MODULHANDBUCH

Übersicht der Module

IT-Sicherheit / Netze und Systeme - Master (1-Fach, PO 2022)

Pflichtbereich

Einführung in die Kryptographie 1

Einführung in die Kryptographie 2

Kryptographie

Mathematik (Netze und Systeme)

Netzsicherheit 1

Netzsicherheit 2

Systemsicherheit

Wahlpflichtbereich

Aktuelle Themen im Bereich der Internet-Sicherheit

Aufbau eines Managementsystems für Informationssicherheit nach DIN ISO / 27001

Authentische Schlüsselvereinbarung: Formale Modelle und Anwendungen

Autonomous Vehicles and Artificial Intelligence

Boolesche Funktionen mit Anwendungen in der Kryptographie

Developer Centered Security

Digitale Forensik

Einführung ins Hardware Reverse Engineering

Foundations of Programming Languages, Verification, and Security

Human Aspects of Cryptography Adoption

Implementierung kryptographischer Verfahren

Information Theory

Introduction to Blockchain Security

Komplexitätstheorie

Kryptographie auf hardwarebasierten Plattformen

Kryptographische Protokolle

Menschliches Verhalten in der IT-Sicherheit

Message Level Security

Microarchitectural Attacks and Defenses

Processor Security

Programmanalyse

Proofs are programs

Public Key Kryptanalyse 1

Public Key Verschlüsselung

Quantum Cryptography

Red- and Blue-Teaming
Software Protection
Software Security
Software-Implementierung kryptographischer Verfahren
Symmetrische Kryptanalyse
Usable Security
Web-und Browsersicherheit
Zero-Knowledge Proof Systems
Master Praktikum/Projektarbeit IT-Sicherheit
Vertiefungsseminar (M.Sc. IT-Sicherheit)

Wahlbereich

Freie Wahlmodule

Abschlussarbeit

Masterarbeit und Kolloquium (ITS)

Titel des Moduls: Einführung in die Kryptographie 1

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Wintersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Einführung in die Kryptographie 1 (212010)	60 h	90 h	300 Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch	keine

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

Verwendung des Moduls
B.Sc. IT-Sicherheit

B.Sc. Informatik

B.Sc. Angewandte Informatik

M.Sc. IT-Sicherheit/ Netze und Systeme

Vorkenntnisse

Lernziele (learning outcomes)

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

Inhalt
Das Modul bietet einen allgemeinen Einstieg in die Funktionsweise moderner Kryptografie und Datensicherheit. Es werden grundlegende Begriffe und mathematisch/technische Verfahren der Kryptografie und der Datensicherheit erläutert. Praktisch relevante symmetrische und asymmetrische Verfahren und Algorithmen werden vorgestellt und an praxisrelevanten Beispielen erläutert.

Die Vorlesung lässt sich in zwei Teile gliedern:

Die Funktionsweise der symmetrischen Kryptographie einschließlich der Beschreibung historisch bedeutender symmetrischer Verschlüsslungsverfahren (Caesar Chiffre, Affine Chiffre) und aktueller symmetrischer Verfahren (Data Encryption Standard, Advanced Encryption Standard, Stromchiffren, One Time Pad) werden im ersten Teil behandelt.

Der zweite Teil besteht aus einer Einleitung zu asymmetrischen Verfahren und einem ihrer wichtigsten Stellvertretern (RSA). Hierzu wird eine Einführung der Grundlagen der Zahlentheorie durchgefuhrt, um ein grundlegendes Verständnis der Verfahren sicherzustellen (u.a. Ringe ganzer Zahlen, Gruppen, Körper, diskrete Logarithmen, euklidischer Algorithmus). Nichtsdestotrotz liegt der Schwerpunkt auf der algorithmischen

Einfuhrung des asymmetrischen Verfahrens.
Lehrformen Vorlesung mit Übung
Prüfungsformen Klausurarbeit (120 Minuten)
Voraussetzungen für die Vergabe von Credits Erfolgreiches Bestehen der Modulklausur.
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) 5/158: B.Sc. Informatik [PO 22] 5/165: B.Sc. Informatik [PO 20] 5/149: B.Sc. IT-Sicherheit [PO 20] 5/150: B.Sc. IT-Sicherheit [PO 22] 5/168: B.Sc. Angewandte Informatik [PO 22] 5/170: B.Sc. Angewandte Informatik [PO 20] 5/96 : M.Sc. IT-Sicherheit/ Netze und Systeme [PO20] 5/99 : M.Sc. IT-Sicherheit/ Netze und Systeme [PO22]

Titel des Moduls: Einführung in die Kryptographie 2

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Sommersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Einführung in die Kryptographie 2 (211009)	60 h	90 h	300 Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch	Keine

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

Verwendung des Moduls

B.Sc. IT-Sicherheit

B.Sc. Informatik

B.Sc. Angewandte Informatik

M.Sc. IT-Sicherheit/ Netze und Systeme

Vorkenntnisse
Inhalte der Vorlesung "Einführung in die Kryptographie 1"

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

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

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

Im zweiten Teil der Vorlesung werden Grundlagen von Sicherheitslösungen aufbauend auf den Konzepten der symmetrischen und asymmetrischen Kryptographie besprochen. Dabei wird vor allem auf die in Unternehmen notwendigen und eingesetzten Lösungen (PKI, digitale Zertifikate etc.) eingegangen.

Lehrformen
Vorlesung mit Übungen

Prüfungsformen
Klausurarbeit (120 Minuten)

Voraussetzungen für die Vergabe von Credits
Bestandene schriftliche Modulabschlussprüfung.

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

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

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

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

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

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

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

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

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

Titel des Moduls: Kryptographie
Cryptography

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	8 CP	240 h	siehe Prüfungsordnung	Wintersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Kryptographie (212017)	90 h	150 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch	

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Prof. Alexander May
Lehrende: Prof. Alexander May

Verwendung des Moduls
B.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Syteme

M.Sc. Informatik

M.Sc. Angewandte Informatik

Vorkenntnisse
Inhalte der Vorlesungen Einführung in die Kryptographie 1 und 2

Lernziele (learning outcomes)
Die Studierdenden haben ein Verständnis der wesentlichen mathematischen Methoden und Verfahren, auf denen moderne kryptographische Verfahren beruhen. Die Tiefe der Behandlung der Verfahren geht deutlich uber das in den vorhergehenden Veranstaltungen vermitteltes Maß hinaus. Die Teilnehmer sind zur Analyse und dem Design aktueller und zukunftiger kryptographischer Methoden befähigt. Zudem weisen sie ein Bewusstsein fur Methodik und Mächtigkeit verschiedenster Angriffsszenarien auf.

Inhalt
Es wird eine Einführung in moderne Methoden der symmetrischen und asymmetrischen Kryptographie geboten. Dazu wird ein Angreifermodell definiert und die Sicherheit der vorgestellten Verschlüsselungs-, Hash- und Signaturverfahren unter wohldefinierten Komplexitätsmaßnnahmen in diesem Angreifermodell nachgewiesen.

Themenubersicht:

- Sichere Verschlusselung gegenüber KPA-, CPA- und CCA-Angreifern
- Pseudozufallsfunktionen und -permutationen
- Message Authentication Codes
- Kollisionsresistente Hashfunktionen
- Blockchiffren
- Konstruktion von Zufallszahlengeneratoren
- Diffie-Hellman Schlusselaustausch
- Trapdoor Einwegpermutationen
- Public Key Verschlusselung: RSA, ElGamal, Goldwasser-Micali, Rabin, Paillier
- Einwegsignaturen
- Signaturen aus kollisionsresistenten Hashfunktionen
- Random-Oracle Modell

Lehrformen
Vorlesung und Übungen

Prüfungsformen Schriftliche Modulabschlussprüfung (120 Minuten)
Voraussetzungen für die Vergabe von Credits Bestandene schriftliche Modulabschlussprüfung.
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) 8/150: B.Sc. IT-Sicherheit/ Informationstechnik [PO 22] 8/149: B.Sc. IT-Sicherheit/ Informationstechnik [PO 20] 8/99: M.Sc. IT-Sicherheit/ Netze und Syteme [PO 22] 8/96: M.Sc. IT-Sicherheit/ Netze und Syteme [PO 20] 8/97: M.Sc. Informatik 8/105: M.Sc. Angewandte Informatik

Titel des Moduls: Mathematik (Netze und Systeme)
Mathematics

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	8 CP	240 h	1. oder 2.	Wintersemester	Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Diskrete Mathematik (150308 + 09, bis WiSe 22/23)	90 h	150 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch	

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r:
Lehrende:

Verwendung des Moduls
M.Sc. IT-Sicherheit/ Netze und Systeme

Vorkenntnisse

Lernziele (learning outcomes)
Ein allgemeines Lernziel ist der professionelle Umgang mit abstrakten, diskreten Strukturen.
Dazu gehört die Fähigkeit, konkrete Problemstellungen mit solchen Strukturen zu modellieren und scharfsinnige Schlussfolgerungen aus gegebenen Informationen zu ziehen (Anwendung kombinatorischer Schlussweisen).
Dazu gehört weiterhin ein Verständnis für grundlegende algorithmische Techniken, und die Analyse von Algorithmen. In den einzelnen Abschnitten der Vorlesung werden die jeweils grundlegenden Konzepte (in Kombinatorik, Graphtheorie, elementarer Zahlentheorie und elementarer Wahrscheinlichkeitstheorie) erworben.
Es wird die intellektuelle Fähigkeit geschult, die logischen Zusammenhänge zwischen den Konzepten zu überblicken und 'versteckte' Anwendungsmöglichkeiten zu erkennen.

Inhalt

Die Diskrete Mathematik beschäftigt sich mit endlichen Strukturen. Die Vorlesung gliedert sich in 5 Abschnitte. Abschnitt 1 ist der Kombinatorik gewidmet. Insbesondere werden grundlegende Techniken vermittelt, um sogenannte Zählprobleme zu lösen. In Abschnitt 2 beschäftigen wir uns mit der Graphentheorie. Graphen werden zur Modellierung von Anwendungsproblemen benutzt. Wir behandeln Techniken zur Graphenexploration und weitere ausgesuchte Graphenprobleme. Abschnitt 3 vermittelt Grundkenntnisse in elementarer Zahlentheorie und endet mit einem Ausblick auf kryptographische Anwendungen. Grundlegende Designtechniken für effiziente Algorithmen bilden das zentrale Thema von Abschnitt 4. Daneben geht es auch um das Aufstellen und Lösen von Rekursionsgleichungen. Abschnitt 5 liefert eine Einführung in die Wahrscheinlichkeitstheorie mit Schwergewicht auf diskreten Wahrscheinlichkeitsräumen.

