RUHR UNIVERSITÄT BOCHUM

RUB

isits
International School of IT Security AG

Modulhandbuch

des Weiterbildungsstudiengangs

„Applied IT Security“

(Master of Science)

Modulhandbuch

„Applied IT Security“ (M. Sc.)

isits AG
International School of IT Security

Ruhr-Universität Bochum
Fakultät für Elektrotechnik und Informationstechnik

Inhaltsverzeichnis

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.

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

Pflichtmodule: Im Umfang von 70 CP obligatorisch zu belegende Module. Für die Belegung der Module 2, 3 und 4 werden je nach Vorkenntnissen Empfehlungen ausgesprochen.

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

Schriftliche Hausarbeit: Form der Modulabschlussprüfung. Umfang: ca. 20 Seiten.

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

2 Exemplarischer Studienverlaufsplan

Semester	Modul											
	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)	IST-CP
1. (WS)	Einführung Kryptographie	*Diskrete Mathematik**										
	10 CP	*10 CP*										20
2. (SoSe)			*Informatik**	*Informations-technik**			Kryptographie					
			10 CP	*10 CP*			10 CP					20
3. (WS)					Netz-sicherheit			Sicherheits-management	Einführung BSI			
					10 CP			5 CP	5 CP			20
4. (SoSe)						Sicherheits-systeme u. -protokolle			Software Implemen-tierung	Rechtliche Aspekte		
						10 CP			5 CP	5 CP		20
5. (WS)									Information Security		Thesis	
									5 CP		*25 CP (verteilt auf 2 Sem)*	
									Mobile Security			
									5 CP		5 CP	15
6. (SoSe)									Einführung Forensik			
									5 CP		20 CP	25
Gesamt												**120**

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

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

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.

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.

Inhalte

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.

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.

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.

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.

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
Erfolgreiches Bestehen der Modulabschlussklausur.
Verwendung des Moduls in anderen Studiengängen
Nein
Stellenwert der Note für die Endnote
1/12
Modulbetreuer
Prof. Dr. Christof Paar
Literatur
Paar, Christof/ Pelzl, Jan: Understanding Cryptography: A Text-book for Students and Practitioners, Springer, 2009
Sonstige Informationen

Pflichtmodul:
Modul 2: Diskrete Mathematik für IT-Sicherheit

Workload	Studienphase	Turnus	Dauer	
10 CP (300 h)	1. Studienjahr	Semesterweise	1 Semester	
Lehrveranstaltungen		**Kontaktzeit**	**Selbststudium**	**Gruppengröße**
Diskrete Mathematik für IT-Sicherheit		0 h	300 h	Max. 50

Teilnahmevoraussetzungen

keine

Lernergebnisse

Nach erfolgreichem Abschluss des Moduls haben die Studierenden den professionellen Umgang mit abstrakten, diskreten Strukturen erlernt. Sie haben die Fähigkeit, konkrete Problemstellungen mit solchen Strukturen zu modellieren und Schlussfolgerungen aus gegebenen Informationen zu ziehen. Dabei gelangen sie zu einem Verständnis für grundlegende algorithmische Techniken und die Analyse von Algorithmen.

In den einzelnen Teilen der Vorlesung erwerben die Studierenden die jeweils grundlegenden Konzepte (in Kombinatorik, Graphentheorie, elementarer Zahlentheorie und elementarer Wahrscheinlichkeitstheorie). Sie schulen ihre intellektuelle Fähigkeit, die logischen Zusammenhänge zwischen den Konzepten zu überblicken und „versteckte“ Anwendungsmöglichkeiten zu erkennen. Sie können Probleme aus dem Alltag abstrakt modellieren und ihr Modell argumentativ verteidigen.

Inhalte

Die Vorlesung „Diskrete Mathematik“ beschäftigt sich mit endlichen Strukturen. Sie gliedert sich in 5 Teile.

Teil 1 ist der Kombinatorik gewidmet. Insbesondere werden grundlegende Techniken vermittelt, um so genannte Zählprobleme zu lösen.

