AALBORG UNIVERSITET

CURRICULUM FOR THE MASTER'S PROGRAMME IN CYBER SECURITY, 2020

MASTER OF SCIENCE (MSC) IN ENGINEERING
COPENHAGEN

Link to this studyline

TABLE OF CONTENTS

§ 1: PREFACE

Pursuant to consolidation Act 778 of August 7, 2019 on Universities (the University Act), the following is established. The programme also follows the Joint Programme Regulations and the Examination Policies and Procedures for Aalborg University.

§ 2: BASIS IN MINISTERIAL ORDERS

The Master's programme is organised in accordance with the Ministry of Higher Education and Science's Order no. 20 of January 9, 2020 on Bachelor's and Master's Programmes at Universities (the Ministerial Order of the Study Programmes) and Ministerial Order no. 22 of January 9, 2020 on University Examinations (the Examination Order). Further reference is made to Ministerial Order no. 153 of February 26, 2020 (the Admission Order) and Ministerial Order no. 114 of February 3, 2015 (the Grading Scale Order).

§ 3: CAMPUS

The programme is offered in Copenhagen.

§ 4: FACULTY AFFILIATION

The Master's programme falls under the The Technical Faculty of IT and Design, Aalborg University.

§ 5: STUDY BOARD AFFILIATION

The Master's programme falls under the Study Board of Electronics and IT.

§ 6: AFFILIATION TO CORPS OF EXTERNAL EXAMINERS

The Master's programme is associated with the Nationwide engineering examiners/Electronics, IT and Energy (Electromagnetic direction).

§ 7: ADMISSION REQUIREMENTS

Applicants with a legal right of admission (retskrav)

Aalborg University offers no bachelor's programmes with a legal right of admission to this Master's programme.

Applicants without legal right of admission

Bachelor's programmes qualifying students for admission:

- Aalborg University:
  - Bachelor in IT, Communication and New Media
  - Bachelor in Computer Engineering
  - Bachelor in Electronic Engineering
  - Bachelor of Engineering in Electronics
  - Bachelor in Computer Science
  - Bachelor in Software
  - Bachelor in Information Technology
- Technical University of Denmark:
  - Bachelor in Electrical Engineering
  - Bachelor of Engineering in Electrical Engineering
  - Bachelor in Cyber Technology (former Network Technology and IT)
  - Bachelor in Software Technology
  - Bachelor of Engineering in Software Technology
- University of Copenhagen:
  - Bachelor in Computer Science
- IT University of Copenhagen:
  - Bachelor in Software Development
- Aarhus University:
  - Bachelor in Computer Science
    Bachelor in Computer Engineering

  - Bachelor of Engineering in Electronics

- University of Southern Denmark:
  - Bachelor in Electronics
  - Bachelor in Software Engineering
  - Bachelor in Computer Science

All applicants must prove that their English language qualifications is equivalent to level B (Danish level) in English.

§ 8: THE PROGRAMME TITLE IN DANISH AND ENGLISH

The Master's programme entitles the graduate to the Danish designation Civilingeniør, cand.polyt. i cybersikkerhed. The English designation is: Master of Science (MSc) in Engineering (Cyber Security)

§ 9: PROGRAMME SPECIFICATIONS IN ECTS CREDITS

The Master's programme is a 2-year, research-based, full-time study programme. The programme is set to 120 ECTS credits.

§ 10: RULES CONCERNING CREDIT TRANSFER (MERIT), INCLUDING THE POSSIBILITY FOR CHOICE OF MODULES THAT ARE PART OF ANOTHER PROGRAMME AT A UNIVERSITY IN DENMARK OR ABROAD

The Study Board can approve that passed programme elements from other educational programmes at the same level replaces programme elements within this programme (credit transfer).

Furthermore, the Study Board can, upon application, approve that parts of this programme is completed at another university or a further education institution in Denmark or abroad (pre-approval of credit transfer).

The Study Board's decisions regarding credit transfer are based on an academic assessment.

§ 11: EXEMPTIONS

The Study Board's possibilities to grant exemption, including exemption to further examination attempts and special examination conditions, are stated in the Examination Policies and Procedures published at this website: https://www.studieservice.aau.dk/regler-vejledninger

§ 12: RULES FOR EXAMINATIONS

The rules for examinations are stated in the Examination Policies and Procedures published at this website: https://www.studieservice.aau.dk/regler-vejledninger

§ 13: RULES CONCERNING WRITTEN WORK, INCLUDING THE MASTER'S THESIS

In the assessment of all written work, regardless of the language it is written in, weight is also given to the student's formulation and spelling ability, in addition to the academic content. Orthographic and grammatical correctness as well as stylistic proficiency are taken as a basis for the evaluation of language performance. Language performance must always be included as an independent dimension of the total evaluation. However, no examination can be assessed as 'Pass' on the basis of good language performance alone; similarly, an examination normally cannot be assessed as 'Fail' on the basis of poor language performance alone.

The Study Board can grant exemption from this in special cases (e.g., dyslexia or a native language other than Danish).

The Master's Thesis must include an English summary. If the project is written in English, the summary can be in Danish. The summary is included in the evaluation of the project as a whole.

§ 14: REQUIREMENTS REGARDING THE READING OF TEXTS IN A FOREIGN LANGUAGE

It is assumed that the student can read academic texts and use reference works, etc., in English.

§ 15: COMPETENCE PROFILE ON THE DIPLOMA

The following competence profile will appear on the diploma:

A Candidatus graduate has the following competency profile:

A Candidatus graduate has competencies that have been acquired via a course of study that has taken place in a research environment.

A Candidatus graduate is qualified for employment on the labour market based on his or her academic discipline as well as for further research (PhD programmes). A Candidatus graduate has, compared to a Bachelor, developed his or her academic knowledge and independence so as to be able to apply scientific theory and method on an independent basis within both an academic and a professional context.

§ 16: COMPETENCE PROFILE OF THE PROGRAMME

The graduate of the Master's programme

Knowledge

- Must have knowledge about the analysis of complex security problems and the design of secure distributed solutions for such problems.
- Must have knowledge about the relation between security risks and business processes, including identification and protection of business critical assets.
- Must have knowledge about implementation of distributed systems, with a focus on the security aspects.
- Must have knowledge that is based on the highest international research in a number of subject areas within cyber security, such as:
  - Network security
  - Design of secure systems and software
  - Security in IoT and cloud architectures
  - Risk assessment
- Must have knowledge in one or more of the following areas:
  - Privacy engineering
  - