewertung wissenschaftlicher Aufsätze,
- Verfassen eigener wissenschaftlicher Zusammenfassungen
- Diskussion der Arbeiten in der Gruppe
- Erarbeiten gemeinsamer Standards für wissenschaftliche Arbeiten
- Präsentationstechnik

Spezifische Vertiefung in Bezug auf das individuelle Thema des Seminars.
Der typische Ablauf eines Seminars ist wie folgt:

- Vorbereitende Gespräche zur Themenauswahl
- Regelmäßige Treffen mit Diskussion ausgewählter Beiträge
- Vortrag und Ausarbeitung zu einem der Beiträge
- Mündliche Prüfung über das erarbeitete Themengebiet

Weitere Informationen

Die Unterrichtssprache ist deutsch oder englisch. Die Literatur zum Modul kann englisch- und/oder deutschsprachig sein und wird zu Beginn der Veranstaltung bekannt gegeben. Wechselnde Titel je nach Thema.

Modul **Privacy Enhancing Technology**					Abk. **PET**
Studiensem.	Regelstudiensem.	Turnus	Dauer **1 Semester**	SWS **2+2**	ECTS-Punkte **6**

Modulverantwortliche/r	Prof. Dr. Matteo Maffei
Dozent/inn/en	Prof. Dr. Matteo Maffei, Prof. Dr. Backes
Zuordnung zum Curriculum	Wahlpflicht I im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	Security
Leistungskontrollen / Prüfungen	Schriftliche oder mündliche Abschlussprüfung über das gesamte Themengebiet
Lehrveranstaltungen / SWS	Vertiefungsvorlesung Privacy Enhancing Technology, 4 SWS (6 CP)
Arbeitsaufwand	Arbeitsaufwand: insgesamt 180 Stunden 80 Stunden Präsenzzeit Vorlesung und Übung, 100 Stunden Selbststudium (Prüfungsvorbereitung)
Modulnote	Das Modul ist insgesamt bestanden, wenn die Prüfungsleistung bestanden wurde.

Lernziele/Kompetenzen

The students will acquire a comprensive knowledge of the privacy threats in the digital society, a deep understanding of the theoretical foundations of information privacy, and hands-on experience on the state-of-the-art in privacy-enhancing technologies.

Inhalt

- Privacy in databases
- Privacy in web services
- Privacy in cloud computing
- Privacy in e-cash
- Privacy in e-voting
- Anonymous communication networks
- Censorship circumvention techniques
- Trusted Computing
- Private information retrieval
- Oblivious protocols
- Zero knowledge proofs and privacy-preserving credentials
- Practical secure multiparty computation

Weitere Informationen
The teaching language is English. The teaching material will be in English and it will consist of slides and papers from the literature.

Modul **Advanced Cryptography**					Abk. **AC**
Studiensem.	Regelstudiensem.	Turnus	Dauer **1 Semester**	SWS **2+2**	ECTS-Punkte **6**

Modulverantwortliche/r	Prof. Dr. Dominique Schröder
Dozent/inn/en	Prof. Dr. Michael Backes, Prof. Dr. Dominique Schröder
Zuordnung zum Curriculum	Wahlpflicht I im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	Grundlagen der Cybersicherheit, Cryptography, Security
Leistungskontrollen / Prüfungen	Art der Prüfung wird zu Beginn der Vorlesung bekannt gegeben: Klausur (120 Minuten, benotet) oder mündliche Prüfung (25 – 30 Minuten, benotet); zusammenfassende Modulprüfung über den Stoff der Vorlesungen (benotet)
Lehrveranstaltungen / SWS	Advanced Cryptography, Vorlesung 2 SWS Übung 2 SWS
Arbeitsaufwand	Arbeitsaufwand: insgesamt 180 Stunden 80 Stunden Präsenzzeit Vorlesung und Übung, 100 Stunden Selbststudium (Prüfungsvorbereitung)
Modulnote	Das Modul ist insgesamt bestanden, wenn die Prüfungsleistung bestanden wurde.

Lernziele/Kompetenzen

Die Studierenden kennen die Grundlagen der Kryptographie. Sie kennen die verschiedenen Komplexitätsklassen der Kryptographie. Sie sind vertraut mit dem Begriff der Simulierbarkeit.

Inhalt

- Konstruktion von kryptographischen Primitiven von One-way (trapdoor) Funktionen.
- (Non-interactive) Zero-knowledge Beweissysteme
- Sichere Berechnung beliebiger Funktionen
- Ausgewählte Themen aktueller Forschung

Weitere Informationen

Die Unterrichtssprache ist englisch. Die Literatur zum Modul wird zu Beginn der Veranstaltung bekannt gegeben.

Modul **Malware Analysis and Intrusion Detection**					Abk. **IDS**
Studiensem.	Regelstudiensem.	Turnus	Dauer **1 Semester**	SWS **2+2**	ECTS-Punkte **6**

Modulverantwortliche/r	Prof. Dr. Michael Backes
Dozent/inn/en	Prof. Dr. Michael Backes, , Prof. Dr. Christian Hammer, Dr. Christian Rossow
Zuordnung zum Curriculum	Wahlpflicht I im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	Security
Leistungskontrollen / Prüfungen	Abschlussklausur
Lehrveranstaltungen / SWS	Malware Analysis and Intrusion Detection, Vorlesung 2 SWS Übung 2 SWS
Arbeitsaufwand	Arbeitsaufwand: insgesamt 180 Stunden 80 Stunden Präsenzzeit Vorlesung und Übung, 100 Stunden Selbststudium (Prüfungsvorbereitung)
Modulnote	Das Modul ist insgesamt bestanden, wenn die Prüfungsleistung bestanden wurde.

Lernziele/Kompetenzen

Die Studierenden kennen Intrusion Detection Systeme und deren Grundlagen, Funktionsweise sowie darauf basierend Stärken und Schwächen. Sie können die unterschiedlichen Formen von IDS unterscheiden und erklären. Sie können geeignete Abwehrmechanismen gegen Angriffe aufzeigen und erklären.

Inhalt

- Host-basierte IDS vs. Netzwerk-basierte IDS und Hybride
- Funktionsweise signaturbasierter, zustandsbasierter und anomaliebasierter Verfahren
- Aktive vs. passive IDS
- Schwächen und Angriffsvektoren von IDS
- Einsatzszenarien von IDS
- Computerforensik
- Weitergehende Verfahren (z.B. Honeypots)
- Zusammenspiel von IDS mit anderen Sicherheitskomponenten
- Kennenlernen und Experimentieren mit realistischen IDS

Weitere Informationen

Die Unterrichtssprache ist deutsch oder englisch und wird zu Beginn der Veranstaltung bekannt gegeben. Die Literatur zum Modul kann englisch- und/oder deutschsprachig sein und wird zu Beginn der Veranstaltung bekannt gegeben.

Modul **Theoretical Foundation of Cyber Security**					Abk. **CSF**
Studiensem.	Regelstudiensem.	Turnus	Dauer **1 Semester**	SWS **2+2**	ECTS-Punkte **6**

Modulverantwortliche/r	Prof. Dr. Matteo Maffei
Dozent/inn/en	Prof. Dr. Michael Backes, Prof. Dr. Matteo Maffei, Dr. Deepak Garg
Zuordnung zum Curriculum	Wahlpflicht I im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	Security
Leistungskontrollen / Prüfungen	Schriftliche oder mündliche Abschlussprüfung über das gesamte Themengebiet
Lehrveranstaltungen / SWS	Vertiefungsvorlesung Privacy Enhancing Technology [PET], 4 SWS (6 CP)
Arbeitsaufwand	Arbeitsaufwand: insgesamt 180 Stunden 80 Stunden Präsenzzeit Vorlesung und Übung, 100 Stunden Selbststudium (Prüfungsvorbereitung)
Modulnote	Das Modul ist insgesamt bestanden, wenn die Prüfungsleistung bestanden wurde.

Lernziele/Kompetenzen

The students will learn various formal methods to rigorously specify, analyse, and enforce security properties of IT systems, and they will acquire an hands-on experience with the state-of-the-art security analysis tools.