Teil 2 beschäftigt sich mit der Graphentheorie. Graphen werden zur Modellierung von Anwendungsproblemen benutzt. Es werden Techniken zur Graphexploration und weitere ausgesuchte Graphenprobleme behandelt.

Teil 3 vermittelt Grundkenntnisse in elementarer Zahlentheorie und endet mit einem Ausblick auf kryptographische Anwendungen.

Grundlegende Designtechniken für effiziente Algorithmen bilden das zentrale Thema von Teil 4. Daneben geht es auch um das Aufstellen und Lösen von Rekursionsgleichungen. Teil 5 liefert eine Einführung in die Wahrscheinlichkeitstheorie mit Schwergewicht auf diskreten Wahrscheinlichkeitsräumen.

Besondere Lehrformen

Vorlesung in Fernlehre (eLearning): Interaktive Lernplattform, Übungsaufgaben im Selbststudium. 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

Erfolgreiches Bestehen der Modulabschlussklausur.

Verwendung des Moduls in anderen Studiengängen

nein

Stellenwert der Note für die Endnote

1/12

Modulbetreuer

Prof. Dr. Tanja Lange, Technische Universität Eindhoven

Literatur

Skript „Diskrete Mathematik für IT-Sicherheit“
Edward A. Bender & S. Gill Williamson (2004): A Short Course in Discrete Mathematics

Sonstige Informationen

Pflichtmodul:
Modul 3: Informatik für IT-Sicherheit

Workload	Studienphase	Turnus	Dauer	
10 CP (300 h)	1. Studienjahr	Jährlich zum Sommersemester	1 Semester	
Lehrveranstaltungen		**Kontaktzeit**	**Selbststudium**	**Gruppengröße**
Informatik für IT-Sicherheit		0 h	300 h	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

Erfolgreiches Bestehen der Modulabschlussklausur.

Verwendung des Moduls in anderen Studiengängen

nein

Stellenwert der Note für die Endnote

1/12

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

Nach erfolgreicher Absolvierung des Moduls haben die Studierenden Grundkenntnisse über die Hardware-Aspekte von Rechensystemen erworben. Sie verfügen über ein Verständnis von den Hardware-Grundlagen in digitalen Systemen – dies aber nicht nur beschränkt auf Computer – und der Funktionsweise moderner Rechner, und können dieses Verständnis zur Lösung von Problemen einsetzen. Ferner entwickeln sie ein Grundverständnis für die Beziehung zwischen Softwarefunktionen und Hardware-Realisierung. Sie können mit diesem Verständnis mit ihren Kollegen über Probleme der Computerhardware diskutieren und auftretende Probleme im Gespräch korrekt klassifizieren.

Inhalte

Das Modul behandelt im ersten Teil die Grundlagen der modernen Digitaltechnik und die Funktionsweise moderner Mikrorechner. Es beginnt mit einer kurzen Einführung in Zahlensysteme. Auf der Basis der Boole´schen Algebra werden Schaltnetze und speicherbehaftete Schaltwerke sowie Register und Speicherbausteine auf Gatterebene abstrahierend von der physikalisch / elektronischen Realisierung der Bauelemente betrachtet. Zusätzlich wird ein Überblick über moderne VLSI Technologien (Standardcell, full custom, FPGA) gegeben.

Im zweiten Teil werden Mikrorechnersysteme ausgehend von der von-Neumann-Struktur eingeführt und die Elemente wie Rechenwerk, Steuerwerk, Speicher mit Aufbau und Funktion sowie die Befehlsbearbeitung mit ihren Befehlssätzen und Adressierungsarten behandelt. Dabei werden auch die wichtigsten Komponenten wie Busse, Schnittstellen und Peripherie beschrieben. Ebenso werden die Speicherhierarchien mit Hauptspeicher, Cachestufen und Hintergrundspeicher sowie die virtuelle Speicherverwaltung behandelt. Es folgt eine Betrachtung weit verbreiteter Rechnerarchitekturen und Prozessortechniken. Das Pipelining-Prinzip wird erläutert und dabei das große Problem der Pipeline-Konflikte mit deren Lösungsmöglichkeiten behandelt. Aufbauend darauf folgt eine Einführung in die Superskalartechnik mit den speziellen Sprungbearbeitungstechniken. Den Abschluss bildet ein ausführlicheres Kapitel über den Aufbau und die Organisation des Arbeitsspeichers.

Besondere Lehrformen

Vorlesung in Fernlehre (eLearning): Interaktive Lernplattform, Skript, Begleitmaterial und Aufgabenbuch, 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

Erfolgreiches Bestehen der Modulabschlussklausur.

Verwendung des Moduls in anderen Studiengängen

nein

Stellenwert der Note für die Endnote

1/12

Modulbetreuer

PD Dr. Klaus Gotthardt (FernUniversität in Hagen)

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

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.

Inhalte

Wenn Kryptographie in einer technischen Umgebung wie einem Computer-, Daten- oder Telefonnetz eingesetzt wird, hängt die Sicherheit außer von rein kryptographischen Faktoren auch von der technischen Einbettung der Verschlüsselungs- und Signaturalgorithmen ab. Prominente Beispiele (für fehlerhafte Einbettungen) sind EFAIL (efail.de), Angriffe auf die WLAN-Verschlüsselungssysteme WEP und WPA (KRACK) und diverse Angriffe auf TLS (Bleichenbacher, POODLE, DROWN, ROBOT).

Das Modul „Netzsicherheit“ beschäftigt sich mit konkreten Netzen zur Datenübertragung und beleuchtet diese von allen Seiten auf ihre Sicherheit hin. Es umfasst folgende Teile:

- 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)
- IP Multicast
- 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 (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.

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
Erfolgreiches Bestehen der Modulabschlussklausur.
Verwendung des Moduls in anderen Studiengängen
nein
Stellenwert der Note für die Endnote
1/12
Modulbetreuer
Prof. Dr. Jörg Schwenk
Literatur
Schwenk, Jörg: Sicherheit und Kryptographie im Internet, Vieweg, 2014 Skript (ergänzende Folien) „Netzsicherheit“
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

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.

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.

Inhalte

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.

Besondere Lehrformen

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.

Prüfungsformen

Klausur (3 Stunden)

Voraussetzungen für die Vergabe von Kreditpunkten

Erfolgreiches Bestehen der Modulabschlussklausur.

Verwendung des Moduls in anderen Studiengängen

nein

Stellenwert der Note für die Endnote

1/12

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

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.

Inhalte

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:

In Teil 1 der Veranstaltung werden wesentliche Bereiche der symmetrischen Kryptographie behandelt. Dieser Teil beinhaltet insbesondere Block- und Strom-Algorithmen sowie Hashfunktionen. 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 vorgesellt, um das Verständnis zu vertiefen.

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.

Im abschließenden Teil 3 werden Generische Gruppen und Pairing-Based Cryptography vorgestellt. Hier stehen in Ergänzung zu Modul 4 die mathematischen Grundlagen im Vordergrund.

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

Erfolgreiches Bestehen der Modulabschlussklausur.

Verwendung des Moduls in anderen Studiengängen

nein

Stellenwert der Note für die Endnote

1/12

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

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.

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.

Inhalte

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.

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.

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

Erfolgreiches Bestehen der Modulabschlussklausur.

Verwendung des Moduls in anderen Studiengängen

nein

Stellenwert der Note für die Endnote

0,5/12

Modulbetreuer

Prof. Dr. Rainer Böhme, Universität Innsbruck

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	Gruppengröße
Rechtliche Aspekte der IT-Sicherheit		0 h	300 h	Max. 50

Teilnahmevoraussetzungen

keine

Lernergebnisse

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.

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, Protokollierung von Ereignissen -auch im Rahmen von IDS-, Generierung und Analyse von Logfiles, digitale Forensik, etc., zu bewerten und diese entsprechend den gesetzlichen Grundlagen zu handhaben. Die Studenten 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.

