

Ausführungsbestimmungen des Master of Science Studienganges IT Security vom 01.08.2010 zu den Allgemeinen Prüfungsbestimmungen der Technischen Universität Darmstadt (APB)

Zu § 2

Die Technische Universität Darmstadt verleiht nach bestandener Abschlussprüfung des Master of Science Studienganges IT Security den akademischen Grad „Master of Science“ (M.Sc.).

Zu § 3 Abs. 4

Es wird empfohlen, Prüfungen unmittelbar im Anschluss an die Belegung des zugehörigen Moduls abzulegen.

Zu § 5 Abs. 2:

Alle Modulprüfungen der Masterprüfung finden studienbegleitend statt.

Zu § 5 Abs. 3

Die Masterprüfung wird gemäß Studien- und Prüfungsplan (Anhang I) in Modulen abgelegt. Die Masterprüfung setzt sich zusammen aus den Modulprüfungen des Wahlpflichtbereiches einschließlich der Abschlussarbeit (Master-Thesis).

Zu § 5 Abs. 4

Die Modulprüfungen werden entsprechend den Angaben im Studien- und Prüfungsplan (Anhang I) schriftlich und/oder mündlich durchgeführt.

Zu § 5 Abs. 5

Die Prüfungen können schriftlich und/oder mündlich durchgeführt werden. Soweit im Studien- und Prüfungsplan (Anhang I) nicht festgelegt, geben die Prüfenden die Prüfungsform spätestens bis zum Melde-termin bekannt.

Zu § 5 Abs. 7

Die Prüfungsanforderungen in den einzelnen Modulen sind im Modulhandbuch für den Masterstudiengang IT Security beschrieben und begrenzt. Änderungen sind durch Beschluss des Fachbereichsrates zulässig und werden semesterweise bekannt gegeben.

Zu § 5 Abs. 8

Die Anzahl der zu erwerbenden Kreditpunkte pro Pflichtmodul und pro Wahlpflichtbereich sind im Studien- und Prüfungsplan (Anhang I) festgelegt.

Zu § 17a Abs. 1.

(1) Zugangsvoraussetzung zum M.Sc. – Studiengang ist ein B.Sc. in der Fachrichtung Informatik an der TU Darmstadt oder vergleichbare Studiengänge. Fehlt diese Voraussetzung, ist eine bestandene Eingangsprüfung Zulassungsvoraussetzung.

(2) Der Fachbereichsrat legt Mindestgrenzen für Grundlagen Vorlesungen und Vorlesungen der Kerninformatik fest. Der Vorsitzende der Prüfungskommission nimmt im Rahmen der Prüfung der Bewerbung eine Gesamtwürdigung des Einzelfalls vor und entscheidet gegebenenfalls im Falle des Abs. 1 Satz 2 über Art und Umfang einer Eingangsprüfung. Näheres ist in Anlage II bestimmt.

(3) Die zuständige Prüfungskommission bestimmt den Zeitpunkt der Eingangsprüfung und benennt die oder den Prüfer. Die Eingangsprüfung wird als mündliche Prüfung durchgeführt.

(4) Die Prüfer entscheiden, ob der Prüfling die notwendigen Kenntnisse für das M.Sc. – Studium mitbringt. Die Entscheidung kann mit Auflagen verbunden werden, die den Prüfling in die Lage versetzen sollen, eventuell fehlende Kenntnisse aus dem B.Sc. – Studium in einer bestimmten Zeit während des Studiums an der Technischen Universität Darmstadt nachzuholen.

(5) Werden die Auflagen nicht erfüllt, ist die mit ihr verbundene Entscheidung zu widerrufen.

Zu § 20 Abs. 1

Zum Erwerb des Master of Science im Studiengang IT Security sind benotete Prüfungen und benotete Studienleistungen in den im Studien- und Prüfungsplan (Anhang I) aufgeführten Modulen des Wahlpflichtbereiches abzulegen und 120 Kreditpunkte zu erwerben.

