Study Regulations Governing the Master's Degree Programme 'Cybersecurity' at Saarland University

25 February 2021

Note: This translation is provided for information purposes only. In the event of any discrepancy between the translation and the original German version published in the Official Bulletin (*Dienstblatt der Hochschulen des Saarlandes*), the provisions of the latter shall take precedence.

Pursuant to Section 60 of the Saarland Higher Education Institutions Act (SHSG) (Official Gazette of Saarland I, p. 1080) most recently amended in law by the Act of 8–9 December 2020 (Official Gazette I (2021), p. 53) and on the basis of the Joint Examination Regulations for Bachelor's and Master's Degree Programmes of the Faculty of Mathematics and Computer Science of 25 February 2021 (Official Bulletin No. 62, p. 580) and with the consent of the Saarland University Senate, the Faculty of Mathematics and Computer Science at Saarland University hereby issues the following Study Regulations Governing the Master's Degree Programme 'Cybersecurity'.

Section 1
Scope

These study regulations, which govern the content and structure of the Master's degree programme 'Cybersecurity', are based on the Joint Examination Regulations for the Bachelor's and Master's Degree Programmes of the Faculty of Mathematics and Computer Science of 25 February 2021 (Official Bulletin No. 62, p. 580) and on the Subject-Specific Regulations for the Master's Degree Programme 'Cybersecurity' of 25 February 2021 (Official Bulletin No. 67, p. 638). The Faculty of Mathematics and Computer Science is responsible for organizing the teaching, study curriculum and examinations associated with this programme.

Section 2
Objectives of the degree programme and career relevance

The objective of this Master's degree programme is to prepare graduates to undertake challenging national and international research and development work in the field of cybersecurity. The Master's programme 'Cybersecurity' aims to offer students a broad range of different but complementary options that enable them to deepen their knowledge and understanding of cybersecurity. Students can pursue in depth study in areas such as cryptography, privacy, software security, secure systems and networks, formal methods or legal aspects of cybersecurity, while also acquiring an understanding of related topics in computer science. Graduates are well suited to pursue further research in the field of cybersecurity, but also have a solid understanding of the discipline so that they can take up positions as cybersecurity professionals in either the private or public sectors.

Section 3
Start and duration of programme

(1) Students can begin the programme at the beginning of the winter or summer semester of each year.

(2) The curriculum is organized such that the programme can be completed in four semesters (standard period of study).

Section 4
Types of academic instruction

The curriculum content is taught using the following types of academic instruction:

1. Lectures ('L', standard class size = 100): Lectures serve to introduce a particular subject area and also provide an overview of the relevant theoretical concepts and principles, methodologies and skills, technologies and practical implementations that are common to the subject. Lecture courses provide suggestions for further reading on a topic and open the way to acquiring a deeper understanding of an area through subsequent exercise and problem-solving classes, practical skills classes and self-directed study.

2. Exercise and problem-solving classes ('EP', standard class size = 20): Exercise and problem-solving classes are small-group sessions used primarily to supplement and reinforce what was learned in the lectures. Students work on representative problems as this provides an opportunity for them to apply and deepen the knowledge they acquired in the lectures, to assess their personal understanding of a specific area and to clarify any questions that they may have.

3. Seminars ('S', standard class size = 15): Seminars provide an opportunity for students to broaden the knowledge and skills that they have already acquired and to gain a deeper understanding of a particular field of research by participating in discussions, giving presentations or completing seminar assignments based on their study of the specialist literature and relevant academic sources. They also help students acquire the skills necessary for the effective oral and visual presentation of scientific and academic content and encourage students to engage in critical analysis and discussion of research results. A seminar may also include project-related work in areas of current scientific interest or debate. The deeper understanding of a particular field that students acquire through project-related work in the Master's seminar may provide the basis for their final-year Master's thesis.

