

Modulhandbuch

des weiterbildenden Masterstudiengangs

„Applied IT Security“ (Master of Science, M.Sc.)

isits AG
International School of IT Security

Ruhr-Universität Bochum
Fakultät für Informatik

Inhaltsverzeichnis

1	Einleitung	1
2	Exemplarischer Studienverlaufsplan.....	2
3	Module des Pflichtbereichs	3
	Modul 1: Einführung in die Kryptographie.....	3
	Modul 2: Diskrete Mathematik für IT-Sicherheit.....	5
	Modul 3: Informatik für IT-Sicherheit.....	6
	Modul 4: Informationstechnik für IT-Sicherheit	7
	Modul 5: Netzsicherheit	8
	Modul 6: Sicherheitssysteme und -protokolle	10
	Modul 7: Kryptographie.....	11
	Modul 8: Sicherheitsmanagement	12
	Modul 10: Rechtliche Aspekte der IT-Sicherheit.....	13
	Modul 11: Masterarbeit	14
4	Module des Wahlpflichtbereichs	15
	Modul 9.1: Aktuelle Themen der IT-Sicherheit	15
	Modul 9.2: Datenschutz in der betrieblichen Praxis.....	16
	Modul 9.3: Einführung in die Forensische Informatik.....	18
	Modul 9.4: Group-Oriented Communication and Application Security	19
	Modul 9.5: Implementierung kryptographischer Verfahren	20
	Modul 9.6: Information Security Management in der Praxis	21
	Modul 9.7: Einführung in BSI-Grundschutz und ISO 27001	23
	Modul 9.8: Mobile Security	24
	Modul 9.9: Virenschutz im Unternehmen.....	25
	Modul 9.10: Systemsicherheit.....	26
	Modul 9.11: Programmanalyse.....	27
	Modul 9.12: Menschliches Verhalten in der IT-Sicherheit	28
	Modul 9.13: Human Aspects of Cryptography Adoption and Use	30

1 Einleitung

Das Modulhandbuch beschreibt die Module des weiterbildenden Fernstudiengangs „Applied IT Security“. Neben den Lernzielen werden die zum erfolgreichen Abschluss eines Moduls erforderlichen Leistungen spezifiziert. Die Form der Prüfungsleistungen regelt § 6 der Prüfungsordnung des weiterbildenden Masterstudiengangs „Applied IT Security“. Umfang und Dauer der Prüfungen orientieren sich an den zu vergebenden Credit Points.

Glossar:

Bonuspunkte: Bonuspunkte werden für semesterbegleitende Zusatzleistungen (Einsendeaufgaben) vergeben; der erfolgreiche Abschluss eines Moduls mit voller Punktzahl ist ohne Bonuspunkte möglich.

Einsendeaufgaben: Schriftliche Übungsaufgaben zur semesterbegleitenden Kontrolle des Lernerfolgs; die Bearbeitung der Einsendeaufgaben ist freiwillig, durch erfolgreich bearbeitete Einsendeaufgaben können Bonuspunkte erworben werden.

Fallstudien: Besondere Form der Einsendeaufgabe im Modul 9, z.B. im Modul „Einführung in BSI-Grundschutz und ISO 27001“.

Kontaktzeit: Der Masterstudiengang „Applied IT Security“ wird in Fernlehre angeboten. Aufgrund dieser Studienform sind Präsenz- und somit Kontaktzeiten in der Regel nicht vorgesehen. Betreuung und Lehre erfolgen nicht face-to-face wie in klassischen Studiengängen, sondern online und gehen nicht in die Berechnung der Kontaktzeiten ein.

Klausur: Form der Modulabschlussprüfung. In der Regel im Umfang von 3 Stunden für ein 10 CP Modul und 2 Stunden für ein 5 CP Modul. Klausuren finden in der Regel in Präsenz statt.

Masterarbeit: Form der Modulabschlussprüfung. Wissenschaftliche Abschlussarbeit zu einem bestimmten Thema aus dem Bereich der IT-Sicherheit. Die Bearbeitungsdauer beträgt 6 oder 12 Monate. Die Masterarbeit hat ein Umfang von 25 CP.

Mündliche Prüfung: Form der Modulabschlussprüfung. In der Regel im Umfang von 20-30 Minuten. Die mündliche Prüfung kann als online per Video oder persönlich erfolgen. Das Prüfungsergebnis ist zu protokollieren.

Pflichtmodule: Im Umfang von 70 CP obligatorisch zu belegende Module. Die Module 2, 3 und 4 werden je nach Vorkenntnissen zugewiesen.

Projektarbeit: Selbständige Bearbeitung eines gestellten Themas im Rahmen eines Wahlpflichtmoduls. Die Benotung geht in die Modulabschlussnote ein.

Reading Assignments: Lektüreaufgaben für das Selbststudium zu aktuellen Themen in einem Wahlpflichtmodul; Reading Assignments sind Gegenstand der Modulabschlussprüfung.

Schriftliche Hausarbeit: Form der Modulabschlussprüfung, ggf. mit Abschlusspräsentation. Umfang: ca. 20 Seiten.

Wahlpflichtmodule: Im Umfang von 25 CP zu wählende Module aus dem Angebot des Wahlpflichtbereichs (Modul 9).

2 Exemplarischer Studienverlaufsplan

EXEMPLARISCHER STUDIENVERLAUF (6 Semester Variante)

Semester	Modul												IST-CP
	1 (10 CP)	2 (10 CP)	3 (10 CP)	4 (10 CP)	5 (10 CP)	6 (10 CP)	7 (10 CP)	8 (5 CP)	9 (25 CP)	10 (5 CP)	Thesis (25 CP)		
1.	Einführung Kryptographie 10 CP	Diskrete Mathematik* 10 CP											20
2.			Informatik* 10 CP	Informationstechnik* 10 CP			Kryptographie 10 CP						20
3.					Netz- sicherheit 10 CP			Sicherheits- management 5 CP	WPF** I 5 CP				20
4.						Sicherheits- systeme und -protokolle 10 CP			WPF II 5 CP	Rechtliche Aspekte 5 CP			20
5.									WPF III 5 CP		Thesis 25 CP (verteilt auf 2 Semester)		15
6.									WPF IV 5 CP			5 CP	25
									WPF V 5 CP			20 CP	25
Gesamt													120

* Von diesen 3 Modulen sind zwei je nach Vorstudium zu studieren.

** WPF: Wahlpflichtmodul

EXEMPLARISCHER STUDIENVERLAUF (8 Semester Variante)

Semester	Modul												IST-CP
	1 (10 CP)	2 (10 CP)	3 (10 CP)	4 (10 CP)	5 (10 CP)	6 (10 CP)	7 (10 CP)	8 (5 CP)	9 (25 CP)	10 (5 CP)	Thesis (25 CP)		
1.	Einführung Kryptographie 10 CP	Diskrete Mathematik* 10 CP											20
2.			Informatik* 10 CP	Informationstechnik* 10 CP				Sicherheits- management 5 CP					15
3.							Kryptographie 10 CP		WPF** I 5 CP				15
4.					Netz- sicherheit 10 CP				WPF II 5 CP				15
5.						Sicherheits- systeme und -protokolle 10 CP			WPF III 5 CP				15
6.									WPF IV 5 CP	Rechtliche Aspekte 5 CP			10
7.									WPF V 5 CP		Thesis 25 CP (verteilt auf 2 Semester)		10
8.											5 CP		20
Gesamt													120

* Von diesen 3 Modulen sind zwei je nach Vorstudium zu studieren.

** WPF: Wahlpflichtmodul

3 Module des Pflichtbereichs

Pflichtmodul:				
Modul 1: Einführung in die Kryptographie				
Workload	Studienphase	Turnus	Dauer	
10 CP (300 h)	1. Studienjahr	Semesterweise	1 Semester	
Lehrveranstaltungen		Kontaktzeit	Selbststudium	Gruppengröße
Einführung in die Kryptographie		0 h	300 h	Max. 50
Teilnahmevoraussetzungen				
keine				
Lernergebnisse				
<p>Nach erfolgreichem Abschluss des Moduls verfügen die Studierenden über Kenntnisse der grundlegenden Anwendungen symmetrischer, 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.</p> <p>Zum anderen erreichen die Studierenden durch Beschreibungen ausgewählter praxisrelevanter Algorithmen wie z. B. dem 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. Sie erwerben durch das konsequent zweisprachige eLearning-Angebot (Videos zu den Lerninhalten sind in Deutsch und Englisch verfügbar) Sprachkompetenzen in der Wissenschaftssprache Englisch.</p>				
Inhalte				
<p>Das Modul bietet einen allgemeinen Einstieg in die Funktionsweise moderner Kryptographie und Datensicherheit. Es werden grundlegende Begriffe und mathematisch/technische Verfahren der Kryptographie und der Datensicherheit erläutert. Praktisch relevante symmetrische und asymmetrische Verfahren und Algorithmen werden vorgestellt und an praxisrelevanten Beispielen erläutert.</p> <p>Die Vorlesung lässt sich in drei Teile gliedern: Die Funktionsweise der symmetrischen Kryptographie einschließlich der Beschreibung historisch bedeutender symmetrischer Verschlüsselungsverfahren (Caesar Chiffre, Affine Chiffre) und aktueller symmetrischer Verfahren (Data Encryption Standard, Advanced Encryption Standard, Stromchiffren, One Time Pad) werden im ersten Teil behandelt.</p> <p>Der zweite Teil beginnt mit einer Einleitung zu asymmetrischen Verfahren und deren wichtigsten Stellvertretern (RSA, Diffie-Hellman, elliptische Kurven). Hierzu wird eine Einführung der Grundlagen der Zahlentheorie durchgeführt, 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 Einführung der asymmetrischen Verfahren, die sowohl Verschlüsselungsalgorithmen als auch digitale Signaturen beinhalten. Abgeschlossen wird dieser Teil durch Hashfunktionen, die eine große Rolle für digitalen Signaturen und Message Authentication Codes (MACs oder kryptographische Checksummen) spielen.</p> <p>Im dritten 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.</p>				