Inhalte

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.

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.

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

Erfolgreiches Bestehen der Modulabschlussklausur.

Verwendung des Moduls in anderen Studiengängen

nein

Stellenwert der Note für die Endnote

0,5/12

Modulbetreuer

Prof. Dr. Georg Borges, Universität des Saarlandes

Literatur

Skript „Rechtliche Aspekte der IT-Sicherheit“
Bürgerliches Gesetzbuch, 82. Auflage
Medienrecht, 14. Auflage
BDSG 2018

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; ständige Kommunikation mit dem Betreuer möglich

Prüfungsformen

Schriftliche Prüfungsarbeit

Voraussetzungen für die Vergabe von Kreditpunkten

Erfolgreiches Bestehen der schriftlichen Masterarbeit.

Verwendung des Moduls in anderen Studiengängen

nein

Stellenwert der Note für die Endnote

2,5/12

Modulbetreuer

Prof. Dr. Jörg Schwenk (Studiendekan)

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	Max. 15

Teilnahmevoraussetzungen

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 Systemsicherheit.
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

Schriftliche Hausarbeit (Umfang ca. 20 Seiten)

Voraussetzungen für die Vergabe von Kreditpunkten

Vortrag im Rahmen der Präsenzveranstaltung und erfolgreiches Bestehen der schriftlichen Ausarbeitung der Präsentation im Rahmen einer Hausarbeit.

Verwendung des Moduls in anderen Studiengängen

nein

Stellenwert der Note für die Endnote

0,5/12

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	Semesterweise	1 Semester	
Lehrveranstaltungen		**Kontaktzeit**	**Selbststudium**	**Gruppengröße**
Datenschutz in der betrieblichen Praxis		0 h	150 h	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 Datenschutzanforderungen: 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
Mündliches Prüfungsgespräch über die zuvor erarbeiteten Modulinhalte und Reading Assignments (Dauer ca. 20-30 Minuten)
Voraussetzungen für die Vergabe von Kreditpunkten
Erfolgreiches Bestehen des Prüfungsgespräches.
Verwendung des Moduls in anderen Studiengängen
nein
Stellenwert der Note für die Endnote
0,5/12
Modulbetreuer
Dr. Kai-Uwe Loser
Literatur
Skript „Datenschutz in der betrieblichen Praxis“
Sonstige Informationen

Wahlpflichtmodul:
Modul 9.3: Einführung in die Forensische Informatik

Workload	Studienphase	Turnus	Dauer	
5 CP (150 h)	2. Studienjahr	Jährlich zum Sommersemester	1 Semester	
Lehrveranstaltungen		**Kontaktzeit**	**Selbststudium**	**Gruppengröße**
Einführung in die Forensische Informatik		20 h	130 h	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 Computereinbruch 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

Erfolgreiches Bestehen des Prüfungsgespräches.

Verwendung des Moduls in anderen Studiengängen

nein

Stellenwert der Note für die Endnote

1/24

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	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:

- 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

Mündliches Prüfungsgespräch über die zuvor erarbeiteten Modulinhalte und Reading Assignments (Dauer ca. 20-30 Minuten)

Voraussetzungen für die Vergabe von Kreditpunkten

Erfolgreiches Bestehen des Prüfungsgespräches.

Verwendung des Moduls in anderen Studiengängen

nein

Stellenwert der Note für die Endnote

0,5/12

Modulbetreuer

Prof. Dr. Mark Manulis, University of Surrey

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**	**Gruppengröße**
Implementierung kryptographischer Verfahren		0 h	150 h	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

Klausur (2 Stunden)

Voraussetzungen für die Vergabe von Kreditpunkten

Erfolgreiches Bestehen der Modulabschlussklausur.

Verwendung des Moduls in anderen Studiengängen

nein

Stellenwert der Note für die Endnote

0,5/12

Modulbetreuer

Prof. Dr. Christof Paar

Literatur

Skript „Implementation of cryptographic schemes“

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	Max. 50

Teilnahmevoraussetzungen

keine

Lernergebnisse

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.