Lehrformen
Vorlesung mit Übung

Prüfungsformen
vorr. Modulabschlussklausur

Voraussetzungen für die Vergabe von Credits

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

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

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

Titel des Moduls: Netzsicherheit 1
Network Security 1

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	3. Semester	Wintersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Netzsicherheit 1 (212012)	60 h	90 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch	

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

Verwendung des Moduls

B.Sc. IT-Sicherheit / Informationstechnik

M.Sc. IT-Sicherheit / Netze und Systeme

M.Sc. Angewandte Informatik

Vorkenntnisse
Grundkenntnisse in TCP/IP, Grundkenntnisse der Sicherheitsprobleme von Computernetzen auf dem Niveau populärer Fachzeitschriften (z.B. c't).

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

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

- Einführung: Internet
- Einführung: Vertraulichkeit
- Einführung: Integrität
- Einführung: Kryptographische Protokolle
- PPP-Sicherheit (insb. PPTP), EAP-Protokolle
- WLAN-Sicherheit (WEP, WPA, Wardriving, KRACK)
- GSM- und UMTS-Mobilfunk (Authentisierung und Verschlüsselung)
- IPSec (ESP und AH, IKEv1 und v2, Angriffe auf IPSec)
- Dateiverschlüsselung mit OpenPGP (Datenformat, Efail, Klima-Rosa)
- E Mail-Verschlüsselung mit S/MIME (SMTP, Datenformat, Efail, POP3, IMAP)

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

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

Prüfungsformen
Schriftliche Modulabschlussprüfung (120 Minuten)

Voraussetzungen für die Vergabe von Credits
Bestandene schriftliche Modulabschlussprüfung

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)
5/150: B.Sc. IT-Sicherheit/ Informationstechnik [PO 22]

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

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

5/105: M.Sc. Angewandte Informatik

Titel des Moduls: Netzsicherheit 2
Network Security 2

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP				Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Netzsicherheit 2 (211013)			Studierende

Unterrichtssprache	Teilnahmevoraussetzungen

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r:
Lehrende:

Verwendung des Moduls

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

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

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

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

Vorkenntnisse

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

Inhalt

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

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

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

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

Titel des Moduls: Systemsicherheit
System Security

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Sommersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Systemsicherheit (211011)	60 h	90 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Englisch	keine

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Prof. Dr. Ghassan Karame
Lehrende: Prof. Dr. Ghassan Karame

Verwendung des Moduls
B.Sc. IT-Sicherheit/ Informationstechnik

B.Sc. Informatik

M.Sc. Angewandte Informatik

M.Sc. IT-Sicherheit/ Netze und Systeme

Vorkenntnisse
Background in Cryptographic primitives (encryption methods, signatures, MACs, hash functions), principles of communication networks, is recommended.

Lernziele (learning outcomes)
At the end of this course, students will be able to

- classify and describe vulnerabilities and protection mechanisms of popular systems and protocols, and
- analyze / reason about basic protection mechanisms for modern OSs, software, and hardware systems. Students will also develop the ability to reason about the security of a given protocol and independently develop appropriate security defenses and security models.

Inhalt
While clearly beneficial, the large-scale deployment of online services has resulted in the increase of security threats against existing services. As the size of the global network grows, the incentives of attackers to abuse the operation of online applications also increase and their advantage in mounting successful attacks becomes considerable.

These cyber-attacks often target the resources, availability, and operation of online services. With an increasing number of services relying on online resources, integrating proper security measures therefore becomes integral to ensure the correct functioning of every online service.

In this course, we discuss important theoretical and analytical aspects in system security. The focus of the course is to understand basic attack strategies on modern systems and platforms, with a focus on side-channel attacks, software-based attacks, malware analysis, as well as software-based defenses (e.g., address space randomization and non-executable memory) and hardware-based defenses (e.g., using TPMs and TEEs). Other topics of the course include analyzing the security of modern cryptocurrencies and ML platforms, and similar aspects in system security.

An integral part of this course are exercises and homeworks, which aim to deepen the understanding of the material with practical examples.

Lehrformen

Prüfungsformen

Voraussetzungen für die Vergabe von Credits
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) 5/150: B.Sc. IT-Sicherheit/ Informationstechnik [PO 22] 5/149: B.Sc. IT-Sicherheit/ Informationstechnik [PO 20] 5/158: B.Sc. Informatik [PO 22] 5/165: B.Sc. Informatik [PO 20] 5/105: M.Sc. Angewandte Informatik 5/99: M.Sc. IT-Sicherheit/ Netze und Systeme [PO 22] 5/96: M.Sc. IT-Sicherheit/ Netze und Systeme [PO 20]

Titel des Moduls: Aktuelle Themen im Bereich der Internet-Sicherheit

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP			Wintersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
211099 - Aktuelle Themen im Bereich der Internet-Sicherheit			Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch	

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Prof. Jörg Schwenk
Lehrende: Prof. Jörg Schwenk

Verwendung des Moduls

Vorkenntnisse
Keine

Lernziele (learning outcomes)
In der Vorlesung werden ausgewählte Themen der IT-Sicherheit behandelt, die vom Lehrstuhl für Netz- und Datensicherheit in den letzten Jahren publiziert wurden. Es werden unter anderem folgende Themen behandelt:

- Portable Document Flaws
- Overview over Cryptographic Modelling with the Example of Messaging
- 0-RTT and Tor
- Padding Oracles
- Racoon
- Breaking Microsoft RMS 2020
- IPsec-Bleichenbacher
- DEMONS: DNS-Poisoning by Exhaustive Misappropriation of Network Sockets
- DOM
- XS Leaks
- UI Redressing

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

Inhalt
Studierende verfügen nach erfolgreichem Abschluss des Moduls über ein umfassendes Verständnis der aktuellen Forschungsthemen im Bereich der Internet-Sicherheit. Sie haben die neuesten Angriffe und Sicherheitsmechanismen kennengelernt. Zusätzlich wissen Sie, wie man mit Sicherheitsschwachstellen korrekt umgeht und wie man diese an den Hersteller meldet. Durch die wissenschaftsnahe Themen haben die Studierenden Einblicke in die Forschung im Bereich der Internetsicherheit gekriegt, wodurch sie sich auch auf ihre potentielle Forschungsrolle vorbereitet haben.

Lehrformen
Vorlesung

Prüfungsformen
Schriftliche Klausur (120 Minuten, elektronisch)

Voraussetzungen für die Vergabe von Credits

Bestandene Modulabschlussprüfung

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

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

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	4 CP	120 h	siehe Prüfungsordnung	Sommersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Aufbau eines Managementsystems für Informationssicherheit nach DIN ISO / IEC 27001 (211021)	45 h	75 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch	Keine

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Professur für Systemsicherheit
Lehrende: Dr.-Ing. Sebastian Uellenbeck

Verwendung des Moduls
B.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

Vorkenntnisse
Vorkenntnisse über Systemsicherheit und Netzsicherheit z. B. aus den Vorlesungen Systemsicherheit 1&2 und Netzsicherheit 1&2

Lernziele (learning outcomes)
Die Studierenden haben ein fundiertes Verständnis über den Aufbau eines ISMS nach ISO 27001 und kennen die notwendigen Schritte, um ein Unternehmen zur Zertifizierungsreife zu begleiten. Studierenden können eigenständig neue Probleme analysieren und neue Lösungsmöglichkeiten entwickeln. Sie können mit diesem Verständnis mit ihren Kollegen über ISO/IEC 27001 diskutieren und auftretende Probleme im Gespräch korrekt klassifizieren.

Inhalt

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

- 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).

Lehrformen
Vorlesung mit Übung (Blockveranstaltung in den Semesterferien Anmeldung über syssec@rub.de)

Prüfungsformen schriftliche Modulabschlussprüfung (90 Minuten)
Voraussetzungen für die Vergabe von Credits bestandene schriftliche Modulabschlussprüfung
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS) 4/150: B.Sc. IT-Sicherheit/ Informationstechnik [PO 22] 4/149: B.Sc. IT-Sicherheit/ Informationstechnik [PO 20] 4/91: M.Sc. IT-Sicherheit/ Informationstechnik [PO 22] 5/99: M.Sc. IT-Sicherheit/ Netze und Systeme [PO 20]

Titel des Moduls: Authentische Schlüsselvereinbarung: Formale Modelle und Anwendungen

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Sommersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Au-then-ti-sche Schlüs-sel-ver-ein-ba-rung: For-ma-le Mo-del-le und An-wen-dun-gen (211038)	60 h	90 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch	Keine

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

Verwendung des Moduls
M.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

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

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

Inhalt

as Modul 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.

Lehrformen
Vorlesung mit Übung

Prüfungsformen
schriftlich, 120 Minuten

Voraussetzungen für die Vergabe von Credits
Bestandene Modulabschlussprüfung

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

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

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

Titel des Moduls: Autonomous Vehicles and Artificial Intelligence

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Sommersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Autonomous Vehicles and Artificial Intelligence (211044)	60 h	90 h	25 Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Englisch	keine

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Prof. Thorsten Berger
Lehrende: Prof. Dr. Thorsten Berger, Dr. Sven Peldszus

Verwendung des Moduls
B.Sc. Informatik

B.Sc. IT-Sicherheit

B.Sc. Angewandte Informatik

M.Sc. Informatik

M.Sc. Angewandte Informatik

M.Sc. IT-Sicherheit/Informationstechnik

Vorkenntnisse
The Software Engineering lecture or a comparable course, Programming experiences e.g. as part of other courses

Lernziele (learning outcomes)
- Understanding requirements on autonomous vehicles
- Understanding the architecture of autonomous vehicles
- Ability to build a self-driving car with ROS2
- Understanding and applying quality assurance for autonomous vehicles

Inhalt
Autonomous driving is the future of individual mobility and all major manufacturers are working on fully autonomous vehicles. While there are robust and good solutions for the individual problems in autonomous driving, the main challenge lies in their integration. Altogether, an autonomous vehicle’s software is the biggest problem. Therefore, the key in self-driving vehicles is about getting the software right. In this course, we will investigate the different aspects of self-driving vehicles as well as the importance and application of artificial intelligence in this domain. The course will primarily focus on the following topics:
- Requirements on autonomous vehicles
- Architecture of autonomous vehicles
- Operation systems and frameworks for robotic systems
- Specification and Implementation of autonomous vehicles based on ROS2
- Artificial intelligence for autonomous vehicles
- Simulation of autonomous vehicles ∙ Localization and perception
- Mission planning
- Quality assurance for autonomous vehicles In the course’s lecture, we provide the required theoretical background and practically apply the course’s content in exercises by building a self-driving robot.