Besondere Lehrformen
Vorlesung in Fernlehre (eLearning): Interaktive Lernplattform, Fachbuch mit Übungsaufgaben, Videoinhalte in Deutsch und Englisch verfügbar. Vorlesungsbegleitend werden freiwillige Einsendeaufgaben angeboten. Das Feedback erfolgt über einen Tutor, der mit den Studierenden über ein Forum und über E-Mail kommuniziert.
Prüfungsformen
Klausur (3 Stunden)
Voraussetzungen für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussklausur.
Verwendung des Moduls in anderen Studiengängen
Nein
Stellenwert der Note für die Endnote
10/120
Modulbetreuer
Prof. Dr. Christof Paar
Literatur
Paar, Christof/ Pelzl, Jan/ Güneysu, Tim: Understanding Cryptography – from Established Symmetric and Asymmetric Ciphers to Post-Quantum Algorithms, 2. Auflage, Springer, 2024
Sonstige Informationen

Pflichtmodul: Modul 2: Diskrete Mathematik für IT-Sicherheit			
Workload 10 CP (300 h)	Studienphase 1. Studienjahr	Turnus Semesterweise	Dauer 1 Semester
Lehrveranstaltungen Diskrete Mathematik für IT-Sicherheit	Kontaktzeit 0 h	Selbststudium 300 h	Gruppengröße Max. 50
Teilnahmevoraussetzungen keine			
Lernergebnisse Nach dem erfolgreichen Abschluss des Moduls haben die Studierenden den professionellen Umgang mit abstrakten, diskreten Strukturen erlernt. Sie kennen die zugrundeliegenden Begrifflichkeiten, Beweismethoden und Algorithmen aus der elementaren Zahlentheorie, der Kombinatorik und der Graphentheorie und können diese selbstständig anwenden. Sie können konkrete Strukturen mathematisch sauber modellieren und Eigenschaften der Modelle nachweisen.			
Inhalte Die Vorlesung „Diskrete Mathematik“ beschäftigt sich mit diskreten Strukturen. Sie gliedert sich in 5 Teile. Teil 1: Algebraische Grundlagen. Es werden Eigenschaften der ganzen, der rationalen und der reellen Zahlen axiomatisch beschrieben und abstraktes Argumentieren vermittelt. Teil 2: Zahl-Darstellungen. Es werden verschiedene Darstellungen von Zahlen diskutiert und durch Polynomarithmetik beschrieben. Teil 3: Ganzzahlige Arithmetik. Es werden Grundkenntnisse der elementaren Zahlentheorie vermittelt, zahlentheoretische Algorithmen vorgestellt und schließt mit kryptographischen Anwendungen. Teil 4: Abzählende Kombinatorik. Es werden die binomischen Lehrsätze besprochen sowie induktiv beschriebene kombinatorische Strukturen vorgestellt. Teil 5: Graphentheorie. Mit Hilfe von Graphen werden verschiedenste Anwendungsprobleme modelliert. Es werden abstrakte Eigenschaften von Graphen untersucht sowie Algorithmen zu deren Untersuchung vorgestellt.			
Besondere Lehrformen Vorlesung in Fernlehre (eLearning): Interaktive Lernplattform, Skript und Übungsaufgaben im Selbststudium. Feedback erfolgt über einen Tutor, der mit den Studierenden über ein Forum und per E-Mail kommuniziert.			
Prüfungsformen Klausur (3 Stunden)			
Voraussetzungen für die Vergabe von Kreditpunkten Bestehen der Modulabschlussklausur.			
Verwendung des Moduls in anderen Studiengängen nein			
Stellenwert der Note für die Endnote 10/120			
Modulbetreuer Prof. Dr. Christian Stump, Ruhr-Universität Bochum			
Literatur Skript „Diskrete Mathematik für IT-Sicherheit“			
Sonstige Informationen			

Pflichtmodul: Modul 3: Informatik für IT-Sicherheit				
Workload 10 CP (300 h)	Studienphase 1. Studienjahr	Turnus Jährlich zum Sommersemester	Dauer 1 Semester	
Lehrveranstaltungen Informatik für IT-Sicherheit		Kontaktzeit 0 h	Selbststudium 300 h	Gruppengröße Max. 50
Teilnahmevoraussetzungen keine				
Lernergebnisse Nach erfolgreicher Absolvierung des Moduls haben die Studierenden Kenntnisse über die systematische Darstellung, Speicherung und Verarbeitung von Informationen erworben. Sie sind in der Lage, professionell kleine Programme zu entwickeln, in UML zu beschreiben und in einer Hochsprache zu implementieren, zu generieren und auszuführen. Sie sind in der Lage, über diese Programme die Dienste des Betriebssystems zu nutzen und größere Datenbestände über eine professionell entworfene Datenbank zu verwalten. Dabei finden Aspekte der IT-Sicherheit Berücksichtigung. Die Studierenden bekommen die notwendige Methodenkompetenz, Sicherheitsprobleme mithilfe der Informatik strukturiert und unter Berücksichtigung von IT-Sicherheit zu lösen. Für die Realisierung der Lösung erhalten diese das notwendige, praxisrelevante Rüstzeug. Sie sind in der Lage, im Gespräch grundlegende Aspekte der Informatik zu beschreiben und argumentativ auf neue Problemstellungen anzuwenden.				
Inhalte Das Modul vermittelt die Grundlagen der Informatik, die im Weiteren auch für die anderen Module im Bereich der IT-Sicherheit relevant sind. Dazu gehören neben den programmiertechnischen Grundlagen wie „Sprachen und Automaten“, „Datenstrukturen“, „Algorithmen“ und „Komplexitätstheorie“ auch die Grundzüge der Programmierung in einer imperativen und einer objektorientierten Programmiersprache wie C, C++ oder Java. Des Weiteren beschäftigt sich dieses Modul mit der Systemsoftware (Betriebssysteme), auf denen die Anwendungen ablaufen. Neben dem internen Aufbau (Task-, Memory-, IO-Management) liegt ein Schwerpunkt bei den Sicherheitsmechanismen moderner Betriebssysteme (Rechtemodelle, Zutrittskontrolle, Ausführungskontrolle, sicherer Bootprozess). Für viele Anwendungsbereiche der modernen IT-Landschaft ist der Einsatz von Datenbanken ebenfalls zentral. Das Modul behandelt daher auch die Konzipierung und Realisierung von Datenbanken auf Basis von SQL.				
Besondere Lehrformen Vorlesung in Fernlehre (eLearning): Interaktive Lernplattform, angeleitetes Selbststudium mit Übungsaufgaben. Das Feedback erfolgt durch den Lehrenden, der mit den Studierenden über ein Forum und über E-Mail kommuniziert.				
Prüfungsformen Klausur (3 Stunden)				
Voraussetzungen für die Vergabe von Kreditpunkten Bestehen der Modulabschlussklausur.				
Verwendung des Moduls in anderen Studiengängen nein				
Stellenwert der Note für die Endnote 10/120				
Modulbetreuer Prof. Dr. Jürgen Quade, Hochschule Niederrhein, Krefeld				
Literatur Skript „Informatik für IT-Sicherheit“				
Sonstige Informationen				

Pflichtmodul: Modul 4: Informationstechnik für IT-Sicherheit				
Workload	Studienphase	Turnus	Dauer	
10 CP (300 h)	1. Studienjahr	Semesterweise	1 Semester	
Lehrveranstaltungen		Kontaktzeit	Selbststudium	Gruppengröße
Informationstechnik für IT-Sicherheit		0 h	300 h	Max. 50
Teilnahmevoraussetzungen				
keine				
Lernergebnisse				
<p>Nach erfolgreicher Absolvierung des Moduls haben die Studierenden Grundkenntnisse über die Organisation und Funktionsweise von modernen Rechensystemen erworben. Sie verfügen über ein Verständnis der technischen Grundlagen von digitalen Schaltungen und dem Zusammenwirken der Komponenten moderner Rechner sowie der beim Entwurf zu lösenden Problemstellungen und können dieses Verständnis zur Lösung von Problemen einsetzen. Ferner entwickeln sie ein Grundverständnis für die Beziehung zwischen Softwarefunktionen und Hardware-Realisierung mit einem Fokus auf sicherheitskritische Aspekte moderner Beschleunigungstechniken. Sie können mit diesem Verständnis mit ihren Kollegen über Probleme der Computerhardware diskutieren und auftretende Probleme im Gespräch korrekt klassifizieren.</p>				
Inhalte				
<p>Das Modul behandelt im ersten Teil die Rechnerarchitektur, also den Aufbau und die Funktionsweise moderner Digitalrechner. Ausgehend von dem grundlegenden Aufbau gemäß dem von Neumann-Prinzip wird das Zusammenwirken der Komponenten eines Rechners und der Informationsaustausch über Bussysteme – sowohl intern als auch mit externen Peripheriegeräten – behandelt. Anschließend wird die Befehlsverarbeitung innerhalb von Prozessoren vertieft inklusive der Betrachtung verschiedener Befehlssätze, Adressierungsarten und Beschleunigungstechniken. Insbesondere wird dabei das Pipelining-Prinzip erläutert sowie das große Problem der Pipeline-Konflikte mit deren Lösungsmöglichkeiten behandelt. Weitergehend wird der Aufbau einer typischen Speicherhierarchie mit Hauptspeicher, Cachestufen und Hintergrundspeicher sowie die virtuelle Speicherverwaltung vorgestellt. Der erste Teil schließt mit einer Betrachtung von Parallelisierungstechniken, weit verbreiteten Rechnerarchitekturen und den Sicherheitsaspekten von typischen Beschleunigungstechniken.</p> <p>Im zweiten Teil stehen der Aufbau und Entwurf der zuvor kennengelernten Komponenten mittels digitaler Schaltungen im Fokus. Auf der Basis von Boole'scher Algebra und Boole'schen Funktionen werden Schaltnetze und speicherbehaftete Schaltwerke sowie Register und Speicherbausteine auf Gatterebene betrachtet, d.h. abstrahierend von der physikalischen bzw. elektrotechnischen Realisierung der Bauelemente. Zusätzlich wird ein Überblick über den Entwurfsablauf für moderne Schaltungstechnologien (Standardzellen, full custom, FPGA) gegeben.</p>				
Besondere Lehrformen				
Vorlesung in Fernlehre (eLearning): Interaktive Lernplattform, Skript, online Übungsbetrieb mit freiwilligen Einsendeaufgaben. Die Betreuung erfolgt über den Dozenten, der mit den Studierenden über ein Forum und über E-Mail kommuniziert.				
Prüfungsformen				
Klausur (3 Stunden)				
Voraussetzungen für die Vergabe von Kreditpunkten				
Bestehen der Modulabschlussklausur.				
Verwendung des Moduls in anderen Studiengängen				
nein				
Stellenwert der Note für die Endnote				
10/120				
Modulbetreuer				
Ehem. Vertr.-Prof. Dr. Philipp Niemann, Ruhr-Universität Bochum				
Literatur				
Skript „Informationstechnik für IT-Sicherheit“				
Sonstige Informationen				