4. Practical skills classes and project work ('P', standard class size = 15; Master's thesis project, standard class size = 6): Practical skills classes or projects offer a number of practical, subject-related topics that introduce students to the specific approaches and methods used in a particular discipline or field of study. The necessary theoretical knowledge underlying a specific topic is acquired by attending lectures and studying the relevant scientific literature. An additional goal of the practical skills classes is to provide students with the opportunity to gain practical experience with computer-aided methods. Projects tend to address interdisciplinary topics. Working on a topic offers students the opportunity to work in supervised groups to tackle specific assignments from the initial solution design concept through to its final practical implementation. Students learn about the relationships between theory and practice not only through their own independent study and research, but also through project-based teamwork. Participation in a particular practical skills class or project may be dependent on a student having first successfully completed a required course of lectures and exercise and problem-solving classes.

Section 5
Structure and content of the programme

(1) To graduate from the Master's programme 'Cybersecurity', students shall earn a total of 120 credits (often referred to in Germany as 'credit points' or 'CPs') as defined by the European Credit Transfer System (ECTS). Of these, at least 106 credits and at most 110 credits shall be from graded assignments. As a rule, students are required to earn 30 credits per semester.

(2) The degree programme includes modules from the following module categories. Appendix A provides details of the modules and module elements offered in the different sections of the

programme, the type of academic instruction used, the number of credit hours per week and the ECTS credits earned, the module frequency, the type of academic assessment and whether the module is graded.

1. 27 graded credits from core lecture courses (each worth 9 CP). In this section, students must successfully complete the two core lectures 'Cryptography' and 'Security', unless previously acquired credits from earlier studies can be accepted as equivalent.

   Students who have already successfully completed the two Bachelor-level introductory lecture courses 'Fundamentals of Cybersecurity I' and 'Fundamentals of Cybersecurity II' in their previous Bachelor's degree shall take another core lecture course in place of the core lecture course 'Security'.

2. At least 30 and at most 34 graded credits shall be earned from the core lectures (each worth 9 CP), the advanced lectures on cybersecurity (usually 6 credits, exact number depends on course taken) or the seminars on cybersecurity (each worth 7 credits; module category: mandatory elective). Within this requirement, students may also take a maximum of one further seminar (cf. Sec. 5(2), item 3) and one further core lecture course (cf. Sec. 5(2), item 1).

3. 7 graded credits from the cybersecurity seminars offered (each worth 7 credits; mandatory elective)

4. 12 graded credits from the 'Master's Seminar' module (12 credits)

5. 30 graded credits from the 'Master's Thesis' module (30 credits)

6. At least 14 ungraded credits from freely selectable modules in the following areas (mandatory elective section):
   a. Master's level practical assignments or projects (each worth 6 credits)
   b. Freely selectable modules from the core lecture courses, the advanced lecture courses in cybersecurity or the seminars in cybersecurity or the corresponding modules of the Master's programme in Computer Science,
   c. Tutoring and supervising undergraduate students in exercise and problem-solving classes (usually 4 credits). Tutoring several groups of students is permitted, provided that the exercise and problem-solving classes are from different modules.
   d. Language courses (maximum of 6 credits; modern languages only and not the student's native language).
   e. Soft Skills Seminar
   f. Work placement or internship in industry (maximum of 6 credits) for which an application was submitted to and approved by the Examination Board.
   g. Modules for which an application has been submitted to and approved by the Examination Board. For example, students have the option of submitting an application to the Examination Board requesting recognition of certain student activities (particularly university-related administrative activities) or of attendance at courses teaching key skills (maximum of 3 credits in each case).

(3) Students may select either entire modules or individual module elements from the mandatory electives offered. Credits from academic assessments and examinations that were used to obtain the preceding Bachelor's degree cannot also be used to meet the degree requirements of the Master's programme. However, any credits from academic assessments and examinations that were earned during the Bachelor's degree period but that were not used to meet the total credit requirements for the Bachelor's programme may be transferred to the Master's programme provided that they do not exceed 30 credits in total.

(4) Students are required to earn a total of 42 credits in the mandatory section of the curriculum

(of which 30 credits are from the ‘Master’s Thesis’ module and 12 credits are from the ‘Master’s Seminar’) and at least 78 credits from modules or module elements in the mandatory elective section.

(5) The number of places available in practical skills classes, seminars and in the mandatory elective modules ‘Tutoring’, ‘Soft Skills Seminar’ and ‘Language Courses’ are limited and vary depending on the specific module or module element. Admission to these modules is managed by the module coordinator.

(6) Academic credits are either graded or ungraded. A graded academic assessment or examination cannot be split into ungraded and graded credits.

(7) A student who received academic credits for successfully completing the core lecture courses in cybersecurity and computer science is permitted to retake the assessment or examination on one further occasion within the same examination period and during the standard period of study in order to improve the grade awarded (cf. Sec. 13(4) of the Examination Regulations). A student who received academic credits for successfully completing an advanced lecture course in cybersecurity is permitted to retake the assessment or examination on one further occasion within the same examination period in order to improve the grade awarded, provided that the lecturer gave notice at the beginning of the course that the final examination or assessment may be repeated for this purpose. The student will be awarded the better of the two grades achieved. In all other cases, students are not permitted to repeat an assessment or examination for which they have already achieved at least the minimum passing grade.

(8) The core lecture courses taken within the mandatory electives block are offered at least once every two years. Seminars and advanced lecture courses will not necessarily be repeated. The Dean of Studies will ensure that a sufficient number of courses and modules are offered each year.

(9) The language of instruction is usually English and will be announced at the beginning of each module or module element. It shall be ensured that the Master’s degree programme ‘Cybersecurity’ can be studied completely in English.

(10) The modules or module elements offered as mandatory electives may be modified, though any such change shall require the approval of the Examination Board. New or modified modules or module elements, their weighting in ECTS credits and their classification within the different sections of the programme will be announced before the semester begins.

(11) Detailed information regarding the content of modules and module elements is provided in the module catalogue that will be made available in suitable form. Any changes or amendments to the information in the module catalogue that are not covered by the provisions of these regulations shall be reported to the Dean of Studies and documented appropriately.

(12) Course attendance may be compulsory for certain seminars and practical skills classes. Students will be notified of this by the instructor at the beginning of the module or module element. The compulsory attendance requirement is normally deemed to have been met if a student was present for at least 85% of the course sessions. If there are reasonable grounds for a student’s absence, the student may be offered the option of completing alternative assignments.

(13) Modules that have the same content and that differ only in the language of instruction used shall be treated as a single module with respect to the number of examination attempts permitted and the rules regarding failed first attempts (*Freiversuch* option) and retakes to improve the grade attained, if such provisions are contained in the relevant study regulations.

Section 6
Study plan

The Dean of Studies will compile a study plan based on these study regulations that includes details of the types and scope of the module elements offered (Appendix A) with recommendations on how students can organize and structure their studies efficiently (Appendix B). The study plan will be made available in suitable form. The range of modules offered in a particular semester will be published in the Saarland University course catalogue for that semester.

Section 7
Study counselling

(1) The Central Student Advisory Service (*Zentrale Studienberatung*) at Saarland University provides counselling and guidance to prospective students and enrolled students concerning the content, structure and requirements of academic study at Saarland University. It can also assist students when deciding between various study options and can provide advice on general questions regarding study planning and organization.

(2) Questions concerning curricular demands, learning objectives, admission requirements and programme-specific study planning and organization can be addressed to the programme adviser for 'Cybersecurity'.

(3) Questions specific to individual modules should be addressed to the respective module coordinators.

Section 8
Studying abroad

Students have the opportunity to spend part of the programme studying abroad. Students interested in studying abroad should attend a study-abroad consultation session, take preparatory language courses if required, and should clarify credit transfer arrangements in accordance with the relevant examination regulations by completing a study abroad learning agreement. Information on study abroad opportunities, exchange programmes, scholarships and administrative formalities is available from the Saarland University International Office or from the relevant departmental or subject representative. As foreign host universities and scholarship-awarding bodies often have early application deadlines and long application processing times, study abroad applications should normally be submitted to the Examinations Office one year before the planned start date.

Section 9
Master's thesis and Master's seminar

(1) By completing a Master's thesis, students demonstrate that they are able to work independently on tackling problems in the field of cybersecurity.
The thesis topic will be taken from one of the specified subdisciplines and will be supervised by a member of teaching staff on the Master's degree programme 'Cybersecurity'. The completion period for the Master's thesis is six months. Students are awarded 30 ECTS credits for completing their Master's thesis.