Lehrformen
Vorlesung mit Übungen

Prüfungsformen
Mündliche Prüfung

Voraussetzungen für die Vergabe von Credits
Bestandene Modulabschlussprüfung und erfolgreiche Teilnahme an den Übungen

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

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

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

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

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

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

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

5/ 97: M.Sc. Informatik

5/105: M.Sc. Angewandte Informatik

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

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

Titel des Moduls: Boolesche Funktionen mit Anwendungen in der Kryptographie

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Sommersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Boolesche Funktionen mit Anwendungen in der Kryptographie (211020)	60 h	90 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch (bei Bedarf Englisch)	

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Prof. Dr. Nils-Gregor Leander
Lehrende: Prof. Dr. Nils-Gregor Leander

Verwendung des Moduls
B.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

Vorkenntnisse
Grundlegende Kenntnisse über endliche Körper.

Lernziele (learning outcomes)
Die Studierenden lernen die theoretischen Hintergründe von Booleschen Funktionen kennen.

Inhalt

In dieser Vorlesung beschäftigen wir uns mit der Theorie von Booleschen Funktionen.
Der Fokus liegt hierbei auf den kryptographisch relevanten Kriterien f ̈ur Boolesche Funktionen wie Nicht-Linearität und differentielle Uniformität.

Lehrformen
Vorlesung mit Übung

Prüfungsformen
schriftliche Modulabschlussprüfung (120 Minuten)

Voraussetzungen für die Vergabe von Credits
Bestandene schriftliche Modulabschlussprüfung

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

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

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

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

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

Titel des Moduls: Developer Centered Security
Developer Centered Security

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Sommersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Developer Centered Security (211050)	45 h	105 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch	keine

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Jun.-Prof. Dr. Alena Naiakshina
Lehrende: Jun.-Prof. Dr. Alena Naiakshina

Verwendung des Moduls
M.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

Vorkenntnisse
keine

Lernziele (learning outcomes)
Benutzbarkeitsprobleme, Sicherheitsanforderungen und Schwachstellen aktueller Systeme kennen. Methodik zur Untersuchung der Benutzbarkeit von Sicherheitsfunktionalitäten verstehen. Verhaltensstudien mit Softwareentwicklern und Administratoren unter Beachtung der vorgestellten Guidelines durchführen können. Sichere und benutzerfreundliche Systeme für Softwareentwickler und Administratoren entwickeln und beurteilen können.

Inhalt
Softwareentwickler und Administratoren sind häufig keine Sicherheitsexperten. Die von ihnen gebauten Systeme weisen daher oft Sicherheitslücken auf, durch die Millionen Nutzer und vertrauliche Daten gefährdet werden. Wie genau kommt es aber dazu, dass Softwareentwickler und Administratoren solche gravierenden Sicherheitsfehler machen, obwohl es fertige Anwendungsschnittstellen (application programming interface (API)), Programmbibliotheken und Tools gibt, die das Entwicklern und Verwenden von Sicherheitskonzepten erleichtern sollen? Es wird ein Einblick in die Grundlagen der benutzbaren Sicherheit und Privatsphäre sowie aktuelle, sicherheitsrelevante Studien mit Softwareentwicklern und Administratoren gegebenen. Die daraus gewonnenen Erkenntnisse werden systematisch aufgearbeitet und dargelegt. Es wird ferner aufgezeigt, was Sicherheitssystemdesigner, Toolentwickler, und Kryptographen beim Entwurf ihrer Systeme beachten sollten, um Softwareentwickler und Administratoren dabei zu unterstützen sicherheitskritische Fehler zu vermeiden. Zudem werden Guidelines zum Durchführen von Studien mit Softwareentwicklern und Administratoren vorgestellt. Dabei wird eine Abgrenzung zu Studien mit Endbenutzern gezogen.

Lehrformen
Vorlesung mit Übung

Prüfungsformen
Schriftliche Modulabschlussprüfung

Voraussetzungen für die Vergabe von Credits
Bestandene Modulabschlussprüfung

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

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

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

Titel des Moduls: Digitale Forensik

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Wintersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Digitale Forensik (211017)	60 h	90 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch	

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Studiendekan IT-Sicherheit
Lehrende: Dr. Christof Fein

Verwendung des Moduls
B.Sc. IT-Sicherheit/ Informationstechnik

B.Sc. Informatik

M.Sc. IT-Sicherheit/ Netze und Systeme

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

Lernziele (learning outcomes)
Die Studierenden beherrschen verschiedene Konzepte, Techniken und Tools aus dem Themengebiet der digitalen Forensik. Sie kennen die relevanten Konzepte und haben ein Überblick zum Forensischen Prozess. Es ist grundlegendes Verständnis von verschiedenen Methoden zur Sammlung, Analyse und Aufbereitung digitaler Spuren in IT-Systemen vorhanden. Die Studierenden können eigenständig neue Probleme analysieren und neue Lösungsmöglichkeiten entwickeln. Sie können mit diesem Verständnis mit ihren Kollegen über Probleme der Computerforensik diskutieren und auftretende Probleme im Gespräch korrekt klassifizieren.

Inhalt

Digitale Forensik befasst sich mit der Sammlung, Analyse und Aufbereitung digitaler Spuren in IT-Systemen. Im Rahmen der Vorlesung werden diese drei Themenbereiche vorgestellt und jeweils erläutert, mit welchen Verfahren und Ansätzen man diese Aufgaben erreichen kann. Ein Schwerpunkt der Vorlesung liegt auf dem Bereich der Analyse von Dateisystemen. Dazu werden verschiedene Arten von Dateisystemen detailliert vorgestellt und diskutiert, wie relevante Daten erfasst, analysiert und aufbereitet werden können. Darüber hinaus werden weitere Themen aus dem Bereich der digitalen Forensik behandelt, z.B. die Analyse von Smartphones und SQLite-Datenbanken. Ein integraler Teil der Veranstaltung sind die Übungen, die den Stoff mit praktischen Beispielen verdeutlichen und vertiefen.

Lehrformen
Vorlesung mit Übung als Blockveranstaltung

Prüfungsformen
Schriftliche Modulabschlussprüfung (120 Minuten)

Voraussetzungen für die Vergabe von Credits
Bestandene schriftliche Modulabschlussprüfung

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

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

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

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

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

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

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

Titel des Moduls: Einführung ins Hardware Reverse Engineering

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Wintersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Einführung ins Hardware Reverse Engineering (212025)	60 h	90 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Englisch	

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

Verwendung des Moduls
B.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

Vorkenntnisse
Inhalte der Vorlesungen “Technische Informatik 1 - Rechnerarchitektur” und “Technische Informatik 2 - Digitaltechnik”.

Lernziele (learning outcomes)

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

Inhalt

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

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

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

Lehrformen
Vorlesung mit Übung

Prüfungsformen
Die Modulprüfung ist in eine schriftliche Klausur (max. 60%) und mehrere vorlesungsbegleitende Projekte (max. 40%) aufgeteilt. Zusätzlich können bis zu 5% Bonus erworben und insgesamt maximal 100% erreicht werden.

Voraussetzungen für die Vergabe von Credits
Bestandene Modulabschlussprüfung und erfolgreiche Teilnahme an den praktischen Übungen am Rechner.
Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)
5/150: B.Sc. IT-Sicherheit/ Informationstechnik [PO 22]
5/149: B.Sc. IT-Sicherheit/ Informationstechnik [PO 20]
5/99: M.Sc. IT-Sicherheit/ Netze und Systeme [PO 22]
5/96: M.Sc. IT-Sicherheit/ Netze und Systeme [PO 20]

Titel des Moduls: Foundations of Programming Languages, Verification, and Security

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h		Wintersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Foundations of Programming Languages, Verification, and Security	60 h	90 h	Studierende

Unterrichtssprache
Englisch

Teilnahmevoraussetzungen

This advanced course for MSc and PhD students requires having attended the Proofs are Programs course or having a working knowledge of the contents of the Logical Foundations book (https://mpi-sp-pap-2023.github.io/book), including familiarity with logic, mechanized proofs, and functional programming in the Coq proof assistant.

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Dr. Roberto Blanco
Dr. Catalin Hritcu
Lehrende: Dr. Roberto Blanco
Dr. Catalin Hritcu

Verwendung des Moduls
o Master Computer Science

o Master IT-Sicherheit/Netze und Systeme (Wahl oder Wahlpflicht)

o Master IT-Sicherheit/Informationstechnik (Wahl oder Wahlpflicht)

o Master Mathematik (Nebenfach Informatik)

Vorkenntnisse

Lernziele (learning outcomes)
After successful completion of this course, students will be able to

l understand how to define in Coq the syntax of simple programming languages: variants of a simple imperative language and the simply-typed lambda calculus;

l define the big-step and small-step operational semantics of such simple languages;

l formally define type systems for such languages as inductive relations;

l work out the metatheory of such languages, by proving results such as type soundness;

l understand the semantic foundations of Hoare Logic and Relational Hoare Logic;

l use Hoare Logic for verifying the correctness of simple imperative programs, both formally in Coq and informally on paper;

l understand the semantic foundations of Secure Information Flow Control and Noninterference.

l use Relational Hoare Logic for proving program equivalence as well as Noninterference of simple imperative programs;

Inhalt
Complex proofs on paper are difficult to write, check, and maintain. This holds not only for interesting proofs in mathematics, but also for complex formal proofs about interesting programs. For this reason, machine-checked proofs created with the help of interactive tools called proof assistants are gaining increased traction in academia and industry. Proof assistants have been used to prove the correctness and security of realistic compilers, operating systems, cryptographic libraries, or smart contracts, and also to construct machine-checked proofs for challenging mathematical results.

This course will use the Coq proof assistant [2] to lay down the foundations of Programming Languages, Verification, and Security. The Coq proof assistant enables us to program formal proofs interactively and it machine-checks the correctness of the proofs along the way. We will use Coq to define the syntax and semantics of programming languages, to define type systems, and to prove theorems such as type soundness. We will also formalize Hoare Logic and Relational Hoare Logic in Coq and use them to prove the correctness and security of simple imperative programs. Finally, the course will introduce static and dynamic enforcement mechanisms for Secure Information Flow Control and Cryptographic Constant Time as well as their formal noninterference guarantees.

This hands-on course is based on the Programming Languages Foundations online textbook [1], which is itself formalized and machine-checked in the Coq proof assistant. The many exercises in each book chapter are to be solved weekly mostly in Coq, from easy exercises allowing the students to practice concepts from the lecture, building incrementally to slightly more interesting programs and proofs and also to various optional challenges.

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

Prüfungsformen
Written final exam (mandatory, 120 minutes) and exercise sheets.