Pflichtmodul: Modul 5: Netzsicherheit				
Workload	Studienphase	Turnus	Dauer	
10 CP (300 h)	2. Studienjahr	Semesterweise	1 Semester	
Lehrveranstaltungen		Kontaktzeit	Selbststudium	Gruppengröße
Netzsicherheit		0 h	300 h	Max. 50
Teilnahmevoraussetzungen				
keine				
Lernergebnisse				
<p>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.</p>				
Inhalte				
<p>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).</p> <p>Das Modul „Netzsicherheit“ beschäftigt sich mit konkreten Netzen zur Datenübertragung und beleuchtet diese von allen Seiten auf ihre Sicherheit hin. Es umfasst folgende Teile:</p> <ul style="list-style-type: none"> • Einführung „Kryptographie und das Internet“ • 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) • 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 • Dateiverschlüsselung mit OpenPGP (Datenformat, Efail, Klima-Rosa) • E-Mail-Verschlüsselung mit S/MIME (SMTP, Datenformat, Efail, POP3, IMAP) • das Domain Name System und DNSSEC (faktorisierebare Schlüssel) • Sicherheit von Webanwendungen (HTML, URI, XSS, CSRF, SQLi, SSO) • XML- und JSON-Sicherheit <p>Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studierenden stellen selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit an.</p>				

Besondere Lehrformen
Vorlesung in Fernlehre (eLearning): Interaktive Lernplattform, Buch und Folienausdrucke, freiwillige Einsendeaufgaben mit Feedback durch einen Tutor, der mit den Studierenden über ein Forum und über E-Mail kommuniziert.
Prüfungsformen
Klausur (3 Stunden)
Voraussetzungen für die Vergabe von Kreditpunkten
Bestehen der Modulabschlussklausur.
Verwendung des Moduls in anderen Studiengängen
nein
Stellenwert der Note für die Endnote
10/120
Modulbetreuer
Prof. Dr. Jörg Schwenk
Literatur
Schwenk, Jörg: Sicherheit und Kryptographie im Internet, Vieweg, 2020 Skript (ergänzende Folien) „Netzicherheit“
Sonstige Informationen

Pflichtmodul: Modul 6: Sicherheitssysteme und -protokolle				
Workload	Studienphase	Turnus	Dauer	
10 CP (300 h)	2. Studienjahr	Semesterweise	1 Semester	
Lehrveranstaltungen		Kontaktzeit	Selbststudium	Gruppengröße
Sicherheitssysteme und -protokolle		0 h	300 h	Max. 50
Teilnahmevoraussetzungen				
keine				
Lernergebnisse				
<p>Im Rahmen dieses Moduls erlernen die Studierenden die wichtigsten Methoden und Werkzeuge moderner Sicherheitsbegriffe und -protokolle, welche zur professionellen Konzeption und Entwicklung sicherer IT-Systeme in der Praxis benötigt werden. Die Studierenden sind nach Abschluss des Moduls in der Lage, Sicherheitsaspekte gegebener Protokolle zu analysieren, Schwachstellen im Design aufzudecken sowie selbständig neue Protokolle zu entwickeln.</p> <p>Insbesondere erwerben die Studierenden die Fähigkeit zum Modellieren konkreter Fragestellungen und Anforderungsanalysen aus vorhandenen Systeminformationen bzw. Systemgegebenheiten. Hierzu gehört neben einer Einführung in die verschiedenen Konzepte und Begriffe auch die Vertiefung ausgewählter Bereiche der Kryptographie und Sicherheitstechnologie. Die Studierenden können diese Fähigkeiten in ihrer Firma einsetzen, um argumentativ bessere Sicherheitslösungen durchzusetzen.</p>				
Inhalte				
<p>Nach der Vermittlung grundlegender Sicherheitsdefinitionen, Sicherheitsziele und Vertrauensmodelle werden die wesentlichen Protokollprimitive und Protokolle (Commitments, Zero-Knowledge, Proof of Knowledge, Secret Sharing) detailliert behandelt. Darüber hinaus werden auch andere Aspekte aus dem Bereich der Systemsicherheit betrachtet. Ein Schwerpunkt der Veranstaltung liegt auf Authentifizierungs- und Schlüsselaustauschprotokollen und deren bekannte Schwachstellen und daraus resultierenden Problemen. Des Weiteren werden Aspekte betrachtet, die für Systemsicherheit, konkret für die Sicherheit von Rechnerplattformen, von Bedeutung sind wie beispielsweise Sicherheitsprotokolle.</p>				
Besondere Lehrformen				
<p>Vorlesung in Fernlehre (eLearning): Interaktive Lernplattform, Skript, online Übungsbetrieb mit Einsendeaufgaben. Die Betreuung erfolgt über einen Tutor, der mit den Studierenden über ein Forum und über E-Mail kommuniziert.</p>				
Prüfungsformen				
Klausur (3 Stunden)				
Voraussetzungen für die Vergabe von Kreditpunkten				
Bestehen der Modulabschlussklausur.				
Verwendung des Moduls in anderen Studiengängen				
nein				
Stellenwert der Note für die Endnote				
10/120				
Modulbetreuer				
Prof. Dr. Thorsten Holz				
Literatur				
Skript „Sicherheitssysteme und -protokolle“				
Sonstige Informationen				

Pflichtmodul: Modul 7: Kryptographie				
Workload	Studienphase	Turnus	Dauer	
10 CP (300 h)	1. Studienjahr	Semesterweise	1 Semester	
Lehrveranstaltungen		Kontaktzeit	Selbststudium	Gruppengröße
Kryptographie		0 h	300 h	Max. 50
Teilnahmevoraussetzungen				
Empfehlenswerte Voraussetzungen:				
Modul 1: Einführung in die Kryptographie, Modul 2: Diskrete Mathematik				
Lernergebnisse				
<p>Studierende haben nach erfolgreicher Absolvierung dieses Moduls ein tiefes Verständnis der wesentlichen mathematischen Methoden und Verfahren, auf denen moderne kryptographische Verfahren beruhen, entwickelt. Nach Abschluss des Moduls verfügen die Studierenden über die Fähigkeit zu Analyse und Design aktueller und zukünftiger kryptographischer Methoden auf dem hohen Abstraktionsgrad, der in der Forschung zur modernen Kryptographie eingesetzt wird. Die Studierenden entwickeln ein Bewusstsein für Methodik und Mächtigkeit verschiedenster Angriffsszenarien. Sie sind in der Lage, neue Sicherheitsmodelle selbst zu erstellen und diese argumentativ zu verteidigen.</p>				
Inhalte				
<p>Die Vorlesung „Kryptographie“ behandelt die grundlegenden mathematischen Prinzipien moderner kryptographischer Verfahren. Die notwendigen mathematischen Grundkenntnisse der Algebra, Zahlentheorie, Komplexitätstheorie, Kombinatorik und Wahrscheinlichkeitsrechnung werden im Laufe der Vorlesung vertieft und ergänzt. Die Veranstaltung gliedert sich in drei Teile:</p> <p>In Teil 1 der Veranstaltung werden wesentliche Bereiche der symmetrischen Kryptographie behandelt. Dieser Teil beinhaltet insbesondere Block- und Strom-Algorithmen sowie Hash-funktionen. Bei der Darstellung wird stets auf den mathematischen Hintergrund bzw. die präzise mathematische Formulierung eingegangen. Im Unterschied zu Modul 1 werden hier auch Angriffe (differentielle und lineare Kryptoanalyse) auf die Algorithmen vorgesehlt, um das Verständnis zu vertiefen.</p> <p>Teil 2 befasst sich mit den wichtigsten asymmetrischen Verfahren. Ein wesentlicher Teil befasst sich mit dem RSA Algorithmus und den sich anschließenden mathematischen Fragestellungen wie Faktorisierung großer Zahlen, die in Modul 1 nicht behandelt wurden, aber zum vertieften Verständnis notwendig sind. Weitere Gebiete sind Verfahren, die auf diskreten Logarithmen basieren sowie die Analyse gängiger Algorithmen für die digitale Signatur.</p> <p>Im abschließenden Teil 3 werden Generische Gruppen und Pairing-Based Cryptography vorgestellt. Hier stehen in Ergänzung zu Modul 4 die mathematischen Grundlagen im Vordergrund.</p>				
Besondere Lehrformen				
Vorlesung in Fernlehre (eLearning): Interaktive Lernplattform, Skript mit Übungsaufgaben, online Übungsbetrieb. Die Betreuung erfolgt über einen Tutor, der mit den Studierenden über ein Forum und über E-Mail kommuniziert.				
Prüfungsformen				
Klausur (3 Stunden)				
Voraussetzungen für die Vergabe von Kreditpunkten				
Bestehen der Modulabschlussklausur.				
Verwendung des Moduls in anderen Studiengängen				
nein				
Stellenwert der Note für die Endnote				
10/120				
Modulbetreuer				
Prof. Dr. Gregor Leander				
Literatur				
Skript „Kryptographie“				
Sonstige Informationen				

