Ordnung des Studiengangs IT Security Master of Science (M.Sc.)

Ausführungsbestimmungen
mit Anhängen
I: Studien- und Prüfungsplan
II: Kompetenzbeschreibungen
III: Modulhandbuch (*nur elektronisch veröffentlicht*)
vom 09.02.2023

Beschluss des Fachbereichsrats am 09.02.2023

In Kraft-Treten der Ordnung am 01.06.2024

TECHNISCHE UNIVERSITÄT DARMSTADT

Aufgrund der Genehmigung des Präsidiums der TU Darmstadt vom 27.07.2023 (Az.: 652-7-1) wird die Ordnung des Studiengangs M.Sc. IT Security (Fachbereich Informatik) vom 09.02.2023 zu den Allgemeinen Prüfungsbestimmungen der TU Darmstadt (APB) bekannt gemacht.

Darmstadt, 27.07.2023

gez.
Die Präsidentin der TU Darmstadt
Professorin Dr. Tanja Brühl

Inhaltsverzeichnis der Ordnung

Inhaltsverzeichnis der Ordnung		2
Präambel		3
Artikel 1		3
Ausführungsbestimmungen zu den APB		3
Artikel 2		6
Anhang I	Studien- und Prüfungsplan	6
Anhang II	Kompetenzbeschreibungen	8
Anhang III	Modulbeschreibungen	11
Artikel 3		12

Präambel

Der Fachbereichsrat des Fachbereichs Informatik hat am 09.02.2023 gem. § 3 Abs. 1 der Allgemeinen Prüfungsbestimmungen der TU Darmstadt (APB) die folgende Ordnung des Studiengangs IT Security Master of Science (M.Sc.) mit den Bestandteilen

1. Anhang I Studien- und Prüfungsplan
2. Anhang II Kompetenzbeschreibungen
3. Anhang III Modulbeschreibungen

beschlossen:

Artikel 1

Ausführungsbestimmungen zu den APB

zu § 2 (1): Akademische Grade

Der Studiengang IT Security (M.Sc.) wird vom Fachbereich Informatik der TU Darmstadt getragen. Die TU Darmstadt verleiht nach Erreichen der im Studiengang erforderlichen Summe von 120 Leistungspunkten (CP) den akademischen Grad Master of Science.

zu § 3 (4) – Zeitpunkte der Prüfungen

Für alle Prüfungen wird empfohlen, dass sie in der in Anhang I vorgegebenen Reihenfolge und in dem in Anhang I empfohlenen Fachsemester abgelegt werden.

zu § 5 (3), (4): Module, Bestandteile und Art der Prüfung

In Anhang I dieser Ausführungsbestimmungen, dem Studien- und Prüfungsplan, sind die Art (Fachprüfung, Studienleistung), der Umfang, die Anzahl und die Form oder die Kategorie der Prüfung sowie die Gewichtung mit der deren Bewertung in die Gesamtnote des Moduls einfließt, festgelegt.

Prüfungen, die in anderen Fachbereichen abgelegt werden, richten sich nach den Bestimmungen der anbietenden Fachbereiche der TU Darmstadt.

zu § 11 (5): Allgemeine Zulassungsvoraussetzungen – Unterrichtssprache

Unterrichtssprache des Studiengangs ist Englisch.
Einzelne Lehrveranstaltungen/Module können in deutscher Sprache angeboten werden. Hierauf wird in der Modulbeschreibung hingewiesen.
Es ist davon auszugehen, dass wissenschaftliche Literatur auch in Deutsch zu lesen und zu bearbeiten ist.

zu § 17a (1): Zugangsvoraussetzungen zu Masterstudiengängen

Im Folgenden werden die Zugangsvoraussetzungen für den Masterstudiengang IT Security und insbesondere die von den Bewerber*innen mitzubringenden Vorkenntnisse und Qualifikationen (Eingangskompetenzen) festgelegt.
Bewerbungen für den Masterstudiengang IT Security sind für Bewerber*innen für ein Wintersemester bis zum 15. Juli des Jahres (Ausschlussfrist) und bis zum 15. Januar des Jahres für ein Sommersemester (Ausschlussfrist) möglich.

zu § 17a (2): Eingangskompetenzen für einen konsekutiven Masterstudiengang

Die Eingangskompetenzen für den konsekutiven Masterstudiengang IT Security (M.Sc.) ergeben sich aus dem Kompetenzprofil des zum Masterstudiengang berechtigenden Bachelorstudiengangs Informatik der TU Darmstadt als Referenzstudiengang.