Voraussetzungen für die Vergabe von Credits
There will be a mandatory written final exam (120 minutes) that counts for 60% of the grade and weekly exercise sheets that have to be submitted on time and that count for 40% of the grade. We will also have an optional midterm exam that helps students practice for the final exam, but only counts for bonus points, up to 10% of the final grade. One can additionally get bonus points up to 5% of the final grade by solving all exercise sheets.

To pass the course and receive credit points one has to attend the final exam and the weighed sum of your scores including bonus points (which can add up to a maximum of 115%) has to be at least 50%.

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

Titel des Moduls: Human Aspects of Cryptography Adoption
Human Aspects of Cryptography Adoption

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Wintersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Human Aspects of Cryptography Adoption	60 h	90 h	30 Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Englisch	Keine

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Prof. Dr. Martina Angela Sasse
Lehrende: Prof. Dr. Martina Angela Sasse

Verwendung des Moduls
Master IT-Sicherheit/ Informationstechnik

Master IT-Sicherheit/ Netze und Systeme

Vorkenntnisse
Keine

Lernziele (learning outcomes)
The aim of the lecture is to examine the reasons why

1. cryptographic solutions – which experts agree offer good protection against most oft the common attacks today – are not adopted by most individuals and organisations, and
2. end-users, developers and system administrators who do use cryptographic solutions in some form frequently make mistakes that undermine the security protection.

Inhalt
In 1999, Whitten & Tygar's seminal USENIX paper "Why Johnny Can't Encrypt" established that people cannot use PGP encryption correctly, even with a graphical user interface and instruction.

Over the past 20 years, there has been a string of Johnny papers on studies trying to encourage adoption or correct usage. The aim of this CASA lecture is to systematically examine the results of these studies and identify effective ways of promoting adoption and enable correct use of cryptography.

- Usability, utility and technology adoption
- Security threat models and people's mental models
- Complexity or simplicity – who needs to know what?
- Designing frictionless user journeys
- Methods for testing and tweaking

Lehrformen
Vorlesung mit Übung

Prüfungsformen
Mündliche Prüfung

Voraussetzungen für die Vergabe von Credits
Bestandene Modulabschlussprüfung

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

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

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

Titel des Moduls: Implementierung kryptographischer Verfahren

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Wintersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Implementierung kryptographischer Verfahren (212020)	60 h	90 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch	keine

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Prof. Dr.-Ing. Tim Güneysu
Lehrende: Dr.-Ing. Pascal Sasdrich

Verwendung des Moduls
B.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

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

Lernziele (learning outcomes)
Studierende erlernen die grundlegenden Algorithmen fur die effiziente Implementierung rechenintensiver Kryptoverfahren. Insbesondere den Umgang von Algorithmen mit sehr langen Operanden haben sie nach Abschluss des Moduls verstanden, ebenso wie das Zusammenspiel von Implementierungsmethoden und kryptographischer Sicherheit.

Inhalt
Diese Vorlesung gibt eine Einführung in Verfahren zur schnellen und sicheren Implementierung kryptographischer Algorithmen. Im ersten Teil werden Methoden zum effizienten Potenzieren ausführlich behandelt, da diese für alle verbreiteten asymmetrischen Verfahren von großer Bedeutung sind. Fur den weit verbreiteten RSA Algorithmus werden zudem spezielle Beschleunigungsverfahren vorgestellt. Im zweiten Teil werden Algorithmen für effiziente Langzahlarithmetik entwickelt. Zunächst werden grundlegende Methoden zur Darstellung von Langzahlen in Rechnern und Verfahren zur Addition vorgestellt. Der Schwerpunkt dieses Teils liegt auf Algorithmen zur effizienten modularen Multiplikation. Neben dem Karatsuba-Algorithmus wird die Montgomery-Multiplikation behandelt. Im dritten Teil werden sichere Implementierungen besprochen. Es erfolgt eine Einführung in aktive und passive Seitenkanalattacken. Es werden aktive Attacken gegen Blockchiffren und RSA vorgestellt. Als wichtige Vertreter der passiven Attacken werden die Grundlagen von SPA (simple power analysis) und DPA (differential power analysis) eingefuhrt.

Lehrformen
Vorlesung mit Übungen

Prüfungsformen
Die Endnote ergibt sich zu 70% aus einer Klausur (120 Minuten) und zu 30% aus studienbegleitenden Programmierprojekten (auch zum Nachschreibetermin)

Voraussetzungen für die Vergabe von Credits
Bestandene Modulabschlussprüfung

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

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

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

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

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

Titel des Moduls: Information Theory
Information Theory

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Sommersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Information Theory (211007)	60 h	90 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Englisch	

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Prof. Dr. Michael Walter
Lehrende: Prof. Dr. Michael Walter

Verwendung des Moduls
B.Sc. Informatik

B.Sc. IT-Sicherheit

M.Sc. Informatik

M.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

M.Sc. Angewandte Informatik

Vorkenntnisse
Familiarity with discrete probability (we will briefly remind you of the most important facts). Some experience with precise mathematical statements and rigorous proofs (since we’ll see many of those in the course). Part of the homework will require programming in Python.

Lernziele (learning outcomes)
You will learn fundamental concepts, algorithms, and results in information theory. After successful completion of this course, you will know the mathematical model of information theory, how to design and analyze algorithms for a variety of information processing tasks, and how to implement them in Python. You will have independently read about a topic in information theory and presented it to your peers. You will be prepared for an advanced course or a research or thesis project in this area. Please see the course homepage for a precise list of learning objectives.

Inhalt
This course will give an introduction to information theory – the mathematical theory of information. Ever since its inception, information theory has had a profound impact on society. It underpins important technological developments, from reliable memories to mobile phone standards, and its versatile mathematical toolbox has found use in computer science, machine learning, physics, electrical engineering, mathematics, and many other disciplines.

Starting from probability theory, we will discuss how to mathematically model information sources and communication channels, how to optimally compress information, and how to design error-correcting codes that allow us to reliably communicate over noisy communication channels. We will also see how techniques used in information theory can be applied more generally to make predictions from noisy data.

Tentative syllabus:

- Welcome, Introduction to Information Theory
- Probability Theory Refresher
- Numerical Random Variables, Convexity and Concavity, Entropy
- Symbol Codes: Lossless Compression, Huffman Algorithm
- Block Codes: Shannon’s Source Coding Theorem, its Proof, and Variations

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

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

Lehrformen
Lecture with Exercise

Prüfungsformen
Wird noch nachgeliefert

Voraussetzungen für die Vergabe von Credits

Passed Exam

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)
5/158: B.Sc. Informatik [PO 22]

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

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

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

5/97: M.Sc. Informatik

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

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

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

5/105: M.Sc. Angewandte Informatik

Titel des Moduls: Introduction to Blockchain Security
Introduction to Blockchain Security

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Wintersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
	60 h	90 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Englisch	

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Prof. Dr. Ghassan Karame
Lehrende: Prof. Dr. Ghassan Karame

Verwendung des Moduls
B.Sc. IT-Sicherheit

Vorkenntnisse
Hintergrundwissen in Systemsicherheit, Netzwerksicherheit, kryptographischen Primitiven (Verschlüsselungsmethoden, Signaturen, MACs, Hashfunktionen), Prinzipien von Kommunikationsnetzwerken, wird vorausgesetzt.

Lernziele (learning outcomes)

Nach Abschluss dieses Kurses sollen die Teilnehmer in der Lage sein:

- über die Sicherheits- und Datenschutzdefinitionen von offenen Zahlungssystemen nachzudenken.
- die Sicherheit von PoW-Blockchains vor dem Hintergrund des aktuellen Stands der Technik und der gemeldeten Angriffe zu erklären.
- die möglichen Netzwerksicherheits- und kryptografischen Gegenmaßnahmen zur Abwehr von Angriffen auf Blockchains erläutern zu können.
- die besten Sicherheits-/Privatsphärenpraktiken, um die Sicherheit bestehender Blockchains zu verbessern, erläutern und relevante Lehren für die Entwicklung von Blockchain-Technologien der nächsten Generation ziehen zu können.

Inhalt
Das Hauptziel des Kurses ist es, einen umfassenden Überblick über die Sicherheit und den Datenschutz von Blockchain-Technologien zu geben.

Die Kursteilnehmer werden auch in die grundlegenden Sicherheits- und Datenschutzbestimmungen bestehender populärer Währungen eingeführt und mit den neuesten Angriffen und Bedrohungen vertraut gemacht, die gegen bestehende Systeme/Einführungen gemeldet wurden. Die Teilnehmer werden auch über die Wirksamkeit der Kombination von Sicherheitsprimitiven auf Netzwerkebene mit neuartigen kryptographischen Primitiven zur Abwehr von Angriffen auf Zahlungssysteme nachdenken.

Lehrformen
Vorlesung mit Übung

Prüfungsformen
Schriftliche Modulabschlussprüfung (120 min)

Voraussetzungen für die Vergabe von Credits
Bestandene schriftliche Modulabschlussprüfung

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)
5/150: B.Sc. IT-Sicherheit [PO 22]

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

Titel des Moduls: Komplexitätstheorie
Complexity Theory

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	9 CP	270 h	siehe Prüfungsordnung	Unregelmäßig (i.d.R Sommersemester)	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Komplexitätstheorie	90 h	180 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Englisch	

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Prof. Thomas Zeume
Lehrende: Prof. Thomas Zeume

Verwendung des Moduls
M.Sc. Informatik

M.Sc. Angewandte Informatik

Vorkenntnisse
Kenntnisse aus einem Grundkurs in theoretischer Informatik (Grundlagen der Komplexitätstheorie einschließlich NP-Vollständigkeit und Reduktionen) werden erwartet.

Lernziele (learning outcomes)
Die Studierenden lernen, algorithmische Probleme bezüglich ihrer Komplexität einzuordnen und so geeignete algorithmische Techniken zu ihrer Lösung zu identifizieren. Sie können insbesondere algorithmische Methoden für NP-vollständige Probleme anwenden. Sie können mit unterschiedlichen Berechnungsmodellen umgehen und sind in der Lage, einfache Aussagen über sie zu beweisen. Sie lernen im Diskurs eigene und fremde Lösungsansätze zu bewerten.