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.

Inhalte

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:

- 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

Ferner beschäftigt sich die Vorlesung mit finanziellen Aspekten des Security Managements wie der Kosten-Nutzen-Analyse von Security Lösungen, der Berechnung des Security-Investitionsvolumes und ROI in der Praxis.

Abschließend wird ein Überblick über Fortbildungsmöglichkeiten und Zertifizierungen gegeben.

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
Erfolgreiches Bestehen der schriftlichen Hausarbeit.
Verwendung des Moduls in anderen Studiengängen
nein
Stellenwert der Note für die Endnote
0,5/12
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	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

Erfolgreiches Bestehen der Modulabschlussklausur.

Verwendung des Moduls in anderen Studiengängen

nein

Stellenwert der Note für die Endnote

0,5/12

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**	**Gruppengröße**
Mobile Security		12 h	138 h	Max. 50

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

Flankiert durch ein kurzes Repetitorium der Grundlagen der IT-Sicherheit und Sicherheitstechnologien werden mit den Studierenden Sicherheits- und Datenschutzprobleme beim Einsatz typischer Mobiler Systeme und Anwendungen diskutiert wie:

- WLAN (IEEE 802.11i)
- WiMAX (IEEE 802.16)
- Bluetooth (IEEE 802.15)
- Near Field Communication (NFC)
- Smartphone-Betriebssysteme
- mobile Datenträger
- Mobilfunknetze (2G (GSM, GPRS), 3G (UMTS), 4G (LTE) und 5G)

Darüber hinaus werden Konzepte und Strategien für die Sicherheit und den Datenschutz behandelt und daraus Lösungen und Handlungsempfehlungen abgeleitet. Neben Allgemeingültigem wie Authentisierung, Mobile Security Policy, Endgeräte und Betriebssysteme werden spezifische Konzepte behandelt wie:

- Mobile Identity & Access Management (IAM)
- Bring Your Own Device (BYOD) und Corporate Owned, Personally Enabled (COPE)
- Mobile Device Management (MDM) und
- Schatten-IT

Besondere Lehrformen

Vorlesung in Fernlehre (eLearning) mit Skype-Konferenz. Interaktive Lernplattform, Skript und Folienausdrucke. Schriftliche Ausarbeitung (Essay) mit Feedback durch den Dozenten, der mit den Studierenden über ein Forum, E-Mail und Skype kommuniziert.

Prüfungsformen

Schriftliche Hausarbeit (Umfang ca. 20 Seiten)

Voraussetzungen für die Vergabe von Kreditpunkten

Erfolgreiches Bestehen der schriftlichen Hausarbeit.

Verwendung des Moduls in anderen Studiengängen

nein

Stellenwert der Note für die Endnote

0,5/12

Modulbetreuer

Prof. Dr.-Ing. Evren Eren, Hochschule Bremen

Literatur

Skript „Mobile Security“ sowie diverse thematische PowerPoint-Skripte (E. Eren)

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**	**Gruppengröße**
Virenschutz im Unternehmen		8 h	142 h	Max. 50

Teilnahmevoraussetzungen

keine

Lernergebnisse

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.

Inhalte

Das Modul befasst sich mit Angriffen, die von Malware (einschließlich Viren) ausgehen. Dabei werden die speziellen Anforderungen von Unternehmen und anderen Organisationen besonders berücksichtigt.

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 Virenscanner, Firewalls, Intrusion Detection/ Prevention Systeme und andere Schutztechnologien arbeiten, um vor Malware und ihren Folgen zu schützen.

In einem Überblick werden konkrete Schutzmaßnahmen für verschiedene Anwendungsszenarien vorgestellt.

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

Erfolgreiches Bestehen der Modulabschlussklausur.

Verwendung des Moduls in anderen Studiengängen

nein

Stellenwert der Note für die Endnote

0,5/12

Modulbetreuer

Ralf Benzmüller

Literatur

Skript „Virenschutz in Unternehmen“

Sonstige Informationen