Zugangsvoraussetzung zum Masterstudiengang IT Security (M.Sc.) ist ein Bachelorabschluss Informatik (B.Sc.) der TU Darmstadt oder ein Studienabschluss in einem Studiengang, der Kompetenzen im Umfang von mindestens 180 CP vermittelt, von denen mindestens 60 CP nicht wesentlich verschieden zu den im Referenzstudiengang vermittelten Eingangskompetenzen sind (vergleichbarer Studiengang).

Einzelheiten zu den im Referenzstudiengang an der TU Darmstadt vermittelten Eingangskompetenzen sind in der Kompetenzbeschreibung in Anlage II geregelt.

zu § 17a (4) Lit. a) und b): Formelle Eingangsprüfung

Im Rahmen der formellen Eingangsprüfung wird der Nachweis der erforderlichen Eingangskompetenzen anhand der von den Bewerber*innen einzureichenden schriftlichen Unterlagen überprüft.
Eingereicht werden müssen das Zeugnis über den ersten Studienabschluss und das Diploma Supplement oder vergleichbare Unterlagen des zum ersten Studienabschluss führenden Studiengangs.

zu § 17a (4) Lit. c) (5): Materielle Eingangsprüfung

Konnten die Eingangskompetenzen nicht bereits im Rahmen der formellen Eingangsprüfung eindeutig positiv oder negativ geklärt werden, so wird anschließend eine materielle Eingangsprüfung durchgeführt.
Die Eingangsprüfung kann in diesem Bewerbungsverfahren nicht wiederholt werden.

Im Rahmen der materiellen Eingangsprüfung wird ein mündliches Prüfverfahren von 30 Minuten in den Räumlichkeiten der TU Darmstadt durchgeführt oder ein mündliches Prüfverfahren von 30 Minuten per datenschutzrechtlich unbedenklicher Videotelefonie durchgeführt.

Wenn im Rahmen der Bewerbungsfrist absehbar ist, dass mehr als 10 Bewerberinnen oder Bewerber eine materielle Eingangsprüfung ablegen müssen oder ein Videotelefonat nicht ordnungsgemäß durchgeführt werden kann, kann die Prüfungskommission beschließen, dass stattdessen die Eignung der Kandidatinnen und Kandidaten durch eine schriftliche Prüfung von 90 Minuten Dauer in den Räumlichkeiten der Technischen Universität Darmstadt oder durch ein schriftliches Prüfverfahren als Online-Test überprüft wird.

Die Prüfungskommission legt Form und Zeitpunkt der materiellen Eingangsprüfung fest und benennt Prüferinnen und Prüfer. Diese bestimmen den Inhalt der Prüfung mit dem Ziel, die Eignung der Studienbewerberin oder des Studienbewerbers für den Studiengang M.Sc. IT Security an der Technischen Universität Darmstadt festzustellen.

Die Prüfungskommission kann eine Bewerberin oder einen Bewerber von der materiellen Eingangsprüfung befreien, wenn aufgrund eines Zulassungs- und Eignungstests einer anderen Hochschule oder eines privaten Anbieters mit entsprechenden Standards (z.B. GRE oder vergleichbare Tests) zu erwarten ist, dass er bzw. sie das Masterstudium erfolgreich abschließen wird.

zu § 17a (8): Zulassung unter Auflagen

Stellt sich nach erfolgter Eingangsprüfung heraus, dass den Bewerber*innen Eingangskompetenzen fehlen, die durch das Nachholen von Leistungen im Umfang von nicht mehr als 30 CP ausgeglichen werden können, so kann eine Zulassung unter Auflagen gemacht werden. Welche Module oder Fachprüfungen zur Auflage gemacht werden und bis wann diese zu erbringen sind, wird im Zulassungsbescheid aufgeführt.
Für die Auflagen gelten die Allgemeinen Prüfungsbestimmungen der TU Darmstadt mit Ausnahme der zweiten Wiederholungsprüfung nach § 31 APB und der mündlichen Ergänzungsprüfung nach § 32 APB, d.h. pro Auflage sind nur zwei Versuche erlaubt.