Inhalt
Die Komplexitätstheorie untersucht und klassifiziert Berechnungsprobleme bezüglich ihrer algorithmischen Schwierigkeit. Ziel ist es, den inhärenten Ressourcenverbrauch bezüglich verschiedener Ressourcen wie Rechenzeit oder Speicherplatz zu bestimmen, und Probleme mit ähnlichem Ressourcenverbrauch in Komplexitätsklassen zusammenzufassen. Die bekanntesten Komplexitätsklassen sind sicherlich P und NP, die die in polynomieller Zeit lösbaren bzw. verifizierbaren Probleme umfassen. Die Frage, ob P und NP verschieden sind, wird als eine der bedeutendsten offenen Fragen der theoretischen Informatik, ja sogar der Mathematik, angesehen. P und NP sind jedoch nur zwei Beispiele von Komplexitätsklassen. Andere Klassen ergeben sich unter anderem bei der Untersuchung der des benötigten Speicherplatzes, der effizienten Parallelisierbarkeit von Problemen, der Lösbarkeit durch zufallsgesteuerte Algorithmen, und der approximativen Lösbarkeit von Problemen. Die Vorlesung hat das Ziel, einen breiten Überblick über die grundlegenden Konzepte und Resultate der Komplexitätstheorie zu geben:

- Klassische Resultate für Platz- und Zeitkomplexitätsklassen: z.B. die Korrespondenz zwischen Spielen und Speicherplatz-Beschränkungen, der Nachweis, dass sich mit mehr Platz oder Zeit auch mehr Probleme lösen lassen, weitere grundlegende Beziehungen zwischen Zeit- und Platzbasierten Klassen, und die Komplexitätswelt zwischen NP und PSPACE
- Grundzüge der Komplexitätstheorie paralleler, zufallsbasierter und approximativer Algorithmen
- Einführung in ausgewählte neuere Themen: Komplexitätstheorie des interaktiven Rechnens, des probabilistischen Beweisens und Fine-grained Complexity.

Lehrformen
Vorlesung mit Übungen

Prüfungsformen
Abschlussprüfung; mündlich, 20-30min

Voraussetzungen für die Vergabe von Credits
Bestandene mündliche Modulabschlussprüfung

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

9/105: M.Sc. Angewandte Informatik [PO22]

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

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

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

Titel des Moduls: Kryptographie auf hardwarebasierten Plattformen

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Wintersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Kryptographie auf hardwarebasierten Plattformen (212019)	60 h	90 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch	

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Prof. Dr.-Ing. Tim Güneysu
Lehrende: Prof. Dr.-Ing. Tim Güneysu

Verwendung des Moduls
B.Sc. IT-Sicherheit/ Informationstechnik

B.Sc. Angewewandte Informatik

M.Sc. IT-Sicherheit/ Netze und Systeme

M.Sc. Informatik

Vorkenntnisse

Lernziele (learning outcomes)

Die Studierenden kennen die Konzepte der praxisnahen Hardwareentwicklung mit abstrakten Hardwarebeschreibungssprachen (VHDL) und die Simulation von Hardwareschaltungen auf FPGAs. Sie beherrschen Standardtechniken der hardwarenahen Prozessorentwicklung und sind zur Implementierung von symmetrischen und asymmetrischen Kryptosystemen auf modernen FPGA-Systemen in der Lage.

Inhalt
Kryptographische Systeme stellen aufgrund ihrer Komplexität ins- besondere an kleine Prozessoren und eingebettete Systeme hohe Anforderungen. In Kombination mit dem Anspruch von hohem Datendurchsatz bei geringsten Hardwarekosten ergeben sich hier für den Entwickler grundlegende Probleme, die in dieser Vorlesung beleuchtet werden sollen. Die Vorlesung behandelt die interessantesten Aspekte, wie man aktuelle kryptographische Verfahren auf praxisnahen Hardwaresystemen implementiert. Dabei werden Kryptosysteme wie die Blockchiffre AES, die Hashfunk- tionen SHA-1 sowie asymmetrische Systeme RSA und ECC behandelt. Weiterhin werden auch spezielle Hardwareanforderungen wie beispielsweise der Erzeugung echten Zufalls (TRNG) sowie der Einsatz von Physically Unclo- nable Functions (PUF) besprochen. Die effiziente Implementierung dieser Kryptosysteme, insbesondere in Bezug auf die Optimierung für Hochgeschwindigkeit, wird auf modernen FPGAs besprochen und in praktischen Übungen mit Hilfe der Hardwarebeschreibungssprache VHDL umgesetzt. Vorlesungsbegleitend wird ein Moodle-Kurs angeboten, der zusätzliche Inhalte sowie die praktischen Übungen bereithält.

Lehrformen
Vorlesung mit Übung

Prüfungsformen
Schriftliche Modulabschlussprüfung (120 Minuten)

Voraussetzungen für die Vergabe von Credits
Bestandene schriftliche Modulabschlussprüfung; Durch die erfolgreiche Teilnahme am Übungsbetrieb können bis zu 10 Prozent Bonuspunkte erworben werden, die auf das Ergebnis der Modulklausur angerechnet werden können.

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

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

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

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

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

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

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

5/97: M.Sc. Informatik

Titel des Moduls: Kryptographische Protokolle

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Sommersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Kryptographische Protokolle (211031)	60 h	90 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Englisch	

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Prof. Dr. Eike Kiltz
Lehrende: Prof. Dr. Eike Kiltz

Verwendung des Moduls
M.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

M.Sc. Angewandte Informatik

Vorkenntnisse
Inhalte des Moduls Kryptographie

Lernziele (learning outcomes)
- Vertiefung des Verständnisses für beweisbare Sicherheit
- Schreiben von fehlerfreien Sicherheitsreduktionen
- Neue Techniken für Sicherheitsbeweise
- Erlernen fortgeschrittener kryptographischer Konstruktionen

Inhalt

Die Vorlesung beschäftigt sich mit erweiterten kryptographischen Protokollen und deren Anwendungen.
Themenübersicht:

- Game-based security definitions and proofs
- Bilinear maps
- Digital Signatures
- Identification Protocols
- Zero-Knowledge Proofs
- Identity-based Encryption
- CCA-secure encryption

Lehrformen
Vorlesung mit Übung

Prüfungsformen
Mündliche (30 Minuten) oder schriftliche Modulabschlussprüfung (120 Minuten)

Voraussetzungen für die Vergabe von Credits
Bestandene Modulabschlussprüfung.

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

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

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

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

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

5/105: M.Sc. Angewandte Informatik

Titel des Moduls: Master Praktikum/Projektarbeit IT-Sicherheit

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	4 CP	120 h	3	jedes Semester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
• Praktische Kryptanalyse von symmetrischen Chiffren (211401) • Projekt Netz- und Datensicherheit (212412) • Forschungspraktikum Human-Centred Security (212408) • Initial Research in Information Security (212402) • Praktikum TLS Implementierung (212414) • Praktikum zur Hackertechnik (Hackerpraktikum) (212413) • Research in Software/Internet Security (2124) • Master-Praktikum ARM Processors for Embedded Cryptography (212407) • Developer Centered Security (212417) • Praktikum Wireless Physical Layer Security (142025)	je nach Veranstaltungswahl	abhängig von der Praktikumswahl	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
abhängig von der Praktikumswahl: Deutsch oder Englisch	

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Studiendekan IT-Sicherheit
Lehrende: siehe Praktikumsbeschreibung

Verwendung des Moduls
M.Sc. IT-Sicherheit / Informationstechnik

M.Sc. IT-Sicherheit / Netze und Systeme

Vorkenntnisse
abhängig vom gewählten Praktikum

Lernziele (learning outcomes)

Nach dem erfolgreichen Abschluss des Moduls

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

Inhalt
Es werden aktuell Praktika zu folgenden Themen angeboten:

- Praktische Kryptanalyse von symmetrischen Chiffren
- Projekt Netz- und Datensicherheit
- Forschungspraktikum Human-Centred Security
- Laborstudien Human-Centred Security
- Initial Research in Information Security
- Praktikum TLS Implementierung
- Praktikum zur Hackertechnik (Hackerpraktikum)
- Research in Software/Internet Security
- Master-Praktikum ARM Processors for Embedded Cryptography

- Developer Centered Security (Projekt)
- Praktikum Wireless Physical Layer Security

Weiterführende Informationen zu den jeweiligen Praktika finden Sie im Vorlesungsverzeichnis.

Lehrformen
Praktikum im Block oder als semesterbegleitende Veranstaltung

Prüfungsformen
Praktikum

Voraussetzungen für die Vergabe von Credits

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

Titel des Moduls: Menschliches Verhalten in der IT-Sicherheit

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Sommersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Menschlisches Verhalten in der IT-Sicherheit (211033)	60 h	90 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch	Keine

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Prof. Dr. Martina Angela Sasse
Lehrende: Prof. Dr. Martina Angela Sasse
M. Sc. Jonas Hielscher

Verwendung des Moduls
M.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

Vorkenntnisse
Der vorherige Besuch der Vorlesung "Einführung in die Usable Security and Privacy" wird empfohlen

Lernziele (learning outcomes)
Die Veranstaltung vermittelt theoretische und praktische Kenntnisse uber Forschungs- ¨ methoden im Bereich usable Security mit einem besonderen Schwerpunkt auf Laborstudien. Es werden theoretische Kenntnisse vermittelt, auf deren Grundlage die Studierenden selbstst¨andig eine Laborstudie planen und umsetzen und auf diese Weise praktische Kenntnisse erwerben sollen.

Inhalt
In *Menschliches Verhalten in der IT-Sicherheit* lernt ihr, welche Faktoren Einfluss auf das Sicherheitsverhalten von Angestellten in Unternehmen und Nutzenden im Alltag nehmen, und welche Möglichkeiten bestehen, dieses zu beeinflussen und verändern. Außerdem wird vermittelt, warum bestehende Ansätze des Information Security Management (auch nach ISO 27000) in der Praxis oft nicht funktionieren und wie wir sie erweitern bzw. anpassen sollten. Studierende werden befähigt IT-Sicherheit in Organisationen aus einem ganzheitlichen Ansatz heraus zu betrachten, was unter anderem zwingend erforderlich ist um später Sicherheitsführungsaufgaben wahrzunehmen. Die Vorlesungsinhalte sind dabei umfangreich mit Erfahrungen aus der Praxis angereichert.