Zu § 22 Abs. 2

Die Dauer der mündlichen Modulprüfungen ist im Studien- und Prüfungsplan (Anhang I) festgelegt.

Anhang I: Studien- und Prüfungsplan

Anhang II: Kriterien nach § 17a Abs. 1

Zu § 22 Abs. 5

Die Dauer der schriftlichen Modulprüfungen ist im Studien- und Prüfungsplan (Anhang I) festgelegt.

Zu § 23 Abs. 5

Die Abschlussarbeit (Master-Thesis) ist innerhalb einer Frist von 6 Monaten (900 Stunden) anzufertigen.

Die Abschlussarbeit wird mit einem Kolloquium abgeschlossen.

Zu § 31 Abs. 1

Bei schriftlichen Prüfungen kann die zweite Wiederholungsprüfung im Einvernehmen von Prüfenden und Prüflingen auch mündlich erfolgen.

Zu § 32 Abs. 1

Unter den Voraussetzungen des § 68 Absatz 3 Hessisches Hochschulgesetz in der Fassung der Bekanntmachung vom 31. Juli 2000 (GVBl. I, S.374) kann eine Befristung der Prüfung durch die zuständige Prüfungskommission ausgesprochen werden.

Zu § 35 Abs. 1

Im Zeugnis der bestandenen Masterprüfung werden neben den Prüfungen mit Angaben der Modulnoten die jeweils erworbenen Kreditpunkte aufgeführt.

Darmstadt, den

Der Dekan des Fachbereiches Informatik
der Technischen Universität Darmstadt
Prof. Dr. Karsten Weihe

Anhang I: Studien- und Prüfungsplan

Master of Science Studiengang IT Security											
CP = Kreditpunkte											
Prüfungsart: s = schriftlich; m = mündlich											
f = fakultativ (Bekanntgabe der Prüfungsform bis zum Meldetermin, wobei schriftlich 60-120 Min. und mündlich i.d.R. 30 Min.)											
Studienleistungen: b = benotet; u = unbenotet											
						Empfohlenes Semester		Studienleistung	Prüfungsart		
						1.WS	2.SS			3.WS	4.SS
						CP	CP	CP	CP		
Pflichtbereich											
Introduction to Cryptography						6					f
Embedded System Security						6					f
Introduction to IT Security						6					f
Wahlpflichtbereich A: Cryptography											
Prüfungsleistungen in Vorlesungen und Übungen oder integrierten Lehrveranstaltungen						mindestens 6					f
Wahlpflichtbereich B: System Security											
Prüfungsleistungen in Vorlesungen und Übungen oder integrierten Lehrveranstaltungen						mindestens 6					f
Wahlpflichtbereich C: Software Security											
Prüfungsleistungen in Vorlesungen und Übungen oder integrierten Lehrveranstaltungen						mindestens 6					f
Wahlpflichtbereich D: Selected Complementary Topics											
Prüfungsleistungen in Vorlesungen und Übungen oder integrierten Lehrveranstaltungen						mindestens 6					f
Wahlpflichtbereich E: Studienbegleitende Leistungen											
Studienleistungen in Seminaren, Praktika, Projektpraktika, Praktika in der Lehre, Projekten oder Studienarbeiten. Dabei müssen mindestens zwei der Formen Seminar, Praktikum, Projektpraktikum, Projekt oder Studienarbeit vertreten sein, es sei denn es wird ein Projekt mit mindestens 12 CP gewählt.						12 – 15				b	
Master-Thesis									30		
Summe (120)											

Sollte eines der Pflichtfächer bereits im Bachelorstudiengang absolviert worden sein, können die entsprechenden CP stattdessen in den Wahlpflichtbereichen erbracht werden.

Die Wahlpflichtbereiche sind auf den Web-Seiten des Fachbereichs Informatik beschrieben. Sie werden semesterweise aktualisiert.