Inhalt

- Formal analysis of cryptographic protocols
- Information flow analysis
- Security policy enforcement
- Analysis of mobile applications
- Analysis of web applications

Weitere Informationen

The teaching language is English. The teaching material will be in English and it will consist of slides as well as papers from the literature.

Modul **Web and Mobile Security**					Abk. **WMS**
Studiensem.	Regelstudiensem.	Turnus	Dauer **1 Semester**	SWS **2+2**	ECTS-Punkte **6**

Modulverantwortliche/r	Prof. Dr. Matteo Maffei
Dozent/inn/en	Prof. Dr. Christian Hammer, Prof. Dr. Matteo Maffei
Zuordnung zum Curriculum	Wahlpflicht I im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	Secure Software Engineering
Leistungskontrollen / Prüfungen	Projekt und schriftliche Abschlussklausur
Lehrveranstaltungen / SWS	Vertiefungsvorlesung Web and Mobile Security, 4 SWS (6 CP)
Arbeitsaufwand	Arbeitsaufwand: insgesamt 180 Stunden 80 Stunden Präsenzzeit Vorlesung und Übung, 100 Stunden Selbststudium (Prüfungsvorbereitung)
Modulnote	Das Modul ist insgesamt bestanden, wenn die Prüfungsleistung bestanden wurde.

Lernziele/Kompetenzen

The students will acquire a deep understanding of security threats, defences, and development tools for web and mobile applications.

Inhalt

- State-of-the-art in mobile and web programming
- Security threats
- Programming frameworks, usage and security guarantees
- Security libraries (e.g., for sanitization and authentication)
- Security architectures
- Memory management

Weitere Informationen

The teaching language is English. The teaching material will be in English and it will be announced at the beginning of the lecture .

Modul **Cyber Attacks and Defences**					Abk. **HLab**
Studiensem.	Regelstudiensem.	Turnus	Dauer **1 Semester**	SWS **4**	ECTS-Punkte **6**

Modulverantwortliche/r	Prof. Dr. Michael Backes
Dozent/inn/en	Prof. Dr. Michael Backes, Prof. Dr. Christian Hammer
Zuordnung zum Curriculum	Wahlpflicht I im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	Security
Leistungskontrollen / Prüfungen	Projekt und schriftliche Abschlussklausur
Lehrveranstaltungen / SWS	Vertiefungsvorlesung Privacy Enhancing Technology [PET], 4 SWS (6 CP)
Arbeitsaufwand	Arbeitsaufwand: insgesamt 180 Stunden 80 Stunden Präsenzzeit Vorlesung und Übung, 100 Stunden Selbststudium (Prüfungsvorbereitung)
Modulnote	Das Modul ist insgesamt bestanden, wenn die Prüfungsleistung bestanden wurde.

Lernziele/Kompetenzen

Die Studenten erlangen ein Grundverständnis der typischen Schwachstellen von und resultierender Angriffe auf moderne IT Systeme, welches es Angreifern erlaubt diese Systeme zu manipulieren oder gar unter Kontrolle zu bringen. Aufbauend wird den Studenten grundlegende Kompetenz aktueller Verteidigungsmechanismen von IT Systemen vermittelt. Mit dem erlernten Wissen wird durch praktische Übungen (unter kontrollierten Bedingungen) so ein tiefgehendes Verständnis der Problematik erreicht, das ein Bewusstsein für Sicherheit schärft.

Inhalt

- WLAN und Netzwerksicherheit
- Passwort Sicherheit
- Sicherheit von Web Applikationen
- Forensik Grundlagen
- Software-Sicherheit
- Betriebssystemsicherheit
- Sicherheit von Smarthone Apps
- Aktuelle Inhalte der IT Sicherheitsforschung

Weitere Informationen
Die Unterrichtssprache ist deutsch oder englisch und wird zu Beginn der Veranstaltung bekannt gegeben. Die Literatur zum Modul kann englisch- und/oder deutschsprachig sein und wird zu Beginn der Veranstaltung bekannt gegeben.