(2) Before finishing their Master's thesis, each student shall have successfully completed a Master's seminar in an area with direct relevance to the topic being addressed in the thesis. Students attending a Master's seminar shall give an oral presentation on the problem they propose to tackle in their Master's thesis and submit a written description of the issues to be addressed.

(3) Students shall register their thesis project with the Examinations Office no later than one semester after successfully completing the Master's seminar. Students who fail to meet this deadline will be required to successfully complete another Master's seminar.

Section 10
Commencement

These regulations shall come into force on the day after they are announced in the Official Bulletin of the Institutions of Higher Education in Saarland (*Dienstblatt der Hochschulen des Saarlandes*).

Saarbrücken, 12 August 2021

On behalf of the President of Saarland University
(Univ.-Prof. Dr. Manfred Schmitt)

Vice-President for Administration and Finance
(Dr. Roland Rolles)

Master's degree programme 'Cybersecurity'

Category	Module name	Type of assessment		ECTS credits		Winter semester		Summer semester		Winter semester		Summer semester	
						Subject semester							
						1		2		3		4	
			g	ungraded	graded	L / EP / P credit hrs/wk	ECTS credits	L / EP / P credit hrs/wk	ECTS credits	L / EP / P credit hrs/wk	ECTS credits	L / EP / P credit hrs/wk	ECTS credits
Core lecture course*	(modules offered subject to change, 9 credits each, see below)	written exam(s), PA	g	0	27	4/2/0 4/2/0	9 9	4/2/0	9				
Core lecture course* or advanced lecture courses in cybersecurity* or seminar in cybersecurity*; max. of one core lecture course and one seminar in cybersecurity	(modules offered subject to change; seminar (7 credits), core lecture course (9 credits) or advanced lecture courses (6 credits each))	written exam(s), PA; oral, written	g	0	30–34	2/2/0 2/2/0	6 6	2/2/0	6	2/2/0 2/2/0	6 6		
Seminar in cybersecurity	(modules offered subject to change, 7 credits each, see below)	oral, written	g	0	7			0/0/3	7				
Mandatory electives section	(modules offered subject to change, variable credits, see list below)		u	at least 14	0			4/2/0	8	4/2/0	6		
	Master's seminar	oral, written	g	0	12						12		
	Master's thesis	Master's thesis	g	0	30								30
	TOTAL						30		30		30		30

* For a list of the modules currently offered, please go to the website of the Examinations Office.

Key: L = Lecture, EP = Exercise and problem-solving class, P = Project or practical training, PA = Preliminary assessment, credits = ECTS credits, credit hrs/wk = no. of class or supervised hours per week during the semester, u = ungraded, g = graded