Lehrformen
Vorlesung und Übung

Prüfungsformen
Schriftliche Modulabschlussprüfung (120 Minuten)

Voraussetzungen für die Vergabe von Credits
Bestandene Modulabschlussprüfung

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

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

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

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

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

Titel des Moduls: Message Level Security
Message Level Security

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Wintersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Message-Level Security (212060)	60 h	90 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch	

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Dr.-Ing. Christan Mainka
Lehrende: Dr.-Ing. Christan Mainka
Dr.-Ing. Vladislav Mladenov

Verwendung des Moduls
B.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

Vorkenntnisse
Grundkenntnisse HTTP, HTML und Kryptographie
Grundkenntnisse der englischen Sprache, da dies die Sprache von Foliensatz, Übungsaufgaben und der Virtuellen Maschine sind

Lernziele (learning outcomes)
Studierende verfügen nach erfolgreichem Abschluss der Vorlesung über ein umfassendes Verständnis der Sicherheit der folgenden Technologien: Datenformate im Web, REST APIs, Authentifizierungs- und Autorisierungsprotokollen und Dokumentenformaten. Durch die praxisnahe Arbeit im Rahmen der Übungen bauen die Studierenden ihre Recherche-Fähigkeiten aus und erlernen weiterhin den sicheren Umgang mit verschiedenen Penetrationswerkzeugen. Am Ende der Vorlesung sind die Studierenden in der Lage, systematisch umfassende Sicherheitsanalysen sowie praktische Angriffe auf die behandelten Technologien selbstständig durchzuführen. Weiterhin sind die Studierenden in der Lage, das erlernte Wissen auf andere Technologien zu übertragen und komplexere Angriffsmöglichkeiten selbst durch kreatives Denken zu finden und auszunutzen.

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

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

- **JSON** ist eine universelle Datenbeschreibungssprache, die unter anderem von jedem modernen Browser unterstützt wird. Mithilfe von JSON-Signature und JSON-Encryption können JSON Nachrichten direkt geschützt werden. Doch reicht das aus oder können diese Sicherheitsmechanismen umgangen werden?
- **OAuth** ist eine sehr weitverbreitete Technologie zum Delegieren von Berechtigungen und wird heutzutage von allen großen Webseiten wie Facebook, Google, Twitter, Github usw. eingesetzt. Die Vorlesung erklärt tiefgehende Details und gängige Fehler/Angriffe, die bei der Verwendung von OAuth entstehen können.
- **OpenID Connect** ist eine Erweiterung für OAuth, um Benutzer:innen auf Webseiten mithilfe eines Drittanbieters zu authentifizieren (z. B. mittels Single Sign-On Verfahren wie „Sign in with Google“). OpenID Connect hat sich in den letzten Jahren zum de facto Standard für Web-Logins über Drittanbieter etabliert. In der Vorlesung wird detailliert erklärt, was die Unterschiede zu OAuth sind und welche Angriffe auf OpenID Connect möglich sind. In den praktischen Übungen können Sie Ihre Exploit-Fähigkeiten unter Beweis stellen. Schaffen wir es, den Account des Opfers übernehmen?
- **SAML** steht für Security Assertion Markup Language und ist ein Single Sign-On Standard, der eine weitgehende Verbreitung in Business-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 Studierenden wird ein tiefgehendes Verständnis der Systeme vermittelt. Zu allen untersuchten Systemen werden Angriffe vorgestellt, die sowohl aus der akademischen Welt als auch aus der Pentesting-Community stammen. Die Übungen bieten die Möglichkeit, das erlernte Wissen praktisch auszuprobieren. Hierzu erhalten die Studierenden eine virtuelle Maschine.

Lehrformen
Vorlesung mit Übung

Prüfungsformen
Schriftliche Modulabschlussprüfung (120 Minuten)

Voraussetzungen für die Vergabe von Credits
Bestandene schriftliche Modulabschlussprüfung

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

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

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

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

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

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

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

Titel des Moduls: Microarchitectural Attacks and Defenses

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h		Wintersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
212064 - Microarchitectural Attacks and Defenses	90 h		Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Englisch	none

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Prof. Yuval Yarom
Lehrende: Prof. Yuval Yarom

Verwendung des Moduls
Master ITS - Informationstechnik

Master ITS - Netze und Systeme

Vorkenntnisse
The course assumes that students can program in C or learn the language as they go. They need enough experience to be able to program on remote machines, using SSH. Basic understanding of how computers work, assembly language, and the role of the operating system is required. Understanding of basic concepts in computer security (security domains, vulnerabilities, etc.) and familiarity with basic cryptography (AES, RSA, ECC) is helpful.

Lernziele (learning outcomes)
• Diagnose microarchoitectural vulnerabilities
• Assess software for resilience against microarchitectural vulnerabilities
• Design and program proof-of-concept exploits of vulnerable software and hardware
• Design and implement countermeasures for software executing on vulnerable hardware

Inhalt
The course covers the area of microarchitectural attacks and defences. It starts with cache attacks, covering the main techniques (Prime+Probe, Evict+Time, and Flush+Reload). Building on this basis it explores variants of the attacks targetting other storage elements as well as attacks that exploits bandwidth limitations. In parallel with exploring these attacks, the course will describe various countermeasures, with special focus on constant-time programming. The course then switches to speculative execution attacks, identifying and classifying the various attacks, defences, and counter-attacks. The course further covers several related attacks, including Rowhammer and voltage- and frequency-based attacks. Additionally, the course pays special attention to attack scenarios exploring, in particular, attacks on the operating system kernel, web-based and other remote attacks, and attacks on trusted execution environments. The course puts special focus on practical implementation of both attack and defence techniques.

Lehrformen
Lecture with excercise

Prüfungsformen
Assignments and practical projects.

Voraussetzungen für die Vergabe von Credits

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

Titel des Moduls: Processor Security
Processor Security

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Sommersemester	Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Processor Security (211099)	60 h	90 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch	

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Dr.-Ing. Pascal Sasdrich
Lehrende: Dr.-Ing. Pascal Sasdrich

Verwendung des Moduls

B.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

Vorkenntnisse
Inhalte der Module „Informatik 1 – Programmierung“ und „Technische Informatik 1 – Rechnerarchitektur“

Lernziele (learning outcomes)
Im Rahmen dieser Veranstaltung lernen die Studierenden wichtige Sicherheitsaspekte und -konzepte moderner Prozessoren kennen. Der Fokus der Veranstaltung liegt dabei auf (a) Kenntnis gängiger Angriffsvektoren, (b) Verständnis der zugrundeliegenden Hardware- und Prozessormechanismen, (c) Diskussion möglicher Gegenmaßnahmen, sowohl in Hardware als auch Software.

Inhalt
Moderne Prozessorenarchitekturen, von eingebetteten Mikrocontrollern bis hin zu Server-CPUs, bilden das Kernstück unserer heutigen Informationsgesellschaft und werden seit Jahrzehnten immer komplizierter. Diese gesteigerte Komplexität führt aber unausweichlich zu neuen Schwachstellen und gesteigerter Anfälligkeiten gegen gezielte Angriffe.
Im Rahmen dieser Veranstaltung werden daher verschiedene Sicherheitsaspekte und -konzepte moderner Prozessorarchitekturen vorgestellt und erläutert.
Dazu werden sowohl wichtige Angriffsvektoren (z.B. Buffer Overflows, Privilege Escalation, Control-Flow Manipulation, Side Channel Attacks, Microarchitectural Attacks, …), fundamentale Ursachen in der Prozessorarchitektur, als auch mögliche Abwehrstrategien diskutiert.

Vorlesungsbegleitend wird ein Moodle-Kurs angeboten, der zusätzliche Inhalte sowie die praktischen Übungen bereithält.

Lehrformen
Vorlesung mit Übung

Prüfungsformen
Schriftliche Modulabschlussprüfung (120 Minuten)

Voraussetzungen für die Vergabe von Credits

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

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

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

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

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

Titel des Moduls: Programmanalyse

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Sommersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Programmanalyse (211015)	60 h		Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Englisch	keine

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Prof. Kevin Borgolte
Lehrende: Prof. Kevin Borgolte

Verwendung des Moduls
M.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

Vorkenntnisse
keine

Lernziele (learning outcomes)
Die Studierenden kennen verschiedene Konzepte, Techniken und Tools aus dem Bereich der Programmanalyse. Dies beinhaltet den Überblick über verschiedene Konzepte aus dem Bereich Reverse Engineering sowie Binäranalyse. Die Studierenden haben grundlegendes Verständnis von sowohl statischen als auch dynamischen Methoden zur Analyse eines gegebenen Programms. Sie sind in der Lage, verschiedene Aspekte der Programmanalyse zu beschreiben und auf neue Problemstellungen anzuwenden.

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

- Statische und dynamische Analyse von Programmen
- Analyse von Kontroll- und Datenfluss
- Symbolische Ausführung
- Taint Tracking
- Binary Instrumentation
- Program Slicing
- Überblick zu existierenden Analysetools

Daneben wird im ersten Teil der Vorlesung eine Einführung in x86/x64 Assembler gegeben sowie die grundlegenden Techniken aus dem Themenbereich Reverse Engineering vorgestellt. Begleitet wird die Vorlesung von Übungen, in denen die vorgestellten Konzepte und Techniken praktisch eingeübt werden.

Lehrformen
Vorlesung mit Übung

Prüfungsformen
mündliche oder schriftliche Modulabschlussprüfung (wird zu Beginn des Semester bekanntgegeben), Anmeldung: FlexNow

Voraussetzungen für die Vergabe von Credits
Bestandene Modulabschlussprüfung

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

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

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

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

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

Titel des Moduls: Proofs are programs
Proofs are programs

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Sommersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Proofs are Programms (211003)	60 h	90 h	40 Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Englisch	keine

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Dr. Catalin Hritcu
Lehrende: Dr. Catalin Hritcu
Dr. Clara Schneidewind

Verwendung des Moduls
B.Sc. Informatik

B.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

Vorkenntnisse

Lernziele (learning outcomes)
After successful completion of this course, students will be able to

- develop purely functional programs using recursive functions on numbers, lists, maps, and various kinds of trees, including the abstract syntax trees of programs;
- use functional programming concepts such as type polymorphism and higher-order functions, which are increasingly becoming mainstream;
- formally state and prove theorems in the Coq proof assistant;
- apply different proof techniques in Coq (e.g. equational reasoning, contradiction, case analysis, induction on natural numbers, structural induction, proof automation);
- define new inductive types and relations in Coq and prove statements about them;
- understand the connection between constructive logics and typed functional programming that is at the heart of Coq, in which propositions are types and proofs are programs;
- understand how the syntax and semantics of simple imperative programs can be formally defined in Coq and how to prove theorems about such programs and languages.

Inhalt
Complex mathematical proofs on paper are difficult to write, check, and maintain. This holds not only for interesting proofs in mathematics, but also for complex formal proofs about interesting programs. For this reason, machine-checked proofs created with the help of interactive tools called proof assistants are gaining increased traction in academia and industry. Proof assistants have been used to prove the correctness and security of realistic compilers, operating systems, cryptographic libraries, or smart contracts, and also to construct machine-checked proofs for challenging mathematical results such as the four color theorem, the odd-order theorem (Feit–Thompson), or the construction of perfectoid spaces.