Pflichtmodul: Modul 8: Sicherheitsmanagement				
Workload	Studienphase	Turnus	Dauer	
5 CP (150 h)	2. Studienjahr	Semesterweise	1 Semester	
Lehrveranstaltungen		Kontaktzeit	Selbststudium	Gruppengröße
Sicherheitsmanagement		0 h	150 h	Max. 50
Teilnahmevoraussetzungen				
keine				
Lernergebnisse				
<p>Nach Abschluss des Moduls haben die Studierenden Kenntnisse, wie durch das Ergreifen von geeigneten infrastrukturellen, organisatorischen, personellen und technischen Standardsicherheitsmaßnahmen ein Sicherheitsniveau für die verwendeten IT-Systeme zu erreichen ist, das dem angestrebten und wirtschaftlich vertretbaren Schutzbedarf angemessen und ausreichend ist.</p> <p>Die Studierenden haben Kompetenzen erworben, um die Unternehmensführung durch die Erstellung eines Sicherheitskonzeptes bei den entsprechenden Entscheidungen zu unterstützen. Sie haben gelernt, wie man Kompetenzen und Verantwortlichkeiten für das Sicherheitsmanagement definiert und ein Sicherheitsbewusstsein innerhalb von Unternehmen schafft sowie die Umsetzung der Sicherheitsmaßnahmen im laufenden IT-Betrieb erreicht. Sie können ihre Sicherheitskonzepte sicher gegen Einwände von Kollegen und Vorgesetzten verteidigen, und können dabei auch auf organisatorische und wirtschaftliche Argumente eingehen.</p>				
Inhalte				
<p>Ein Schwerpunkt dieses Informationsmanagements, das sich als Führungsaufgabe versteht (deshalb „Management“), bildet das IT-Sicherheitsmanagement, das sich ebenso als Führungs- bzw. Managementaufgabe mit den sicherheitsrelevanten Aspekten der betrieblichen Informations- und Kommunikationssysteme (IuK-Systeme) auseinandersetzt.</p> <p>Das IT-Sicherheitsmanagement subsummiert die Planung, Entscheidung, Organisation, Steuerung und Kontrolle der Aufgaben und Prozesse, die IT-Sicherheit gewährleisten sollen. Zu den Aufgaben des IT-Sicherheitsmanagements zählt in vielen Unternehmen, die strategischen IT-Sicherheitsziele zu erreichen sowie Voraussetzungen zum Management von IT-Risiko zu schaffen, so dass reale Risiken minimiert werden können.</p>				
Besondere Lehrformen				
Vorlesung in Fernlehre (eLearning): Interaktive Lernplattform, Skript mit Übungsaufgaben; online Übungsbetrieb. Die Betreuung erfolgt über einen Tutor, der mit den Studierenden über ein Forum und über E-Mail kommuniziert.				
Prüfungsformen				
Klausur (2 Stunden)				
Voraussetzungen für die Vergabe von Kreditpunkten				
Bestehen der Modulabschlussklausur.				
Verwendung des Moduls in anderen Studiengängen				
nein				
Stellenwert der Note für die Endnote				
5/120				
Modulbetreuer				
N.N.				
Literatur				
Skript „Sicherheitsmanagement“				
Sonstige Informationen				

Pflichtmodul: Modul 10: Rechtliche Aspekte der IT-Sicherheit			
Workload	Studienphase	Turnus	Dauer
5 CP (150 h)	2. Studienjahr	Semesterweise	1 Semester
Lehrveranstaltungen		Kontaktzeit	Selbststudium
Rechtliche Aspekte der IT-Sicherheit		0 h	150 h
Teilnahmevoraussetzungen			
keine			
Lernergebnisse			
<p>Die Studierenden verfügen nach Abschluss dieses Moduls über Kenntnisse in den Grundlagen der Rechtsgebiete, die für den betrieblichen Arbeitsalltag im Bereich der IT-Sicherheit relevant sind. Sie beherrschen die juristische Arbeitsweise in Grundzügen.</p> <p>Die Studierenden sind danach in der Lage, die Rechtsfragen, die im Bereich der IT-Sicherheit üblicherweise auftauchen, wie beispielsweise das Scannen von E-Mails nach Spam und Viren, Generierung und Analyse von Logfiles, etc., zu bewerten und diese entsprechend den gesetzlichen Grundlagen zu handhaben. Die Studierenden können den Einfluss von regulatorischen und gesetzlichen Vorgaben auf die IT-Sicherheit bewerten und dies in die Erstellung eigener Sicherheitskonzepte einfließen lassen. Sie können argumentieren, warum ein technisches Verfahren rechtlichen Vorgaben entspricht.</p>			
Inhalte			
<p>In einem ersten Teil beschäftigt sich dieses Modul zunächst mit den Grundlagen des Vertragsrechts, Markenrechts sowie dem Urheberrecht; darüber hinaus werden Datenschutzrecht, die wesentlichen Teile des Telekommunikationsrechts, die Telekommunikationsüberwachungsverordnung, das Teledienste-Gesetz, das Domainrecht sowie weitere relevante Gebiete behandelt.</p> <p>Nach dieser Einführung werden in einem zweiten Teil aktuelle Rechtsthemen der IT-Sicherheit aufgegriffen und wird über die aktuelle Rechtsentwicklung informiert. Anhand von praxisnahen Szenarien wird den Studierenden das Handwerkszeug für die Bewältigung vieler alltäglicher Rechtsfragen im Bereich der IT-Sicherheit vermittelt.</p>			
Besondere Lehrformen			
Vorlesung in Fernlehre (eLearning): Interaktive Lernplattform, Skript mit Übungsaufgaben, online Übungsbetrieb. Die Betreuung erfolgt über einen Tutor, der mit den Studierenden über ein Forum und über E-Mail kommuniziert.			
Prüfungsformen			
Klausur (2 Stunden)			
Voraussetzungen für die Vergabe von Kreditpunkten			
Bestehen der Modulabschlussklausur.			
Verwendung des Moduls in anderen Studiengängen			
nein			
Stellenwert der Note für die Endnote			
5/120			
Modulbetreuer			
Prof. Dr. Tobias Gostomzyk, TU Dortmund			
Literatur			
Skript „Rechtliche Aspekte der IT-Sicherheit“			
Sonstige Informationen			

Pflichtmodul				
Modul 11: Masterarbeit				
Workload	Studienphase	Turnus	Dauer	
25 CP (750 h)	3. Studienjahr	Semesterunabhängig	1 oder 2 Semester	
Lehrveranstaltungen		Kontaktzeit	Selbststudium	Gruppengröße
n.a.		0 h	750 h	n.a.
Teilnahmevoraussetzungen				
Erfolgreiche Absolvierung von Pflicht- und Wahlpflichtmodulen im Umfang von wenigstens 80 CP.				
Lernergebnisse				
Die Studierenden dokumentieren, dass sie ein komplexes Problem der angewandten IT-Sicherheit selbstständig mit wissenschaftlichen Methoden und einer zeitlichen Begrenzung unter Betreuung bearbeiten und lösen können.				
Die Studierenden zeigen, dass sie mit Arbeitsmethoden der wissenschaftlichen Forschung und der Projektorganisation vertraut sind und ihre im Studium erworbenen Kenntnisse und Arbeitsergebnisse verständlich schriftlich präsentieren können.				
Inhalte				
Studierende wählen aus dem Portfolio des Studiengangs ein Thema aus dem Bereich der IT-Sicherheit. Im Rahmen der Masterarbeit bearbeiten sie eine anspruchsvolle Fragestellung. Für das zu bearbeitende Thema haben die Studierenden ein Vorschlagsrecht.				
Studierende haben auch die Möglichkeit die Masterarbeit im Rahmen eines Industrieprojekts durchzuführen.				
Besondere Lehrformen				
Eigenständig unter Betreuung				
Prüfungsformen				
Schriftliche Prüfungsarbeit				
Voraussetzungen für die Vergabe von Kreditpunkten				
Bestehen der schriftlichen Masterarbeit.				
Verwendung des Moduls in anderen Studiengängen				
nein				
Stellenwert der Note für die Endnote				
25/120				
Modulbetreuer				
Prof. Dr. Jörg Schwenk				
Literatur				
Sonstige Informationen				

4 Module des Wahlpflichtbereichs

Wahlpflichtmodul: Modul 9.1: Aktuelle Themen der IT-Sicherheit				
Workload	Studienphase	Turnus	Dauer	
5 CP (150 h)	3. Studienjahr	Jährlich zum Wintersemester	1 Semester	
Lehrveranstaltungen		Kontaktzeit	Selbststudium	Gruppengröße
Aktuelle Themen der IT-Sicherheit		8 h	142 h	Mind. 3, Max. 15
Teilnahmevoraussetzungen				
Empfehlenswert: Vorkenntnisse aus den Modulen 5 „Netzsicherheit“ und 6 „Sicherheitssysteme und -protokolle“				
Lernergebnisse				
Die Studierenden lernen in diesem Seminar, eigenständig Fachliteratur zu einem bestimmten Themengebiet zu verstehen und bekommen einen Einblick in aktuelle Forschungsthemen. Durch die Ausarbeitung besteht die Möglichkeit, das Schreiben eigener Texte und die Zusammenfassung komplexer Themengebiete zu üben. Darüber hinaus liefert der Vortrag die Möglichkeit, die Präsentation von wissenschaftlichen Ergebnissen zu erlernen und den Stoff zu vertiefen.				
Inhalte				
Das Seminar gibt ein Überblick über aktuelle Forschungsergebnisse im Bereich System-sicherheit. Der Fokus liegt auf den Bereichen Malware-Analyse, Botnetze, Sicherheit von Smartphones, Netzwerksicherheit und ähnlicher Themen aus dem Bereich der systemnahen IT-Sicherheit.				
Besondere Lehrformen				
Das Seminar wird als Blockveranstaltung gegen Ende des Semesters – nach besonderer Ankündigung – durchgeführt. Die Betreuung erfolgt über einen Tutor, der mit den Studierenden über ein Forum und über E-Mail kommuniziert.				
Prüfungsformen				
Mündlicher Vortrag (40%) und schriftliche Ausarbeitung (Umfang ca. 20 Seiten) (60%)				
Voraussetzungen für die Vergabe von Kreditpunkten				
Bestehen der Modulprüfung (bestandener Vortrag und bestandene Ausarbeitung).				
Verwendung des Moduls in anderen Studiengängen				
nein				
Stellenwert der Note für die Endnote				
5/120				
Modulbetreuer				
Prof. Dr. Thorsten Holz				
Literatur				
Aktuelle Lektüreempfehlungen				
Sonstige Informationen				