zu § 18: Zulassungsvoraussetzungen

Die ggf. vorhandenen Zulassungsvoraussetzungen zu Prüfungen oder Modulen sind in Anhang I zu diesen Ausführungsbestimmungen, dem Studien- und Prüfungsplan, sowie in Anhang III, den Modulbeschreibungen, festgelegt.

zu § 22 (1): Durchführung der Prüfungen – Dauer der mündlichen Prüfung

Die Dauer der mündlichen Prüfung (mind. 15 min. pro Person und Prüfung) ist jeweils in Anhang I zu diesen Ausführungsbestimmungen, dem Studien- und Prüfungsplan, festgelegt.

zu § 22 (5): Durchführung der Prüfungen – Dauer der Aufsichtsarbeit

Die Dauer der Aufsichtsarbeit (mind. 45 min.) ist jeweils in Anhang I zu diesen Ausführungsbestimmungen, dem Studien- und Prüfungsplan, festgelegt.

zu § 22 (6): Durchführung der Prüfungen – besondere Prüfungsformen

Die Mindestdauer von Prüfungen der Kategorie Sonderform ist in Anhang I zu diesen Ausführungsbestimmungen, dem Studien- und Prüfungsplan, festgelegt.

zu § 23 (5): Abschlussarbeit – Bearbeitungszeit

Die Abschlussarbeit umfasst einen Arbeitsaufwand von 30 CP (900 Stunden) und muss innerhalb von 26 Wochen angefertigt und eingereicht werden.

zu § 25 (1), (3): Bildung und Gewichtung der Noten

Das Bewertungssystem jeder Prüfungsleistung ist in Anhang I zu diesen Ausführungsbestimmungen, dem Studien- und Prüfungsplan, festgelegt. Ebenso ist im Studien- und Prüfungsplan festgelegt, mit welchem Gewicht die Noten der Fachprüfungen und Studienleistungen in die Modulnote eingehen.

zu § 28 (2): Gesamtnote

In Anhang I dieser Ausführungsbestimmungen, dem Studien- und Prüfungsplan, ist festgelegt, mit welchem Gewicht die Modulnoten in die Gesamtnote eingehen. Soweit in Anhang I nicht anders festgelegt, gehen die Modulnoten entsprechend der in den Modulen erworbenen Leistungspunkte in die Gesamtnote ein.

Artikel 2

Anhänge

Anhang I Studien- und Prüfungsplan

Masterstudiengang
IT Security (M.Sc.)

TECHNISCHE UNIVERSITÄT DARMSTADT

Informatik

Studien- und Prüfungsplan (Anhang I)