Die Lehrveranstaltungen aus den Pflicht- und Wahlpflichtbereichen sind im Modulhandbuch für den Master of Science Studiengang IT Security im Einzelnen beschrieben.

Anhang II: Kriterien nach § 17a Abs. 1

1. Für die Master of Science Studiengänge des Fachbereichs Informatik der TU Darmstadt erforderliche Kompetenzen

Die folgenden sind nicht die einzigen Kompetenzen, die im Bachelor of Science Studiengang Informatik der TU Darmstadt erworben werden, aber charakteristisch für den Anspruch des Studiengangs und auch wesentliche Voraussetzungen für die Fortsetzung des Studiums in einem der darauf aufbauenden Masterstudiengänge. Jeder Absolvent dieses Studiengangs hat – neben dem Erwerb anderer Kompetenzen – folgende Erfahrungen gesammelt:

1. Absolventen sind intensiv und umfassend geübt in der weitgehend selbstständigen Bearbeitung von Aufgabenstellungen auf allen Inhalten der Pflichtveranstaltungen des Studiengangs. Dabei bedeutet
 - *intensiv und umfassend*, dass diese Erfahrungen nicht nur punktuell gesammelt werden (etwa in eigens dafür eingerichteten Lehrveranstaltungen), sondern dass sich dies durch das gesamte Studium hindurch zieht, wenn auch nicht unbedingt in jeder Lehrveranstaltung in gleichem Maße.
 - *selbstständig*, dass die Beratungsangebote im Wesentlichen der Aufgabenklärung und ersten Einhilfe dienen, aber darüber hinaus müssen die Studierenden die Aufgabe – je nach Vorgabe – einzeln oder im Team selbstständig bearbeiten.

Die Aufgabenstellungen sind in der Regel Transferaufgaben und erfordern Kreativität und Abstraktion bei der Lösung. Das Niveau lässt sich wie folgt genauer beschreiben:

- *Mathematik*: die Fähigkeit, typische Beweise aus einem beweisorientierten Mathematikstudium zu verstehen und in zur Vorlesung analogen elementaren Fällen auch selbst korrekt zu führen.
- *Theoretische Informatik*: die Fähigkeit, mathematische Notationen und Methoden zur Fundierung von Konzepten der Informatik einzusetzen insbesondere zur formalen Modellierung und Verifikation von Softwaresystemen.
- *Praktische Informatik*: die Fähigkeit,
 - die einzelnen Bestandteile einer Sprache, wie sie in einer Vorlesung nacheinander separat eingeführt werden, selbstständig und ohne analoges Beispiel im Rahmen einer Programmieraufgabe zu einer Gesamtlösung zusammenzuführen.
 - Programmieraufgaben in verschiedenen Sprachen zu lösen, die verschiedenen Paradigmen folgen, unterschiedliche Anwendungsbereiche haben und auf der ganzen Bandbreite an Abstraktionsebenen angesiedelt sind.

- *Technische Informatik*: die Fähigkeit,
 - die einzelnen Entwurfsprinzipien, wie sie in einer Vorlesung 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 verschiedener Entwurfswerkzeuge zu lösen.
 - Entwurfswerkzeuge in kleinerem Rahmen selbstständig zu entwickeln.
- 2. Absolventen sind durch die Organisation des Studiums geübt in der selbstständigen Arbeitsorganisation unter engen Rahmenbedingungen auf verschiedenen Zeitskalen (bis hin zu einem Umfang von mehreren Semestern).

2. Kriterien der Eingangsprüfung zum Master of Science Studiengang IT Security

Alle oben beschriebenen Erfahrungen sind wesentlich für die erfolgreiche Absolvierung der Master of Science Studiengänge *Autonome Systeme, Distributed Software Systems, Human Computer Systems, Informatik, Internet- und Web-basierte Systeme, IT Security* und *Visual Computing*. Insbesondere wesentlich ist, dass diese Erfahrungen im Zusammenhang mit den Inhalten der Grundlagenveranstaltungen gesammelt werden und derjenigen kanonischen Einführungen, auf denen der gewählte Masterstudiengang beruht.