Wahlpflichtmodul:**Modul 9.2: Datenschutz in der betrieblichen Praxis**

Workload	Studienphase	Turnus	Dauer	
5 CP (150 h)	2.-3. Studienjahr	Jährlich zum Sommersemester	1 Semester	
Lehrveranstaltungen		Kontaktzeit	Selbststudium	Gruppengröße
Datenschutz in der betrieblichen Praxis		0 h	150 h	Mind. 3, Max. 50

Teilnahmevoraussetzungen

Empfehlenswert: Grundwissen IT-Sicherheitsanalysen, IT- und Datenschutzrecht

Lernergebnisse

Nach Abschluss des Moduls haben die Studierenden Kenntnisse entwickelt, die sie als Ansprechpartner von Datenschutzbeauftragten darin befähigen, für Kontrollen und Einführungsprojekte nötige Informationen und Dokumentationen bereitzustellen. Sie sind durch die Vermittlung der Basisinformationen im Rahmen des Moduls ebenfalls grundlegend auf die Übernahme der Funktion eines Datenschutzbeauftragten vorbereitet. Sie sind in der Lage, ein Datenschutzkonzept zu erstellen, das auch den Bedürfnissen der Datenverarbeitung ihrer Firma gerecht wird, und dieses argumentativ zu verteidigen.

Inhalte

Datenschutz bildet einen der rechtlichen Kontexte, die bei der Einführung und Entwicklung von IT-Produkten zu beachten sind. Unter dem Stichwort Compliance tauchen solche Fragestellungen des Erfüllens von Anforderungen aus gesetzlichen Vorgaben in Unternehmen an verschiedenen Stellen auf.

IT-Sicherheit und Datenschutz sind eng miteinander verbunden und meist sind in der praktischen Umsetzung dieselben Akteure beteiligt. In diesem Lehrmodul stehen daher Fragestellungen einer solchen gekoppelten Betrachtung von Datenschutz- und IT-Sicherheitsfragen im Vordergrund. Dieses an der Praxis orientierte Wissen ist für (potentielle) Datenschutzbeauftragte ebenso relevant, wie für Mitarbeiter in Unternehmen, die Systeme administrieren oder konfigurieren:

- Grundlegende Datenschutzerfordernisse: In der Übersicht werden die grundlegenden Datenschutzregelungen mit Bezug zu konkreten Fragestellungen thematisiert.
- Leseworkshop Gesetzgebung: Grundlegende Techniken und Fragestellungen zu Gesetzestexten bilden die Grundlage dafür die wechselnden Rechtsaspekte umsetzen zu können.
- Erstellen von Verfahrensverzeichnissen: Ein zentrales Dokument im Datenschutz ist das rechtlich geforderte Verzeichnis der Verarbeitungstätigkeiten, das nach formalem Schema zentrale Aspekte eines Softwaresystems/automatisierten Verfahrens aus Sicht des Datenschutzes dokumentiert.
- Weitere Dokumentationen für Datenschutzfragen sind abhängig von den Systemeigenschaften. Typische Dokumentationen werden thematisiert und Realisierungsalternativen werden aufgezeigt.
- Datenschutzfolgenabschätzung: Für Verfahren mit besonderer Gefährdung sieht die Gesetzgebung eine Datenschutzfolgenabschätzung, eine Risikoabwägung vor Inbetriebnahme vor. Der Prozess, die Organisation Datenschutzfolgenabschätzungen und geeignete Dokumentationen der Ergebnisse werden thematisiert.

Die Vermittlung der Inhalte erfolgt anhand konkreter praktischer Beispiele.

Besondere Lehrformen
Vorlesung in Fernlehre (eLearning): Interaktive Lernplattform, Skript, Einsendeaufgaben und Reading Assignments. Die Betreuung erfolgt durch den Dozenten, der mit den Studierenden über ein Forum und über E-Mail kommuniziert.
Prüfungsformen
Mündliche Prüfung über die Modulinhalte und Reading Assignments (Dauer ca. 20-30 Minuten)
Voraussetzungen für die Vergabe von Kreditpunkten
Bestehen des Prüfungsgesprächs. Prüfungsvorleistung für die Zulassung zum Prüfungsgespräch: Bearbeitung von 75 % der Übungsaufgaben mit einem Gesamtergebnis von 50 % der vergebenen Punkte
Verwendung des Moduls in anderen Studiengängen
nein
Stellenwert der Note für die Endnote
5/120
Modulbetreuer
Dr. Kai-Uwe Loser
Literatur
Skript „Datenschutz in der betrieblichen Praxis“
Sonstige Informationen

Wahlpflichtmodul: Modul 9.3: Einführung in die Forensische Informatik				
Workload 5 CP (150 h)	Studienphase 2. Studienjahr	Turnus Jährlich zum Sommersemester	Dauer 1 Semester	
Lehrveranstaltungen Einführung in die Forensische Informatik		Kontaktzeit 20 h	Selbststudium 130 h	Gruppengröße Mind. 3, Max. 20
Teilnahmevoraussetzungen Empfehlenswert: Kenntnisse in Programmierung; Linuxkenntnisse oder die Bereitschaft sich während des Kurses Linuxkenntnisse anzueignen.				
Lernergebnisse Nach erfolgreichem Abschluss des Moduls verfügen die Studierenden über grundlegende Kenntnisse und Kompetenzen in digitaler Beweismittelsicherung. Die Studierenden können anschließend forensische Methoden und forensische Berichte bezüglich ihrer Zweckdienlichkeit in einer Ermittlung bewerten. Sie können für bestimmte Problemstellungen forensische Verfahren einsetzen und ihre Korrektheit argumentativ verteidigen.				
Inhalte Digitale Forensik befasst sich mit der Sammlung, Aufbereitung und Analyse digitaler Spuren zur Verwendung vor Gericht. Ausgangspunkt ist jeweils der Verdacht auf einen Computer-einbruch oder eine Straftat, die mit Hilfe von digitalen Geräten vorgenommen worden ist. Diese Lehrveranstaltung gibt einen Überblick über die methodische Fundierung der digitalen Forensik. Der Schwerpunkt liegt auf der Einbettung der digitalen Forensik in die klassische kontinuierliche (analoge) Forensik sowie auf der Dokumentation von forensischen Untersuchungen.				
Besondere Lehrformen Vorlesung in Fernlehre (eLearning) mit Studienbriefen, Übungen und Tests über die interaktive Lernplattform, Online-Konferenzen, Chat und Forum. Die Betreuung erfolgt über einen Tutor; der mit den Studierenden über ein Forum und über E-Mail kommuniziert.				
Prüfungsformen Mündliches Prüfungsgespräch (Dauer ca. 20-30 Minuten)				
Voraussetzungen für die Vergabe von Kreditpunkten Bestehen des Prüfungsgesprächs.				
Verwendung des Moduls in anderen Studiengängen nein				
Stellenwert der Note für die Endnote 5/120				
Modulbetreuer Prof. Dr. Felix Freiling, Friedrich-Alexander Universität Erlangen-Nürnberg				
Literatur Dewald, Andreas/ Freiling, Felix C. (Hg.): Forensische Informatik, 2015				
Sonstige Informationen				

Wahlpflichtmodul: Modul 9.4: Group-Oriented Communication and Application Security				
Workload	Studienphase	Turnus	Dauer	
5 CP (150 h)	2.-3. Studienjahr	Semesterweise	1 Semester	
Lehrveranstaltungen		Kontaktzeit	Selbststudium	Gruppengröße
Group-Oriented Communication and Application Security		0 h	150 h	Mind. 3, Max. 50
Teilnahmevoraussetzungen				
Empfehlenswert: grundlegende Kenntnisse in Kryptographie sind von Vorteil				
Lernergebnisse				
Studierende können nach erfolgreichem Abschluss des Moduls die erworbenen Kenntnisse anwenden und weiterentwickeln. Sie sind in der Lage als Systemarchitekt oder Produktentwickler, innovative digitale Werkzeuge zur Gruppenkommunikation und Informationsverarbeitung zu entwickeln. Sie können im Prüfungsgespräch selbständig Lösungen entwickeln und deren Sicherheit überzeugend verargumentieren.				
Inhalte				
Diese Online-Vorlesung beschäftigt sich primär mit kryptographischen Sicherheitsverfahren, die zur Absicherung gruppenorientierter und kollaborationsbasierter Kommunikationsanwendungen eingesetzt werden können. Die Online-Vorlesung beschäftigt sich u.a. mit folgenden Themen:				
<ul style="list-style-type: none"> • Gruppenbasierte Anwendungen, Groupware • Anforderungen an eine zuverlässige Gruppenkommunikation • Zentralisierte und verteilte Verfahren zur Realisierung der Zugangs- bzw. Zugriffskontrolle in Gruppen, Vertrauen zwischen den Gruppenteilnehmern • Sichere Gruppenkommunikation (Geheimhaltung und Authentisierung), Schlüsselmanagement 				
Anonyme Gruppenkommunikation, digitale Gruppen- und Ring-Signaturen.				
Besondere Lehrformen				
Vorlesung in Fernlehre (eLearning): Interaktive Lernplattform, Skript. Einsendeaufgaben und Reading Assignments. Die Betreuung erfolgt durch den Dozenten, der mit den Studierenden über ein Forum und über E-Mail kommuniziert.				
Prüfungsformen				
Mündliche Prüfung über die Modulinhalte und Reading Assignments (Dauer ca. 20-30 Minuten)				
Voraussetzungen für die Vergabe von Kreditpunkten				
Bestehen des Prüfungsgesprächs.				
Verwendung des Moduls in anderen Studiengängen				
nein				
Stellenwert der Note für die Endnote				
5/120				
Modulbetreuer				
Prof. Dr. Mark Manulis, Universität der Bundeswehr München				
Literatur				
Skript „Group-Oriented Communication and Application Security“				
Sonstige Informationen				