Modul **Wahlpflicht II**					Abk. **WP**
Studiensem. **6.**	Regelstudiensem. **6.**	Turnus **Jährlich, SS**	Dauer **1 Semester**	SWS **3**	ECTS-Punkte **6**

Modulverantwortliche/r	Studiendekan der Fakultät Mathematik und Informatik bzw. Studienbeauftragter der Informatik
Dozent/inn/en	
Zuordnung zum Curriculum	Wahlpflichtmodul im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	
Leistungskontrollen / Prüfungen	
Lehrveranstaltungen / SWS	Wählbare Veranstaltungen im Umfang von mind. 6 CP aus folgenden Bereichen: **Soft Skills Veranstaltungen laut Kursangebot, z. B.:** *Tutortätigkeit* [CS-T], 4 CP *Soft Skills Seminar* [---], 4 CP *versch. Sprachkurse* [---], 3CP *Kurse der Informatik* *Ringvorlesung*, 2CP
Arbeitsaufwand	Arbeitsaufwand: insgesamt 210 Stunden Abhängig von der gewählten Veranstaltung, z. B.: 60 Stunden Präsenzzeit Seminar, 60 Stunden Vor- und Nachbereitung, 90 Stunden Selbststudium (Prüfungsvorbereitung)
Modulnote	Das Modul ist insgesamt bestanden, wenn die Prüfungsleistung bestanden wurde.

Lernziele/Kompetenzen

- Veranstaltungen des Fachbereichs Informatik:
Die Studierenden haben am Ende der Veranstaltung ein tiefes Verständnis aktueller oder fundamentaler Aspekte eines spezifischen Teilbereiches der Informatik erlangt. Die Veranstaltungen werden von wöchentlichen Übungen begleitet, welche die vorgestellten themenspezifischen Sachverhalte praktisch vertiefen.

- Soft Skill Veranstaltungen:
- Tutoren lernen, wie Lehrveranstaltungen organisiert werden und welche methodischen Ziele dabei verfolgt werden. Sie lernen, komplexe fachliche Inhalte sowohl in einer größeren Gruppe (Übungsgruppe) als auch in individuellen Beratungsgesprächen zu vermitteln.
- Präsentationstechniken, wissenschaftliche Recherche, Projektmanagement
- Erlernen versch. Fremdsprachen in Wort und Schrift

Inhalte

- Veranstaltungen des Fachbereichs Informatik (Stammvorlesungen & Vertiefungsvorlesungen):
Der Inhalt variiert nach belegtem Themenschwerpunkt. Das Kursangebot kann variieren und orientiert sich an dem Vorlesungsangebot des Fachbereichs und spiegelt die Forschungsthemen der Saarbrücker Informatik wieder. In den Veranstaltungen werden zentrale wissenschaftliche Fragestellungen der Kerngebiete der Informatik vorgestellt und behandelt.

Weitere Informationen

Die Unterrichtssprache ist deutsch oder englisch und wird zu Beginn der Veranstaltung bekannt gegeben. Die Literatur zum Modul kann englisch- und/oder deutschsprachig sein und wird zu Beginn der Veranstaltung

bekannt gegeben.

Modul					Abk.
Bachelor-Seminar					**CS 690**
Studiensem.	Regelstudiensem.	Turnus	Dauer	SWS	ECTS-Punkte
6.	**6.**	**Jährlich, WS+SS**	**1 Semester**	**5**	**9**