This course introduces the Coq proof assistant and explains how to use it to prove properties about functional programs and inductive relations. The Coq proof assistant enables us to program formal proofs interactively and it machine-checks the correctness of the proofs along the way. The design of the Coq proof assistant itself exploits a beautiful connection between programs in typed functional programming languages and proofs in constructive logics, which is known as the Curry-Howard Correspondence. This deep connection between programs and proofs should make this course interesting to both computer scientists and mathematicians. For computer

scientists the goal is to demystify proofs as just programs in an elegant programming language, for which the course provides a gentle introduction. For mathematicians this course serves as an introduction to functional programming and also to the idea that proofs are not only a way to convince a human reader, but they can actually be fully formalized in a proof assistant like Coq and automatically checked by a computer.

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

Lehrformen

Prüfungsformen

Voraussetzungen für die Vergabe von Credits

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

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

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

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

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

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

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

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

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

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

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Sommersemester	Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Public Key Kryptanalyse 1 (211055)	45 h	105 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch	keine

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

Verwendung des Moduls

Vorkenntnisse
Vorausgesetzt werden elementare Kenntnisse der Lineare Algebra (Mathematik 1 für Informatiker) und ein Interesse an algorithmischen Techniken und Kryptographie, in Theorie und Praxis (umgesetzt mit Hilfe des Computeralgebra-Systems Sage).

Lernziele (learning outcomes)
Die Studierenden sollen breite Kenntnisse zu algorithmischen Techniken der asymmetrischen Kryptanalyse, insbesondere für codierungsbasierte Kryptographie, erlangen.

Nach dem erfolgreichen Abschluss des Moduls

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

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

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

Prüfungsformen
Schriftliche Modulabschlussprüfung über 120 Minuten

Voraussetzungen für die Vergabe von Credits

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

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

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

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

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

Titel des Moduls: Public Key Verschlüsselung

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Wintersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Public Key Verschlüsselung	60 h	90 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch	

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Jun. Prof. Dr. Nils Fleischhacker
Lehrende: Jun. Prof. Dr. Nils Fleischhacker

Verwendung des Moduls
M.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

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

Lernziele (learning outcomes)
Die Studierenden haben einen Einblick in in theoretische und praktische Aspekte der Public Key Verschlüsselung erhalten

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

Lehrformen
Vorlesung mit Übung

Prüfungsformen
Mündlich (30 Minuten)

Voraussetzungen für die Vergabe von Credits
Bestandene Modulabschlussprüfung

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

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

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

Titel des Moduls: Quantum Cryptography
Quantum Cryptography

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Wintersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Quantum Cryptography (212016)	60 h	90 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Englisch	keine

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

Verwendung des Moduls
M.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

Vorkenntnisse
keine

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

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

Topics to be covered will likely include:

* Basic quantum computing

* Basic cryptography

* Quantum attacks on classical cryptography

* Quantum random oracles and compressed oracle technique

* Quantum-resistant cryptography in light of the NIST competition

* Classical vs quantum information

* Quantum money

* Quantum key distribution

* Quantum complexity theory

* Quantum pseudorandomness

* From classical to quantum fully homomorphic encryption

* Classical verification of quantum computation

* Quantum rewinding

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

Lehrformen
Vorlesung mit Übungen

Prüfungsformen
Modulabschlussprüfung; schriftlich oder mündlich je nach Teilnehmendenzahl.

Voraussetzungen für die Vergabe von Credits
Bestandene Modulabschlussprüfung

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

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

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

Titel des Moduls: Red- and Blue-Teaming
Red- and Blue-Teaming

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Sommersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Red- and Blue Teaming (212024)	60 h	90 h	30 Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch (Material auf Englisch)	

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

Verwendung des Moduls
B.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

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

Gute Kenntnisse der internen Funktionsweise von Linux und Windows Betriebssystem (s. u. Buchempfehlungen)
Der Umgang mit Bash und Powershell sollte für jeden Teilnehmer selbstverständlich sein
Absolvieren des Wargames "Bandit" von Overthewire.org
Gute Englischkenntnisse
Da der Kurs sehr ins Detail geht werden folgende Buchempfehlungen zu den Internas der Betriebssysteme ausgesprochen: How Linux works (3rd Edition, ISBN-13: 9781718500402), Windows Internals Part 1 (ISBN-13: 978-0735684188)

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

Inhalt
Die bisher geplanten Inhalte sind wie folgt aufgeschlüsselt:

Theorie:

- Einführung in das Thema Sicherheitsüberprüfungen (Kategorien, Nutzen/Ziele, Planung und Ablauf)
- Red Teaming: Ursprünge und Geschichte des Red Teamings; Wichtige Standards, Best Practices und Organisationen; Arten, Aufgaben und Ziele eines Red Team Einsatzes; Planung, Ablauf und Nachbereitung eines Red Teaming Einsatzes
- Blue Teaming: Einführung ins Blue Teaming; Wichtige Standards, Best Practices und Organisationen; Arten, Aufgaben und Ziele eines Blue Teams; Planung und Aufbau eines Blue Teams in der Organisation
- Angriffe: Windows Clients und Server Systeme (inkl. Active Directory Domainen); Linux Server und Clients; Simulation von APTs auf Basis von Threat Modelling und dem MITRE ATT&CK Framework

Praxis:

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

Lehrformen
Blockkurs in der vorlesungsfreien Zeit

Prüfungsformen
Schriftliche Modulabschlussprüfung (120 Minuten)

Voraussetzungen für die Vergabe von Credits
Bestandene schriftliche Modulabschlussprüfung

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

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

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

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

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

Titel des Moduls: Software Protection
Software Protection

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Sommersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Software Protection (211107)	45 h	105 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch	keine

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Professur für Systemsicherheit
Lehrende: Dr.-Ing. Tim Blazytko
Philipp Koppe

Verwendung des Moduls
B.Sc. IT-Sicheheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

Vorkenntnisse
Im Bereich Reverse Engineering sind empfohlen, beipielsweise durch Erfahrung mit x86-Assembler. Erfahrung in systemnaher Programmierung (Assembler, C) ist hilfreich.

Lernziele (learning outcomes)
Die Studierenden kennen verschiedene Konzepte, Techniken und Tools aus dem Bereich Software Protection. Dies beinhaltet sowohl Wissen über das Design und die Implementierung von Obfuskierungstechniken als auch die Sicherheitsanalyse gängiger Systeme. Die Studierenden lernen erweiterte Techniken zur Programmanalyse, mit welchen sie komplexe Protection-Mechanismen angreifen können. Sie sind in der Lage, verschiede Aspekte der Software Protection zu beschreiben und auf neue Problemstellungen anzuwenden.

Inhalt
Unter Software Protection versteht man Maßnahmen, welche die Analyse bzw. das Reverse Engineering von Software erschweren. Solche Methoden finden sowohl Anwendung in kommerzieller Software, um Piraterie zu verhindern, als auch in Malware, um deren Funktionsweise zu verschleiern.

In dieser Lehrveranstaltung lernen die Studierenden gängige Methoden der Software Protection kennen sowie Methoden, um diese zu brechen. Dazu designen und implementieren sie in praxisnahen Aufgaben erst ihre eigenen Protection-Mechanismen, welche sie im Anschluss brechen werden mit dem Ziel, diese wieder zu verbessern. Parallel dazu werden Schutzmechanismen aus der echten Welt analysiert, attackiert und diskutiert.

Dabei werden unter anderem die folgenden Themen und Techniken aus dem Bereich Software Protection behandelt:

- Opaque Predicates

- Control-flow Flattening

- Mixed Boolean-Arithmetic Expressions

- Virtual Machines

- Anti-Tamper

- Symbolische Ausfuehrung

- SMT Solving

- Programmsynthese

- Überblick zu existierenden Analysetools und Frameworks

Lehrformen
Vorlesung mit Übung

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

Voraussetzungen für die Vergabe von Credits
Erfolgreiche Kompetenznachweis im Semester

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

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

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

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

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

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

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

Titel des Moduls: Software Security
Software Security

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	9 CP	270 h	siehe Prüfungsordnung	Wintersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Software Security (212026)	60 h	210 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Englisch	Keine

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Prof. Kevin Borgolte
Lehrende: Prof. Kevin Borgolte

Verwendung des Moduls
M.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

M.Sc. Angewandte Informatik

Vorkenntnisse
Keine

Lernziele (learning outcomes)

Inhalt

Lehrformen
Vorlesung mit Übung

Prüfungsformen
Schriftliche Hausarbeit (Take-Home-Exam) am Ende der Vorlesungszeit und ggf. mündlicher Vortrag.

Voraussetzungen für die Vergabe von Credits
Bestandene Hausarbeit und ggf. mündliche Vortrag.

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)
5/91: M.Sc. IT-Sicherheit/ Informationstechnik

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

5/105: M.Sc. Angewandte Informatik

Titel des Moduls: Software-Implementierung kryptographischer Verfahren

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Sommersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Software-Implementierung kryptographischer Verfahren (211035)	60 h	90 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch	keine

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Prof. Dr.-Ing. Tim Guneysu
Lehrende: Dr.-Ing. Max Hoffmann

Verwendung des Moduls
B.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

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

Lernziele (learning outcomes)
Die Studierenden haben ein Verständnis für Methoden für die schnelle Software-Realisierung ausgewählter Krypto-Verfahren und diese selbst implementiert.

Inhalt
Es werden ausgewählte fortgeschrittene Implementierungstechniken der modernen Kryptographie behandelt.

Inhalte:

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

Lehrformen
Vorlesung mit Übungen

Prüfungsformen
Schriftliche Modulabschlussprüfung (120 Minuten)

Voraussetzungen für die Vergabe von Credits

Es müssen mindestens 50 Prozent aller möglichen Punkte in der Klausur und den semesterbegleitenden Projekten erreicht werden.

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

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

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

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

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

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

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

Titel des Moduls: Symmetrische Kryptanalyse

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Wintersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Symmetrische Kryptanalyse	60 h	90 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch	

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Prof. Dr. Nils-Gregor Leander
Lehrende: Prof. Dr. Nils-Gregor Leander

Verwendung des Moduls
M.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

M.Sc. Angewandte Informatik

Vorkenntnisse
Inhalt der Vorlesung "Einführung in die Kryptographie 1"

Lernziele (learning outcomes)
Die Studierenden haben ein vertieftes Verständnis für die Sicherheit symmetrischer Chiffren.

Inhalt

Wir behandeln die wichtigsten Themen in der symmetrischen Kryptanalyse. Nach einer ausführlichen Vorstellung von linearer und differentieller Kryptanalyse werden weitere Angriffe auf symmetrische Primitive, insbesondere Block-Chiffren behandelt. Hierzu zählen insbesondere Integral (auch Square) 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.