Wahlpflichtmodul: Modul 9.5: Implementierung kryptographischer Verfahren			
Workload	Studienphase	Turnus	Dauer
5 CP (150 h)	2.-3. Studienjahr	Semesterweise	1 Semester
Lehrveranstaltungen		Kontaktzeit	Selbststudium
Implementierung kryptographischer Verfahren		0 h	150 h
Gruppengröße Mind. 3, Max. 50			
Teilnahmevoraussetzungen			
Empfehlenswert: Grundkenntnisse der Programmiersprache C++ (falls nur C bekannt ist, sollte die Bereitschaft zum Einarbeiten in die Grundlagen von C++ vorliegen) sowie Modul 1 "Einführung in die Kryptographie".			
Lernergebnisse			
Studierende erlernen die grundlegenden Algorithmen für die effiziente Implementierung rechenintensiver Kryptoverfahren. Insbesondere den Umgang von Algorithmen mit sehr langen Operanden haben sie nach Abschluss des Moduls verstanden, ebenso wie das Zusammenspiel von Implementierungsmethoden und kryptographischer Sicherheit			
Inhalte			
Diese Vorlesung gibt eine Einführung in Verfahren zur schnellen und sicheren Implementierung kryptographischer Algorithmen. Im ersten Teil werden Methoden zum effizienten Potenzieren ausführlich behandelt, da diese für alle verbreiteten asymmetrischen Verfahren von großer Bedeutung sind. Für den weit verbreiteten RSA-Algorithmus werden zudem spezielle Beschleunigungsverfahren vorgestellt. Im zweiten Teil werden Algorithmen für effiziente Langzahlarithmetik entwickelt. Zunächst werden grundlegende Methoden zur Darstellung von Langzahlen in Rechnern und Verfahren zur Addition vorgestellt. Der Schwerpunkt dieses Teils liegt auf Algorithmen zur effizienten modularen Multiplikation. Neben dem Karatsuba-Algorithmus wird die Montgomery-Multiplikation behandelt. Im dritten Teil werden sichere Implementierungen besprochen. Es erfolgt eine Einführung in aktive und passive Seitenkanalattacken. Es werden aktive Attacken gegen Blockchiffren und RSA vorgestellt. Als wichtige Vertreter der passiven Attacken werden die Grundlagen von SPA (simple power analysis) und DPA (differential power analysis) eingeführt.			
Besondere Lehrformen			
Vorlesung in Fernlehre (eLearning): Interaktive Lernplattform, Skript, bewertete Online-Übungen und / oder Einsendeaufgaben. Jeder Übungszettel besteht aus einer oder mehreren theoretischen Aufgaben und einer kleinen Programmieraufgabe. Die Betreuung erfolgt durch einen Tutor, der mit den Studierenden über ein Forum und über E-Mail kommuniziert.			
Prüfungsformen			
Projekte (2 Projekte) und Klausur (2 Stunden)			
Voraussetzungen für die Vergabe von Kreditpunkten			
Bestehen der Modulprüfung, bestehend aus: Projekte 20% (2x10%), Modulabschlussklausur 80%.			
Verwendung des Moduls in anderen Studiengängen			
nein			
Stellenwert der Note für die Endnote			
5/120			
Modulbetreuer			
Prof. Dr. Christof Paar			
Literatur			
Skript „Implementierung kryptographischer Verfahren“			
Sonstige Informationen			

Wahlpflichtmodul: Modul 9.6: Information Security Management in der Praxis				
Workload	Studienphase	Turnus	Dauer	
5 CP (150 h)	2.-3. Studienjahr	Semesterweise	1 Semester	
Lehrveranstaltungen		Kontaktzeit	Selbststudium	Gruppengröße
Information Security Management in der Praxis		15 h	135 h	Mind. 3, Max. 50
Teilnahmevoraussetzungen				
keine				
Lernergebnisse				
<p>Die Studierenden erwerben Kenntnisse zur Errichtung und zum Betrieb einer Security Organisation in mittleren bis großen Unternehmen. Dabei lernen sie organisatorische Strukturen, Budgetierung, Planung, Ressourcen, Architekturen und Prozesse kennen. Nach Abschluss des Moduls können sie Industrie „best practice standards“ auf bestehende Security Prozesse anwenden, verstehen und optimieren.</p> <p>Sie können Awareness-Maßnahmen planen, umsetzen und messen, Key-Performance-Indikatoren bestimmen und auswerten sowie die Kommunikation auf unterschiedliche Zielgruppen anpassen. Sie haben gelernt, eine Vision, Mission und Strategie von Security Einzelprojekten und Security Organisationen zu entwickeln, Security Incidents erfolgreich zu behandeln und zu dokumentieren. Sie können Risikoanalysen durchführen und bewerten sowie Security Assessments durchführen, verstehen und einsetzen. Sie können die von ihnen entwickelten Methoden im Unternehmensumfeld schriftlich und mündlich überzeugend vorstellen.</p>				
Inhalte				
<p>Die Vorlesung beschäftigt sich mit der praktischen Anwendung von Security Industrie-Standards und mit aktuellen und neuen Herausforderungen für das „Security Management“. Folgende „Information Security“ Elemente werden analytisch betrachtet:</p> <ul style="list-style-type: none"> • Vision, Mission und Strategie • Planung & Controlling • Risk Management – Frameworks und Policies und deren Durchsetzung • Typische Security-Organisationen heute: Strukturen, Rollen und Herausforderungen • Awareness & Qualitäts-/Erfolgskontrolle • Skill-Management, -Surveys & -Reporting • Operationelle IT-Security Services vs. “Managed Security Services” - MSS • Compliance und Definition von Ausnahmen, Prozessen und Dienstleistungen • Social Engineering & andere Angriffe • Globale Security Architekturen im Cloud Zeitalter • Program Management <p>Ferner beschäftigt sich die Vorlesung mit finanziellen Aspekten des Security Managements wie der Kosten-Nutzen-Analyse von Security Lösungen, der Berechnung des Security-Investitionsvolumens und ROI in der Praxis.</p> <p>Abschließend wird ein Überblick über Fortbildungsmöglichkeiten und Zertifizierungen gegeben.</p>				

Besondere Lehrformen
Vorlesung in Fernlehre (eLearning) und Präsenzveranstaltung. Interaktive Lernplattform und Skript. Die Betreuung erfolgt durch einen Tutor, der mit den Studierenden über ein Forum und über E-Mail kommuniziert.
Prüfungsformen
Schriftliche Hausarbeit (Umfang ca. 20 Seiten)
Voraussetzungen für die Vergabe von Kreditpunkten
Bestehen der Modulprüfung.
Verwendung des Moduls in anderen Studiengängen
nein
Stellenwert der Note für die Endnote
5/120
Modulbetreuer
Prof. Dr. Thorsten Holz
Literatur
Skript „Information Security Management in der Praxis“
Sonstige Informationen

Wahlpflichtmodul: Modul 9.7: Einführung in BSI-Grundschutz und ISO 27001				
Workload	Studienphase	Turnus	Dauer	
5 CP (150 h)	2.-3. Studienjahr	Semesterweise	1 Semester	
Lehrveranstaltungen		Kontaktzeit	Selbststudium	Gruppengröße
Einführung in BSI-Grundschutz und ISO 27001		15 h	135 h	Mind. 3, Max. 50
Teilnahmevoraussetzungen				
keine				
Lernergebnisse				
Studierende sind nach Abschluss des Moduls in der Lage, die Standards BSI IT-Grundschutz und ISO 27001 / ISO 27002 anzuwenden. Sie können das Sicherheitsniveau innerhalb einer Organisation mit Bezug auf diese Standards analysieren und bewerten und Maßnahmen zur Optimierung entwickeln. Sie können diese Optimierungen gegen Einwände überzeugend verteidigen.				
Inhalte				
Die Vorlesung behandelt die maßgeblichen Industriestandards zur IT- und Informationssicherheit. Dazu werden der BSI IT-Grundschutz und die Normenreihe ISO 2700X detailliert betrachtet und miteinander verglichen. Neben der Beschäftigung mit Definitionen, Zielen und Grenzen der Standards werden außerdem anhand von Fallstudien Fragen der praktischen Umsetzung behandelt. Den Abschluss der Vorlesung bildet die Beschäftigung mit Aspekten der Zertifizierung von Sicherheit.				
Besondere Lehrformen				
Vorlesung in Fernlehre (eLearning) und Präsenzveranstaltung. Interaktive Lernplattform und Skript, Fallstudien. Die Betreuung erfolgt durch den Dozenten, der mit den Studierenden über ein Forum und über E-Mail kommuniziert.				
Prüfungsformen				
Klausur (2 Stunden)				
Voraussetzungen für die Vergabe von Kreditpunkten				
Bestehen der Modulabschlussklausur.				
Verwendung des Moduls in anderen Studiengängen				
nein				
Stellenwert der Note für die Endnote				
5/120				
Modulbetreuer				
Wilhelm Dolle, KPMG				
Literatur				
Skript „Einführung in BSI-Grundschutz und ISO 27001“ (W. Dolle) inkl. Fallstudien				
Sonstige Informationen				