Modulverantwortliche/r	Studiendekan der Fakultät Mathematik und Informatik bzw. Studienbeauftragter der Informatik
Dozent/inn/en	Professoren der Fachrichtung und Spezialisierungsfachrichtungen
Zuordnung zum Curriculum	Wahlpflichtmodul im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	Teilnahme an allen Pflichtmodulen des Bachelor-Studiengangs Cybersicherheit (empfohlen)
Leistungskontrollen / Prüfungen	• Vorstellung eines wissenschaftlichen Artikels im Lesekreis. • Aktive Teilnahme an der Diskussion im Lesekreis. • Vortrag über die geplante Aufgabenstellung mit anschliessender Diskussion. • Schriftliche Beschreibung der Aufgabenstellung der Bachelorarbeit
Lehrveranstaltungen / SWS	Seminar *Bachelor-Seminar* [CS 690], 5 SWS (9 CP)
Arbeitsaufwand	Arbeitsaufwand: insgesamt 270 Stunden 80 Stunden Präsenzzeit Seminarvorträge, 190 Stunden Selbststudium (Prüfungsvorbereitung)
Modulnote	Das Modul ist insgesamt bestanden, wenn die Prüfungsleistung bestanden wurde.

Lernziele/Kompetenzen

Im Bachelorseminar erwirbt der Studierende unter Anleitung die Fähigkeit zum wissenschaftlichen Arbeiten im Kontext eines angemessen Themengebietes.
Am Ende des Bachelorseminars sind die Grundlagen für eine erfolgreiche Anfertigung der Bachelorarbeit gelegt und wesentliche Lösungsansätze bereits eruiert.
Das Bachelorseminar bereitet somit die Themenstellung und Ausführung der Bachelorarbeit vor.
Es vermittelt darüber hinaus praktische Fähigkeiten des wissenschaftlichen Diskurses. Diese Fähigkeiten werden durch die aktive Teilnahme an einem Lesekreis vermittelt, in welchem die Auseinandersetzung mit wissenschaftlich anspruchsvollen Themen geübt wird.

Inhalt

Auf der Grundlage des "State-of-the-Art" werden die Methoden der Informatik systematisch unter Anleitung angewendet.

Weitere Informationen

Die Unterrichtssprache ist deutsch oder englisch. Die Literatur zum Modul kann englisch- und/oder deutschsprachig sein und wird zu Beginn der Veranstaltung bekannt gegeben.

Modul **Bachelor-Arbeit**					Abk. **CS 699**
Studiensem. **6.**	Regelstudiensem. **6.**	Turnus **Jährlich, SS**	Dauer **1 Semester**	SWS	ECTS-Punkte **12**

Modulverantwortliche/r	Studiendekan der Fakultät Mathematik und Informatik bzw. Studienbeauftragter der Informatik
Dozent/inn/en	Professoren der Fachrichtung und Spezialisierungsfachrichtungen
Zuordnung zum Curriculum	Wahlpflichtmodul im Studiengang B.Sc. Cybersicherheit
Zulassungsvoraussetzungen	keine
Leistungskontrollen / Prüfungen	Schriftliche Ausarbeitung. Sie beschreibt sowohl das Ergebnis der Arbeit als auch den Weg, der zu dem Ergebnis führte. Der eigene Anteil an den Ergebnissen muss klar erkennbar sein. Außerdem Präsentation der Bachelorarbeit in einem Kolloquium, in dem auch die Eigenständigkeit der Leistung des Studierenden überprüft wird.
Lehrveranstaltungen / SWS	*Bachelor-Arbeit* [CS 699] (12 CP)
Arbeitsaufwand	Arbeitsaufwand: insgesamt 360 Stunden 20 Stunden Präsenzzeit, 340 Stunden Selbststudium (Prüfungsvorbereitung)
Modulnote	Das Modul ist insgesamt bestanden, wenn die Prüfungsleistung bestanden wurde. [benotet]

Lernziele/Kompetenzen
Die Bachelor-Arbeit ist eine Projektarbeit, die unter Anleitung ausgeführt wird. Sie zeigt, dass der Kandidat/die Kandidatin in der Lage ist, innerhalb einer vorgegebenen Frist ein Problem aus dem Gebiet der Informatik unter Anleitung zu lösen und die Ergebnisse zu dokumentieren.

Inhalt
Auf der Grundlage des "State-of-the-Art" wird die systematische Anwendung der Methoden der Informatik dokumentiert.

Weitere Informationen
Die Unterrichtssprache ist deutsch oder englisch. Die Literatur zum Modul kann englisch- und/oder deutschsprachig sein und wird zu Beginn der Veranstaltung bekannt gegeben.