Legende			Prüfungsleistungen						Kurs					Semester			
Bewertungs-system:	St= Standard (benotet); bnb= bestanden/nicht bestanden													Die Zuordnung der Prüfungen zu Semestern hat empfehlenden Charakter.			
Prüfungsform:	A= Abgabe, B=Bericht, E=Essay, H=Hausarbeit, HÜ= Hausübungen, Arbeitsblätter, K = Klausur, Kq= Kolloquium, M=Mündliche Prüfungsleistung mit Spezifizierung in der Modulbeschreibung, mP= mündliche Prüfungsleistung M/S=Mündliche/Schriftliche Prüfungsleistung mit Spezifizierung in der Modulbeschreibung, P= Protokoll, Pt= Präsentation, R=Referat, S=Schriftliche Prüfungsleistung mit Spezifizierung in der Modulbeschreibung, SF= Sonderform, Th=Thesis	Voraussetzung für Zulassung	Fachprüfung	Studienleistung	Prüfungsform	Dauer (min)	Gewichtung f. Modulnote	Gewichtung f. Gesamtnote	Semesterwochenstunden (SWS)	Status	Lehrform	Anwesenheitspflicht	CP gesamt				
Status:	o= obligatorisch; f= fakultativ																
Art der Lehrform:	VL=Vorlesung; S=Seminar; Ü=Übung; …													Arbeitsaufwand pro Semester (CP)			
CP:	Leistungspunkte																
A Wahlbereiche und Studium Generale													**90**	**30**	**30**	**30**	
A 1. Wahlbereiche Offene Kataloge										**o**			**84-85**	84-85			
A 1.1. Fachprüfungen aus den Wahlbereichen des M.Sc. IT Security und dem Wahlbereich Complementary Topics (Typ § 30 Abs. 5 APB) Prüfungsform und -dauer nach Vorgabe des anbietenden Fachbereichs.										**o**			**69-76**	69-76			
A 1.1.1. Wahlbereichen des M.Sc. IT Security (Typ § 30 Abs. 5 APB)										**o**			**51-70**	51-70			
Cryptography and Foundations (Typ § 30 Abs. 5 APB)										**o**							
Cryptography and Foundations (Typ § 30 Abs. 5 APB)							1			**o**			**12-46**	12-46			
Systems and Communication Security (Typ § 30 Abs. 5 APB)										**o**							
Systems and Communication Security (Typ § 30 Abs. 5 APB)							1			**o**			**12-46**	12-46			
Software and Application Security (Typ § 30 Abs. 5 APB)										**o**							
Software and Application Security (Typ § 30 Abs. 5 APB)							1			**o**			**12-46**	12-46			
A 1.1.2 Wahlbereich Complementary Topics (Typ § 30 Abs. 5 APB)										**o**			**6-18**	6-18			
Complementary Topics (Typ § 30 Abs. 5 APB)							1			**o**			**6-18**	6-18			
A 1.2. Studienbegleitende Leistungen (Typ § 30 Abs. 6 APB) Auswahl von Lehrveranstaltungen aus dem Katalog des M.Sc. IT Security der Seminare (min. 1), dem Katalog des M.Sc. IT Security der Praktika in der Lehre (max. 1) und dem Katalog des M.Sc. IT Security der Praktika, Projektpraktika und ähnlicher Veranstaltungen (min. 1). Prüfungsform und -dauer nach Vorgabe des anbietenden Fachbereichs.										**o**			**9-15**	9-15			
Seminare (min. 1)							1			o			3-9	3-9			
Praktikum in der Lehre (max. 1)							1			f			0-5	0-5			
Praktika, Projektpraktika und ähnliche Veranstaltungen (min. 1)							1			o			6-12	6-12			
Studienarbeit							1			**f**			0-6	0-6			
A 2. Studium Generale Veranstaltungen aus den Gesamtkatalogen der TU Darmstadt außer Fachbereich Informatik (ggf. können weitere Kataloge ergänzt werden). Prüfungsform und -dauer nach Vorgabe des anbietenden Fachbereichs. min. 5 CP - max. 6 CP (Typ § 30 Abs. 6 APB)										o			**5-6**	5-6			
Wahlbereich Sprachen										f			**0-6**				
Gesamtkatalog des Sprachenzentrums							1			f				0-6			
Wahlbereich Mensch, Gesellschaft, Wirtschaft										f			**0-6**				
Gesamtkataloge der Fachbereiche 01, 02, und 03							1			f				0-6			
Wahlbereich Umwelt, Technik, Naturwissenschaft										f			**0-6**				
Gesamtkataloge der Fachbereiche 04, 05, 07, 10, 11, 13, 15, 16, 18							1			f				0-6			
B Masterarbeit													**30**				
20-AM-5415	Masterarbeit IT Security		St		Th			1		o							30
								Summe					**120**	30	30	30	30

v4.0 Stand: 24.04.2022 (JB)

Anhang II Kompetenzbeschreibungen

Eingangsvoraussetzungen für den M.Sc. IT Security:

Die im Folgenden beschriebenen Eingangskompetenzen sind wesentlich für die erfolgreiche Absolvierung des M.Sc. IT Security. Es ist eine Auswahl der wichtigsten Kompetenzen, die im Referenzstudiengang an der TU Darmstadt vermittelt werden. Diese liefern damit auch die wesentlichen Voraussetzungen für die erfolgreiche Fortsetzung des Studiums in einem darauf aufbauenden Masterstudiengang.

Innerhalb der im Umfang von mindestens 180 CP nachzuweisenden Kompetenzen aus ihrem vorherigen Studienabschluss müssen die Bewerber*innen auf den M.Sc. IT Security für eine Zulassung Eingangskompetenzen im Umfang von insgesamt mindestens 60 CP aus dem Referenzstudiengang oder äquivalente Kompetenzen nachweisen.