Wahlpflichtmodul: Modul 9.8: Mobile Security			
Workload	Studienphase	Turnus	Dauer
5 CP (150 h)	2.-3. Studienjahr	Semesterweise	1 Semester
Lehrveranstaltungen		Kontaktzeit	Selbststudium
Mobile Security		12 h	138 h
Teilnahmevoraussetzungen			
Empfehlenswert: Grundlagenwissen in den Bereichen Rechnernetze und IT-Sicherheit			
Lernergebnisse			
Die Studierenden kennen nach erfolgreichem Abschluss des Moduls typische Gefahrenpotentiale und die wesentlichen Sicherheitsprobleme beim Einsatz von mobilen Netzen, Systemen, Anwendungen und Geräten. Sie können Teilaspekte zu einer Gesamtheit integrieren und Risiken kritisch und ganzheitlich (mobile Systeme als Erweiterung oder als integralen Bestandteil einer IT-Infrastruktur) bewerten und haben ein allgemeines Verständnis der verschiedenen Sicherheitstechnologien und -standards. Sie sind in der Lage, Normen, Standards, Richtlinien und Leitfäden zur Absicherung von mobilen Systemen zu verstehen und diese für individuelle Fälle anzuwenden.			
Inhalte			
Die Inhalte, die in Form von Hausarbeiten behandelt werden, umfassen typische Themenbereiche wie:			
<ul style="list-style-type: none"> • WiFi • Bluetooth • Near Field Communication • Mobilfunknetze • Mobile Identity & Access Management (IAM) • Bring Your Own Device (BYOD) und Corporate Owned, Personally Enabled (COPE) • Mobile Device Management (MDM) • Mobile Forensik • Schatten-IT • Pentesting von Smartphones bzw. mobilen Betriebssystemen • Härtung von Smartphones bzw. mobilen Betriebssystemen • Erkennung und Abwehr von Angriffen auf Smartphones 			
Besondere Lehrformen			
Schriftliche Ausarbeitung (Essay) mit Feedback durch den Dozenten, der mit den Studierenden über ein Forum, E-Mail oder ZOOM kommuniziert.			
Prüfungsformen			
Schriftliche Hausarbeit (Umfang mindestens 20 Seiten) (30%) mit abschließender Präsentation (70%)			
Voraussetzungen für die Vergabe von Kreditpunkten			
Bestehen der Modulprüfung.			
Verwendung des Moduls in anderen Studiengängen			
nein			
Stellenwert der Note für die Endnote			
5/120			
Modulbetreuer			
Prof. Dr.-Ing. Evren Eren, Hochschule Bremen			
Literatur			
Wird in der Veranstaltung individuell diskutiert			
Sonstige Informationen			

Wahlpflichtmodul: Modul 9.9: Virenschutz im Unternehmen			
Workload	Studienphase	Turnus	Dauer
5 CP (150 h)	2.-3. Studienjahr	Semesterweise	1 Semester
Lehrveranstaltungen		Kontaktzeit	Selbststudium
Virenschutz im Unternehmen		8 h	142 h
Teilnahmevoraussetzungen		Gruppengröße	
keine		Mind. 3, Max. 50	
Lernergebnisse			
<p>Nach erfolgreichem Abschluss des Moduls sind die Studierenden in der Lage, Konzepte zu erstellen und Maßnahmen einzuleiten, die ein Unternehmen und die dort verwendeten Rechner vor Malware-Angriffen schützen. Sie verstehen die Komplexität und Tragweite dieser wichtigen Bedrohung, und haben einen Einblick in die wichtigsten aktuellsten Forschungsergebnisse eines auf diesem Gebiet führenden Unternehmens erhalten. Sie sind in der Lage, diesen aktuellen Stand der Forschung adäquat und verständlich innerhalb ihrer Firma zu kommunizieren.</p>			
Inhalte			
<p>Das Modul befasst sich mit Angriffen, die von Malware (einschließlich Viren) ausgehen. Dabei werden die speziellen Anforderungen von Unternehmen und anderen Organisationen besonders berücksichtigt.</p> <p>Zunächst wird anhand von ausgewählten Ereignissen in der Vergangenheit die historische Entwicklung aber auch die Bandbreite der Computerschädlinge dargestellt. Danach werden Computerschädlinge nach mehreren Kriterien klassifiziert und Angriffe genauer untersucht. Verschiedene Bedrohungen werden skizziert und auch die Urheber und Nutzer von Malware und deren Motivation werden genauer betrachtet. Mögliche Schutzmaßnahmen werden dargestellt und es wird erläutert, mit welchen Techniken und Technologien Virens Scanner, Firewalls, Intrusion Detection/ Prevention Systeme und andere Schutztechnologien arbeiten, um vor Malware und ihren Folgen zu schützen.</p> <p>In einem Überblick werden konkrete Schutzmaßnahmen für verschiedene Anwendungsszenarien vorgestellt.</p>			
Besondere Lehrformen			
Vorlesung in Fernlehre (eLearning) mit Fallstudien und Präsenzveranstaltung. Interaktive Lernplattform, Skript. Die Betreuung erfolgt durch den Dozenten, der mit den Studierenden über ein Forum und über E-Mail kommuniziert.			
Prüfungsformen			
Klausur (2 Stunden)			
Voraussetzungen für die Vergabe von Kreditpunkten			
Bestehen der Modulabschlussklausur.			
Verwendung des Moduls in anderen Studiengängen			
nein			
Stellenwert der Note für die Endnote			
5/120			
Modulbetreuer			
Ralf Benz Müller			
Literatur			
Skript „Virenschutz in Unternehmen“			
Sonstige Informationen			

Wahlpflichtmodul: Modul 9.10: Systemsicherheit				
Workload	Studienphase	Turnus	Dauer	
5 CP (150 h)	2.-3. Studienjahr	jährlich zum Sommersemester	1 Semester	
Lehrveranstaltungen		Kontaktzeit	Selbststudium	Gruppengröße
Systemsicherheit		8 h	142 h	Min. 3, Max. 30
Teilnahmevoraussetzungen				
Grundwissen Programmierung				
Lernergebnisse				
<p>Die Studierenden beherrschen wichtige theoretische und praktische Aspekte von Sicherheitsmechanismen moderner Softwaresystemen. Sie sind in die Lage, die Sicherheit eines gegebenen Programms eigenständig zu analysieren, Schwachstellen im Design aufzudecken sowie selbständig Lösungsmöglichkeiten und Schutzmechanismen zu entwickeln. Darüber hinaus haben sie grundlegende Begriffe aus dem Bereich der Systemsicherheit kennengelernt. Sie sind in der Lage, neue Sicherheitsmodelle selbst zu erstellen und diese argumentativ zu verteidigen.</p>				
Inhalte				
<p>Im Rahmen der Vorlesung werden wichtige theoretische und praktische Aspekte aus dem Bereich der Systemsicherheit vorgestellt und diskutiert. Der Fokus liegt dabei auf verschiedenen Aspekten der Softwaresicherheit und verschiedene Angriffs- und Verteidigungstechniken werden vorgestellt. Die Studierenden sollen am Ende der Vorlesungsreihe in die Lage sein, die Sicherheit verschiedener Softwaresysteme zu analysieren, Schwachstellen im Design und der Implementierung aufzudecken sowie selbständig Sicherheitsmechanismen zu entwickeln. Darüber hinaus werden auch andere Aspekte aus dem Bereich der Systemsicherheit wie Privatheit und Anonymität betrachtet.</p>				
Besondere Lehrformen				
<p>Vorlesung in Fernlehre (eLearning): Interaktive Lernplattform, Skript, Vorlesungsvideos. Begleitet wird die Vorlesung von Übungen, in denen die vorgestellten Konzepte und Techniken praktisch eingeübt werden. Die Betreuung erfolgt durch den Dozenten, der mit den Studierenden über ein Forum und über E-Mail kommuniziert.</p>				
Prüfungsformen				
Klausur (2 Stunden)				
Voraussetzungen für die Vergabe von Kreditpunkten				
Bestehen der Modulabschlussklausur.				
Verwendung des Moduls in anderen Studiengängen				
nein				
Stellenwert der Note für die Endnote				
5/120				
Modulbetreuer				
Prof. Dr. Thorsten Holz				
Literatur				
Skript „Systemsicherheit“				
Sonstige Informationen				

Wahlpflichtmodul: Modul 9.11: Programmanalyse			
Workload	Studienphase	Turnus	Dauer
5 CP (150 h)	2.-3. Studienjahr	jährlich zum Wintersemester	1 Semester
Lehrveranstaltungen		Kontaktzeit	Selbststudium
Programmanalyse		8 h	142 h
Teilnahmevoraussetzungen			
Grundwissen Programmierung			
Lernergebnisse			
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.			
Inhalte			
In der Vorlesung werden unter anderem die folgenden Themen und Techniken aus dem Bereich der Programmanalyse behandelt:			
<ul style="list-style-type: none"> • Statische und dynamische Analyse von Programmen • Analyse von Kontroll- und Datenfluss • Symbolische Ausführung • Taint Tracking • 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.			
Besondere Lehrformen			
Vorlesung in Fernlehre (eLearning): Interaktive Lernplattform, Skript, Vorlesungsvideos. Begleitet wird die Vorlesung von Übungen, in denen die vorgestellten Konzepte und Techniken praktisch eingeübt werden. Die Betreuung erfolgt durch den Dozenten, der mit den Studierenden über ein Forum und über E-Mail kommuniziert.			
Prüfungsformen			
Klausur (2 Stunden)			
Voraussetzungen für die Vergabe von Kreditpunkten			
Bestehen der Modulabschlussklausur.			
Verwendung des Moduls in anderen Studiengängen			
nein			
Stellenwert der Note für die Endnote			
5/120			
Modulbetreuer			
Prof. Dr. Thorsten Holz			
Literatur			
Skript „Programmanalyse“			
Sonstige Informationen			
Dieses Modul wird letztmalig im WS 26/27 angeboten.			