Lehrformen

Prüfungsformen
Mündliche Modulabschlussprüfung (30 Minuten)

Voraussetzungen für die Vergabe von Credits
Bestandene mündliche Modulabschlussprüfung.

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

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

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

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

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

5/105: M.Sc. Angewandte Informatik

Titel des Moduls: Usable Security
Usable Security

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	4	Sommersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Einführung in die Usable Security and Privacy (211036)	60 h		100 Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch	

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Prof. Dr. Angela Sasse
Lehrende: Prof. Dr. Angela Sasse
M.A. Jennifer Friedauer

Verwendung des Moduls
B.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

Vorkenntnisse
Allgemeine Kenntnisse der IT-Sicherheit

Lernziele (learning outcomes)

Die Studierenden verstehen, warum die Usability technischer Systeme entscheidenden Einfluss auf deren Sicherheit haben kann. Darüber hinaus sollen Sie in die Lage versetzt werden, einfache Stu dien zur Usability selbst durchzuführen.

Inhalt
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

Lehrformen
Vorlesung mit Übung

Prüfungsformen
schriftliche Modulabschlussprüfung (120 Minuten)

Voraussetzungen für die Vergabe von Credits
Bestandene schriftliche Modulabschlussprüfung

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

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

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

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

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

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

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	3 CP	90 h		jedes Semester	Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
211104 Human Centred Security and Privacy 211110 Seminar Real-World Kryptanalyse 211114 Master-Seminar on Security and Privacy of Mobile Operating Systems 211117 Seminar Satisfiability (bis SoSe 23) 211119 Quantum Algorithms (bis SoSe 23) 211121 Fortgeschrittene Themen des Model Checking ( ) 211122 Seminar über Grenzen in der theoretischen Informatik ( ) 211129 Master-Seminar Developer Centered Security 211132 Master-Seminar Digitale Souveränität 211133 Seminar on Current Topics for Systems Security and Privacy 212109 Information Security Seminar 212111 Seminar Ressourceneffiziente Systemsoftware 212112 Seminar Security Engineering 212118 Seminar zur symmetrischen Kryptographie 212121 Seminar Netz- und Datensicherheit 212122 Seminar Current Topics in Device Firmware Security 212125 Software and Internet Security Seminar 212126 Seminar Implementation Security (bis SoSe 23)	30 h		Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch oder Englisch	

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Studiendekan IT-Sicherheit
Lehrende: siehe jeweiliges Seminar

Verwendung des Moduls
B.Sc. IT-Sicherheit

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

Lernziele (learning outcomes)

Nach dem erfolgreichen Abschluss des Moduls

- verfügen Studierende über vertiefte wissenschaftliche Kenntnisse in dem ausgewählten Seminarthema
- haben Studierende das halten eines wissenschaftlichen Vortrags praktisch eingeübt und können Forschungsergebnisse eigenständig in einem didaktisch wohl aufbereiteten Vortrag vermitteln
- können die Teilnehmer konstruktives Feedback formulieren und entgegennehmen

Inhalt

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

Lehrformen

Seminar

Prüfungsformen

Seminarvortrag

Voraussetzungen für die Vergabe von Credits

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

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

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

Titel des Moduls: Web-und Browsersicherheit

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Wintersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Web- und Browsersicherheit (212061)		90 h	30 Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Vorlesung und Prüfung finden in Englisch statt.	

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Prof. Dr. Jörg Schwenk
Lehrende: Dr.-Ing. Mario Heiderich

Verwendung des Moduls
B.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

Vorkenntnisse

Grundkenntnisse in Webprogrammierung
Gute Englischkenntnisse

Lernziele (learning outcomes)

Studierende verfügen nach erfolgreichem Abschluss des Moduls über ein umfassendes Verständnis der technischen Aspekte von Web- und Browsersicherheit. Sie haben ein umfassendes Systemverständnis für komplexe Webanwendungen erworben. Durch eigenständige Überlegungen und deren Umsetzung in praktischen Projekten zur Verbesserung der Netzsicherheit bereiten sich die Studierenden auf ihre Rolle im Berufsleben vor. Sie können neue Probleme analysieren und neue Lösungsmöglichkeiten entwickeln. Sie können im Gespräch den Nutzen
der von ihnen erarbeiteten Lösungen argumentativ begründen.

Inhalt
Die Vorlesung wird als Blockveranstaltung angeboten. Die Veranstaltung ist auch für Studierende geeignet, die bereits XML- und Webservicesicherheit/Websicherheit gehört haben und ihr Wissen vertiefen möchten. Dies ist jedoch keine Voraussetzung.

What to bring:

- A Laptop, OS doesn’t matter
- Working Internet Connection

Kapitel 1: History & Basics

- The History of Web Security and Web Attacks
- The History of Browsers
- HTML, JavaScript, CSS

Kapitel 2: HTTP, Server, SQLi

- Attacks using HTTP and SSL/TLS
- SQL Injections
- Uploads
- SSRF, XXE & XEE

Kapitel 3: Cookies, Sessions, XSS

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

Kapitel 4: Advanced XSS

- Advanced XSS
- mXSS and DOM Mutations

Kapitel 5: Browsers & Beyond

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

Kapitel 6: Sandboxing & Random Bits

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

Lehrformen
Blockveranstaltung in der vorlesungsfreien Zeit

Prüfungsformen
Schriftliche Modulabschlussprüfung (120 Minuten)

Voraussetzungen für die Vergabe von Credits
Bestandene schriftliche Modulabschlussprüfung

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

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

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

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

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

Titel des Moduls: Zero-Knowledge Proof Systems
Zero-Knowledge Proof Systems

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	5 CP	150 h	siehe Prüfungsordnung	Sommersemester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
Ze-ro-Know-ledge Proof Sys-tems (211032)	60 h	90 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Deutsch	keine

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Jun. Prof. Dr. Nils Fleischhacker
Lehrende: Jun. Prof. Dr. Nils Fleischhacker

Verwendung des Moduls
M.Sc. IT-Sicherheit/ Informationstechnik

M.Sc. IT-Sicherheit/ Netze und Systeme

Vorkenntnisse
Einführung in die Kryptographie

Lernziele (learning outcomes)

A deep understanding of the Foundations and Applications of Zero-Knowledge Proof Systems. This includes an understanding of the necessary underlying assumptions, the lower bound on what is possible to achieve, as well as efficient instantiations from concrete assumptions.

Inhalt
Zero-Knowledge protocols are important building blocks for more complex cryptographic protocols. This class covers foundational aspects of zero-knowledge proofs, including: Lower bounds and round complexity, necessary assumptions, communication complexity, and zero-knowledge in a quantum world, as well as theoretical and practical constructions and their security proofs.

Topics:

Cryptography, Interactive Proof Systems, Zero-Knowledge Proofs, Provable Security

Lehrformen
Lecture with exercise

Prüfungsformen
Written Exam / Oral Exam
The form of examination will be determined at the beginning of the lecture.

Voraussetzungen für die Vergabe von Credits
Bestandene Modulabschlussprüfung

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

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

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

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

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

Titel des Moduls: Freie Wahlmodule
free electives

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	17 CP				Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
	siehe Lehrveranstaltungen		Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
	siehe Lehrveranstaltungen

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r:
Lehrende:

Verwendung des Moduls

Vorkenntnisse

Lernziele (learning outcomes)

Die Studierenden beherrschen entsprechend ihrer Wahl verschiedene, das Studium ergänzende Schlüsselqualifikationen und haben ihr Fachwissen vertieft.

Inhalt
Durch die freie Wahl von Lehrveranstaltungen aus dem gesamten Angebot der RUB, UARuhr und UNIC können die Studierenden fachliche und überfachliche Schwerpunkte anhand ihrer eigenen Interessen setzen.

Je nach Veranstaltungswahl werden unterschiedliche Inhalte vermittelt.

Lehrformen

Prüfungsformen

Voraussetzungen für die Vergabe von Credits

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

unbenotet

Titel des Moduls: Masterarbeit und Kolloquium (ITS)

Modul-Nr./Code	Credits	Workload	Semester	Turnus	Dauer
	30 CP	900 h	4	jedes Semester	1 Semester

Lehrveranstaltungen	Kontaktzeit	Selbststudium	Gruppengröße
	15h	885 h	Studierende

Unterrichtssprache	Teilnahmevoraussetzungen
Englisch oder Deutsch	Erfolgreich abgeschlossene Module im Umfang von 70 CP (PO22) bzw. 80 CP (PO20)

Modulbeauftragte/r und hauptamtlich Lehrende
Modulbeauftragte/r: Studiendekan IT-Sicherheit
Lehrende: Lehrende im Studiengang IT-Sicherheit

Verwendung des Moduls
M.Sc. IT-Sicherheit / Informationstechnik

M.Sc. IT-Sicherheit / Netze und Systeme

Vorkenntnisse
Abhängig von der Themenwahl

Lernziele (learning outcomes)
Nach erfolgreichem Abschluss des Moduls:

- können Studierende selbstständig und fristgerecht ein wissenschaftliches Thema bearbeiten von der Recherche bis zur Dokumentation der Resultate
- können Studierende geeignete wissenschaftliche Verfahren und Methoden, die sie im Studium kennengelernt haben, auswählen, anwenden und weiterentwickeln, um ein konkretes Problem zu lösen
- können Studierende ihre Ergebnisse kritisch mit dem Stand der Forschung vergleichen und evaluieren
- können Studierende ihre eigenen Ergebnisse angemessen in Wort und Schrift darstellen.

Inhalt
Die Masterarbeit stellt eine forschungsorientierte, sechsmonatige Arbeit zu einem bestimmten Thema aus dem Bereich der IT-Sicherheit dar und wird im letzten Semester des Studiums geschrieben. Diese hat ein Umfang von 30 Leistungspunkten. Die Masterarbeit wird auf Englisch oder Deutsch verfasst.

Lehrformen
Abschlussarbeit

Prüfungsformen
Masterarbeit und Kolloquiumsvortrag

Voraussetzungen für die Vergabe von Credits
Sowohl die Masterarbeit als auch der Kolloquiumsvortrag müssen bestanden sein.

Der Anteil der Kolloquiumsnote an der Gesamtnote beträgt 10%

Stellenwert der Note für die Endnote (bei einem Gesamtstudienumfang von 120 ECTS)
30/91: M.Sc. IT-Sicherheit/ Informationstechnik [PO 22]

30/84: M.Sc. IT-Sicherheit/ Informationstechnik [PO 20]

30/99: M.Sc. IT-Sicherheit/ Netze und Systeme [PO 22]

30/96: M.Sc. IT-Sicherheit/ Netze und Systeme [PO 20]