Im Folgenden werden die Eingangskompetenzen für den M.Sc. IT Security beschrieben:

- **Theoretische Informatik**: die Fähigkeit, mathematische Notationen und Methoden zur Fundierung von Konzepten der Informatik einzusetzen, insbesondere zur formalen Modellierung und Verifikation von Soft- und Hardwaresystemen. Veranstaltungen, in denen diese Eingangskompetenzen im Referenzstudiengang an der TU Darmstadt vermittelt werden, sind Aussagen- und Prädikatenlogik; Automaten, formale Sprachen und Entscheidbarkeit; Modellierung, Spezifikation und Semantik.

- **Praktische Informatik:** die Fähigkeit,
    - selbstständig aus einer Problembeschreibung die zur Lösung erforderlichen Standardalgorithmen und Datenstrukturen entsprechend den funktionalen und nicht-funktionalen Anforderungen auszuwählen bzw. unter Zugrundelegung von bekannten Strategien neue Algorithmen und Datenstrukturen zur Problemlösung zu konstruieren und einzuschätzen, ggf. unter Berücksichtigung von Parallelität.

    - die einzelnen Bestandteile einer Programmiersprache selbstständig und ohne analoges Beispiel im Rahmen einer Programmieraufgabe zu einer Gesamtlösung zusammenzuführen.

    - Programmieraufgaben in unterschiedlichen, auch parallelen, Programmiersprachen zu lösen, die verschiedenen Paradigmen folgen, unterschiedliche Anwendungsbereiche haben und auf der ganzen Bandbreite an Abstraktionsebenen angesiedelt sind.

    - die Qualität der erstellten Implementierungen durch formalisierte Testverfahren und Entwurfsmethoden sicherzustellen.

    - diese Kenntnisse in praktisch relevanten Bereichen der Informatik wie Netzwerken und verteilten Systemen, Datenbanken, sowie der Erstellung von Programmierwerkzeugen selbst anzuwenden. Dabei sollen jeweils auch nicht-funktionale Aspekte, insbesondere auch die Sicherheit der erstellten IT-Systeme, berücksichtigt werden.

Diese Eingangskompetenzen in praktisch relevanten Bereichen der Informatik werden im Referenzstudiengang an der TU Darmstadt in folgenden Veranstaltungen vermittelt: Algorithmen und Datenstrukturen; Betriebssysteme; Computersystemsicherheit; Computernetze und verteilte Systeme; Einführung in den Compilerbau; Einführung in die Künstliche Intelligenz; Funktionale und objektorientierte Programmierkonzepte; Formale Methoden im Softwareentwurf; Informationsmanagement; Parallele Programmierung; Probabilistische Methoden der Informatik; Scientific Computing; Software Engineering; Visual Computing

- **Technische Informatik**: die Fähigkeit,
  - die einzelnen Entwurfsprinzipien und Grundelemente von digitalen Schaltungen, wie sie in den Vorlesungen nacheinander separat eingeführt werden, selbstständig und ohne analoges Beispiel im Rahmen einer Hardware-Entwurfsaufgabe zu einer Gesamtlösung zusammenzuführen.
  - Entwurfsaufgaben auf unterschiedlichen Abstraktionsebenen und aus unterschiedlichen Anwendungsbereichen durch strukturierte Entwurfsmethoden in verschiedenen Beschreibungssprachen und unter Einsatz eines Spektrums von Entwurfswerkzeugen zu lösen und bezüglich geeigneter Gütemaße zu evaluieren.
  - die Interaktion von Computer-, Prozessor- und Mikroarchitekturen zu verstehen und daraus für die System- und Anwendungssoftwareebene passende Implementierungsentscheidungen zu treffen.

  Veranstaltungen, in denen diese Eingangskompetenzen im Referenzstudiengang an der TU Darmstadt vermittelt werden, sind Digitaltechnik und Rechnerorganisation.

- **IT-Sicherheit:** die Fähigkeit,
  - selbstständig zu erkennen, dass als Teil eines IT-Systems Sicherheitslösungen notwendig sind und diese unterschiedlichen Komponenten wie Hardware, Software, Netzwerk, Systemebene und Nutzerschnittstelle betreffen. Hierzu zählen insbesondere auch das Identifizieren und das Verständnis von eventuellen Schwachstellen eines IT-Systems.