Wahlpflichtmodul: Modul 9.12: Menschliches Verhalten in der IT-Sicherheit				
Workload	Studienphase	Turnus	Dauer	
5 CP (150 h)	2.-3. Studienjahr	Jährlich zum Sommersemester	1 Semester	
Lehrveranstaltungen		Kontaktzeit	Selbststudium	Gruppengröße
Menschliches Verhalten in der IT-Sicherheit		30 h	150 h	Min. 3, Max. 30
Teilnahmevoraussetzungen				
Keine				
Lernergebnisse				
<p>Ziel der Veranstaltung "Menschliches Verhalten in der IT-Sicherheit" ist, dass die Studierenden verstehen lernen, welche Faktoren Einfluss auf das Sicherheitsverhalten bei Angestellten in Unternehmen und Konsumenten im Alltag nehmen, und welche Möglichkeiten bestehen, dieses zu beeinflussen und zu verändern.</p> <p>Außerdem soll vermittelt werden, warum bestehende Ansätze des Information Security Managements (auch nach ISO 27000) in der Praxis oft nicht funktionieren und wie wir sie erweitern bzw. anpassen sollten.</p> <p>Schnittstellen zu anderen Modulen:</p> <ul style="list-style-type: none"> • Modul 8 (Sicherheitsmanagement) • Modul 9.6 (Information Security Management in der Praxis) • Modul 10 (Rechtliche Aspekte der IT-Sicherheit) 				
Inhalte				
<p>In der Veranstaltung "Menschliches Verhalten in der IT-Sicherheit" sollen, nach einer kurzen Einführung in die Human Centred Security, unter anderem folgende Themen behandelt werden:</p> <ol style="list-style-type: none"> 1. Organisationen, Organisationskultur und Sicherheitskultur 2. Change Management 3. Veränderung des Sicherheitsverhaltens von Mitarbeitenden 4. Risk Management 5. Vertrauen in der IT-Sicherheit 6. Konflikte in der IT-Sicherheit 7. Ökonomische Aspekte der IT-Sicherheit 				
Besondere Lehrformen				
<p>Vorlesung, Übungen und Quiz Medienform: Vorlesungsaufzeichnungen, Live-Übungen per Zoom, kooperative Lernangebote, Präsentationen, Online-Quiz´</p>				
Prüfungsformen				
Klausur (2 Stunden)				
Voraussetzungen für die Vergabe von Kreditpunkten				
Bestehen der Modulabschlussklausur.				
Verwendung des Moduls in anderen Studiengängen				
Ja, Studiengang IT-Sicherheit				
Stellenwert der Note für die Endnote				
5/120				
Modulbetreuer				
Prof. Dr. M. Angela Sasse, M.Sc. Jens Odenbusch, M.Sc. Markus Schöps				

Literatur

Auszug aus der Literaturliste:

- Kluge, Annette; Gronau, Norbert (2018): Intentional Forgetting in Organizations: The Importance of Eliminating Retrieval Cues for Implementing New Routines. In: *Frontiers in psychology* 9, S. 51.
- Adams, John (2016): Risk and culture. In: *Routledge handbook of risk studies*. London: Routledge, S. 83–93.
- Kirlappos, Iacovos; Parkin, Simon; Sasse, M. Angela (2014): Learning from “Shadow Security”. Why Understanding Non-Compliant Behaviors Provides the Basis for Effective Security.
- Kirlappos, Iacovos; Parkin, Simon; Sasse, M. Angela (2014): Learning from “Shadow Security”. Why Understanding Non-Compliant Behaviors Provides the Basis for Effective Security. In: Matthew Smith und David Wagner (Hg.): *Proceedings 2014 Workshop on Usable Security*. Workshop on Usable Security. San Diego, CA, February 23, 2014. Reston, VA: Internet Society.
- Ashenden, Debi; Lawrence, Darren (2016): Security Dialogues: Building Better Relationships between Security and Business. In: *IEEE Secur. Privacy* 14 (3), S. 82-87.
- Flechais, I., Mascolo, C., Sasse, M.A. (2007). Integrating security and usability into the requirements and design process. *International Journal of Electronic Security and Digital Forensics*, 1 (1), 12-26.
- Caputo, D.D., Pfleeger, S.L., Sasse, M.A., Ammann, P., Offutt, J., Deng, L. (2016). Barriers to Usable Security? Three Organizational Case Studies. *IEEE Security and Privacy*, 14 (5), 22-32.

Sonstige Informationen

Dieses Modul wird letztmalig im Sommersemester 2026 angeboten.

Wahlpflichtmodul:
Modul 9.13: Human Aspects of Cryptography Adoption and Use

Workload	Studienphase	Turnus	Dauer	
5 CP (150 h)		Jährlich zum Wintersemester	1 Semester	
Lehrveranstaltungen		Kontaktzeit	Selbststudium	Gruppengröße
Human Aspects of Cryptography Adoption and Use		30 h	150 h	Min. 10, Max. 30

Teilnahmevoraussetzungen
 Gute Englisch-Kenntnisse. Das Modul wird auf Englisch angeboten.

Lernergebnisse
 The aim of the lecture is to examine the reasons why
 a) cryptographic solutions – which experts agree offer good protection against most of the common attacks today – are often not adopted by individuals and organisations, and
 b) end-users, developers, and system administrators who do use cryptographic solutions in some form frequently make mistakes that undermine the security protection.
 We then identify effective ways to increase adoption and enable correct use of cryptography.

Inhalte
 In 1999, Whitten & Tygar’s seminal USENIX paper “Why Johnny Can’t Encrypt” established that even though the problem of End-to-End Encryption is technically solved, people cannot use PGP encryption correctly, even with a graphical user interface and instructions. Over the past 20 years, there has been a string of “Johnny” papers trying to encourage adoption or correct usage of secure tools - with mixed results. This lecture aims to systematically examine the results of these and other studies and identify effective ways of promoting adoption and enabling the correct use of cryptography. This course covers the following topics.

- Usability, usable security, utility, and technology adoption
- History of Human Factors and Encryption
- Security threat models and people’s mental models
- What is trust? How is trust impacting the adoption of cryptographic applications?
- Cryptography ecosystem – where do cryptographic standards come from?
- Complexity or simplicity – who needs to know what?
- Applying this knowledge to different cryptographic applications:
 - PGP and S/MIME: End-to-End encrypted Email
 - WhatsApp and Signal: End-to-End security for the masses?
 - TLS: A crypto protocol success story
 - End User Privacy Tools: TOR/TAILS, Disk Encryption, VPNs
 - Passwordless Authentication (FIDO, PassKeys, WebAuthn)

Besondere Lehrformen
 Vorlesungen, Live Nachbesprechungen der Übungsergebnisse, Hausaufgaben und Quiz.
 Medienform: Vorlesungsaufzeichnungen, Live-Besprechung von Übungen per Zoom, Online-Quiz via Moodle.

Prüfungsformen
 Mündliche Prüfung (ca. 20-30 Minuten)

Voraussetzungen für die Vergabe von Kreditpunkten
 Bestehen des Prüfungsgesprächs.

Verwendung des Moduls in anderen Studiengängen
 Ja, Studiengang IT-Sicherheit

Stellenwert der Note für die Endnote
5/120
Modulbetreuer
Prof. Dr. M. Angela Sasse, M.Sc. Jens Odenbusch, M.Sc. Felix Reichmann
Literatur
<p>Excerpt from the literature list:</p> <ul style="list-style-type: none"> • Whitten, A., & Tygar, J. D. (1999, August). <i>Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0</i>. In USENIX security symposium (Vol. 348, pp. 169-184). • Ruoti, S., & Seamons, K. (2019). <i>Johnny's journey toward usable secure email</i>. IEEE Security & Privacy, 17(6), 72-76. • Johnson-Laird, P. N. (1983). <i>Mental models: Towards a cognitive science of language, inference, and consciousness (No. 6)</i>. Harvard University Press. • Norman, D. A. (2014). <i>Some observations on mental models</i>. In <i>Mental models</i> (pp. 15-22). Psychology Press. • Wu, J., & Zappala, D. (2018). <i>When is a tree really a truck? exploring mental models of encryption</i>. In Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018) (pp. 395-409). • Demjaha, A., Spring, J. M., Becker, I., Parkin, S., & Sasse, M. A. (2018). <i>Metaphors considered harmful? An exploratory study of the effectiveness of functional metaphors for end-to-end encryption</i>. In Proc. USEC (Vol. 2018). Internet Society. • Wu, J., Gattrell, C., Howard, D., Tyler, J., Vaziripour, E., Zappala, D., & Seamons, K. (2019). <i>"Something isn't secure, but I'm not sure how that translates into a problem": Promoting autonomy by designing for understanding in Signal</i>. In Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019) (pp. 137-153). • Renaud, K., Volkamer, M., & Renkema-Padmos, A. (2014, July). <i>Why doesn't Jane protect her privacy?</i>. In International Symposium on Privacy Enhancing Technologies Symposium (pp. 244-262). Springer, Cham. • Abu-Salma, R., Sasse, M. A., Bonneau, J., Danilova, A., Naiakshina, A., & Smith, M. (2017, May). <i>Obstacles to the adoption of secure communication tools</i>. In 2017 IEEE Symposium on Security and Privacy (SP) (pp. 137-153). IEEE. • Herzberg, A., & Leibowitz, H. (2016, December). <i>Can Johnny finally encrypt? Evaluating E2E-encryption in popular IM applications</i>. In Proceedings of the 6th Workshop on Socio-Technical Aspects in Security and Trust (pp. 17-28). • Stransky, C., Wermke, D., Schrader, J., Huaman, N., Acar, Y., Fehlhaber, A. L., & Fahl, S. (2021). <i>On the Limited Impact of Visualizing Encryption: Perceptions of E2E Messaging Security</i>. In Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021) (pp. 437-454). • Marks, L. (2012). <i>Between Silk and Cyanide: A Code Maker's War 1941-45</i>. The History Press.
Sonstige Informationen
Dieses Modul wurde letztmalig im WS 25/26 angeboten.