Im Folgenden werden die Anforderungen detailliert definiert, die uneingeschränkt notwendig sind, um den Master of Science Studiengang *IT Security* erfolgreich zu absolvieren:

1. Es müssen die oben definierten Erfahrungen für Lehrveranstaltungen im Bereich Kerninformatik im Gesamtumfang von mindestens 60 CP nachgewiesen sein. Die Inhalte der Lehrveranstaltungen *Grundlagen der Informatik I-III* müssen im Wesentlichen abgedeckt sein. Im Bereich Theoretische Informatik müssen diese Erfahrungen für Lehrveranstaltungen im Umfang von mindestens 5 CP nachgewiesen werden.
2. Kanonische Einführungen¹, deren Inhalte im Wesentlichen abgedeckt sein müssen sind:

Einführung in CMS, Einführung in NCS und Einführung in TS.

¹ Kanonische Gebiete/ Einführungen: CE = Computational Engineering, CMS = Computer Microsystems, DKE = Data and Knowledge Engineering, FoC = Foundations of Computing, HCS = Human-Computer Systems, NCS = Net-Centric Systems, SE = Software Engineering, TS = Trusted Systems.

3. Unter der Voraussetzung aus Punkt 1 gilt: Sollte das Bachelorstudium des Bewerbers generell Erfahrungen in der oben beschriebenen Form vermitteln, aber nicht alle für den Master of Science Studiengang *IT Security* wesentlichen kanonischen Einführungen inhaltlich abdecken, kann eine günstige Erfolgsprognose nur dann gestellt und damit zur Sicherung des Studienerfolgs die Zulassung in der Regel nur erteilt werden, wenn sowohl die Abschlussnote als auch der mit CPs gewichtete Durchschnitt der Einzelnoten von Vorlesungen/Übungen und vergleichbaren Lehrveranstaltungsformen im Kernbereich Informatik nicht schlechter als 3,0 ist und jede Einzelnote in diesem Bereich besser als 4,0 ist. In diesem Fall wird die erfolgreiche Absolvierung der Prüfungen in diesen kanonischen Einführungen im ersten Studienjahr zur Auflage für die endgültige Zulassung.
4. Bei einem Bachelorstudium, das die oben definierten Anforderungen an die Art der Aufgabenstellung und an die Selbstständigkeit der Bearbeitung nicht erfüllt, kann bei überdurchschnittlichen Prüfungsergebnissen im Bereich Kerninformatik davon ausgegangen werden, dass dieser Mangel durch die persönlichen Fähigkeiten des Bewerbers ausgeglichen werden kann. In diesem Fall kann eine günstige Erfolgsprognose nur dann gestellt und damit die Zulassung nur dann erteilt werden, wenn sowohl die Abschlussnote als auch der mit CPs gewichtete Durchschnitt der Einzelnoten von Vorlesungen/Übungen und vergleichbaren Lehrveranstaltungsformen im Kernbereich Informatik „gut“ (2,0) oder besser ist und zudem keine Einzelnote im Kernbereich Informatik schlechter als „befriedigend“ (3,0) ist. Für die Auflagen gelten die Regeln von Punkt 3 entsprechend.

Anderweitig gesammelte Erfahrungen (bspw. aus beruflicher Tätigkeit oder aus Weiterbildungskursen) werden in der Eignungsfeststellung für den Master of Science Studiengang *IT Security* in vollem Umfang berücksichtigt, sofern sie den oben beschriebenen Erfahrungen sowohl vom Inhalt als auch vom Anspruch an Aufgabenstellung und selbstständige Bearbeitung her entsprechen und wenn diese Kompetenzen unter den allgemein üblichen Qualitätssicherungsstandards von Hochschulen erworben und bewertet worden sind.