  - einzelnen Entwurfsprinzipien und grundlegende Methoden aus der IT-Sicherheit anzuwenden, selbstständig und ohne analoges Beispiel zum Schutz eines IT-Systems anzuwenden.

  - die Qualität der IT-Sicherheitslösung auf Korrektheit und Sicherheit hin auf verschiedenen Abstraktionsebenen (Algorithmus, Software, Hardware, etc.) zu evaluieren.

  Diese Eingangskompetenzen werden im Referenzstudiengang an der TU Darmstadt in den Veranstaltungen: Computersystemsicherheit; Algorithmen und Datenstrukturen; Probabilistische Methoden der Informatik vermittelt.

Ausgangskompetenzen

In dem forschungsorientierten Master of Science IT Security entwickeln die Studierenden ihre fachlichen und fachübergreifenden Kompetenzen zum Thema der IT-Sicherheit aufbauend auf dem Vorwissen aus einem vorangegangenen (Informatik-)Bachelor-Studiengang. Diese Kompetenzen sind charakteristisch für den Anspruch des Studiengangs und wesentliche Voraussetzung für eine anschließende Promotion in der IT-Sicherheit. Nach Abschluss des Studienganges sind die Absolvent*innen in der Lage,

- mit ihrer verbesserten Methodenkompetenz komplexe Probleme und Aufgabenstellungen aus der IT-Sicherheit mit wissenschaftlichen Methoden unter Abwägung verschiedener Sicherheitslösungen und Angriffsszenarien selbständig zu analysieren und zu bearbeiten,

- diese Kompetenzen im Bereich der IT-Sicherheit auch in neuen und unvertrauten Situationen bei unvollständiger Information umzusetzen und dabei in Systemzusammenhängen zu denken,
- Aufgaben und Probleme mit hohem Abstraktionsvermögen und Blick für komplexe Zusammenhänge zu lösen,
- zukünftige IT-Sicherheitsprobleme, IT-Sicherheitstechnologien und wissenschaftliche Entwicklungen im Themenfeld der IT-Sicherheit zu erkennen und bei ihrer Tätigkeit angemessen zu berücksichtigen,
- die Ergebnisse ihrer Analysen bzw. die ausgearbeiteten Lösungen auch an fremdsprachliche Fachleute und Laien zu kommunizieren,
- komplexe Projekte im Bereich der IT-Sicherheit effizient zu organisieren und durchzuführen sowie Teams zielgerichtet zu bilden und zu leiten,
- die gesellschaftliche und ethische Verantwortung ihrer Tätigkeit einzuschätzen und angemessen zu berücksichtigen,
- sich eigenständig fachlich weiterzubilden und weitgehend selbständig wissenschaftlich zu arbeiten.

Zusammenfassend entwickelt der Master-Studiengang IT Security bei Studierenden vor allem die Kompetenz, komplexe Problemstellungen im Bereich der IT-Sicherheit zu erkennen und diese bei unvollständiger Information zu lösen. Dazu werden Fertigkeiten aus der theoretischen und praktischen IT-Sicherheit vermittelt, die von den Studierenden passend auf die jeweilige Problemstellung anwendetet und weiterentwickelt werden können. Hinzu kommt verstärkt die Fertigkeit, sich mit der aktuellen Forschungsliteratur auseinandersetzen zu können sowie die Befähigung zum wissenschaftlichen Arbeiten in einer selbst gewählten Vertiefung und zur selbstständigen Lösung aktueller Probleme in der Praxis.

Anhang III Modulbeschreibungen

Die Modulbeschreibungen werden als Modulhandbuch gemäß § 1 Abs. (1) der *Satzung der Technischen Universität Darmstadt zur Regelung der Bekanntmachung von Satzungen der Technischen Universität Darmstadt* vom 18. März 2010 elektronisch veröffentlicht.

Artikel 3

In-Kraft-Treten

Diese Ordnung des Studiengangs tritt am 01.06.2024 in Kraft. Sie wird in der Satzungsbeilage der TU Darmstadt veröffentlicht.

Darmstadt, 01.08.2023

gez. Prof. Dr. Dr. Christian Reuter

Der Dekan des Fachbereichs Informatik
der TU Darmstadt