Core lecture courses				
Cryptography **(compulsory)**	written exam(s), PA	g	0	9
Security **(compulsory)**	written exam(s), PA	g	0	9
Algorithms and Data Structures	written exam(s), PA	g	0	9
Artificial Intelligence	written exam(s), PA	g	0	9
Audio/Visual Communication and Networks	written exam(s), PA	g	0	9
Automated Reasoning	written exam(s), PA	g	0	9
Compiler Construction	written exam(s), PA	g	0	9
Complexity Theory	written exam(s), PA	g	0	9
Computer Algebra	written exam(s), PA	g	0	9
Computer Graphics	written exam(s), PA	g	0	9
Data Networks	written exam(s), PA	g	0	9
Database Systems	written exam(s), PA	g	0	9
Digital Transmission, Signal Processing	written exam(s), PA	g	0	9
Distributed Systems	written exam(s), PA	g	0	9
Embedded Systems	written exam(s), PA	g	0	9
Geometric Modeling	written exam(s), PA	g	0	9
Human Computer Interaction	written exam(s), PA	g	0	9
Image Processing and Computer Vision	written exam(s), PA	g	0	9
Information Retrieval and Data Mining	written exam(s), PA	g	0	9
Introduction to Computational Logic	written exam(s), PA	g	0	9
Machine Learning	written exam(s), PA	g	0	9
Multimedia Transport	written exam(s), PA	g	0	9
Operating Systems	written exam(s), PA	g	0	9
Optimization	written exam(s), PA	g	0	9
Semantics	written exam(s), PA	g	0	9
Software Engineering	written exam(s), PA	g	0	9
Verification	written exam(s), PA	g	0	9
The Examination Board may add modules to or withdraw modules from this list.				
Advanced lecture courses in cybersecurity				
The advanced lecture courses in cybersecurity may vary from semester to semester				
Advanced Public Key Cryptography	written exam(s), PA	g	0	6
Algorithms in Cryptanalysis	written exam(s), PA	g	0	6
Automated Debugging	written exam(s), PA	g	0	6
Ethics for Nerds	written exam(s), PA	g	0	6
Generated Software Tests	written exam(s), PA	g	0	6
Machine Learning in Cybersecurity	written exam(s), PA	g	0	6
Mobile Security	written exam(s), PA	g	0	6
Obfuscation	written exam(s), PA	g	0	6
Parameterized Verification	written exam(s), PA	g	0	6
Physical-Layer Security	written exam(s), PA	g	0	6
Privacy Enhancing Technologies	written exam(s), PA	g	0	6
Reactive Synthesis	written exam(s), PA	g	0	6
Cybersecurity Laws and Regulations – Legal Aspects of Data Protection	written exam(s), PA	g	0	6
Cybersecurity Laws and Regulations – Legal Aspects of Cybercrime	written exam(s), PA	g	0	6
Secure Web Development	written exam(s), PA	g	0	6
Side-Channels Attacks & Defenses	written exam(s), PA	g	0	6
Usable Security	written exam(s), PA	g	0	6
Web Security	written exam(s), PA	g	0	6
The Examination Board may add modules to or withdraw modules from this list.				
Seminars in cybersecurity				
The cybersecurity seminars offered may vary from semester to semester.	oral, written	g	0	7
The Examination Board may add modules to or withdraw modules from this list.				
Mandatory electives section				
Tutoring	Student tutoring work	u	4	0
Soft Skills Seminar	oral, written	u	variable	0
Language courses (max. 6 credits)	oral, written	u	3 or 6	0
Industrial work placement / internship (max. 6 credits)		u	6	0
Master's level practical assignments or projects (each worth 6 credits)		u	6	0
Additional modules from the areas cybersecurity or computer science	written exam(s), PA	u	variable	0
The Examination Board may add modules to or withdraw modules from this list.				

Appendix B

Sample study plan
Master's Degree Programme 'Cybersecurity' (for students with no prior knowledge of cybersecurity)

1	Security (9 credits)	Core Lecture Course (9 credits)	Advanced Lecture Course in Cybersecurity (6 credits)	Advanced Lecture Course in Cybersecurity (6 credits)	30
2	Cryptography (9 credits)	Advanced Lecture Course in Cybersecurity (6 credits)	Seminar CySec (7 credits)	Mandatory Elective (8 credits)	30
3	Advanced Lecture Course in Cybersecurity (6 credits)	Advanced Lecture Course in Cybersecurity (6 credits)	Mandatory Elective (6 credits)	Master's Seminar (12 credits)	30
4	Master's Thesis (30 credits)				30

Sample study plan
Master's Degree Programme 'Cybersecurity' (for graduates from Bachelor's degree programmes 'B.Sc. Cybersicherheit' or 'B.Sc. Cybersecurity (English)')

1	Core Lecture Course (9 credits)	Core Lecture Course (9 credits)	Advanced Lecture Course in Cybersecurity (6 credits)	Advanced Lecture Course in Cybersecurity (6 credits)	30
2	Core Lecture Course (9 credits)	Advanced Lecture Course in Cybersecurity (6 credits)	Seminar CySec (7 credits)	Mandatory Elective (8 credits)	30
3	Advanced Lecture Course in Cybersecurity (6 credits)	Advanced Lecture Course in Cybersecurity (6 credits)	Mandatory Elective (6 credits)	Master's Seminar (12 credits)	30
4	Master's Thesis (30 credits)				30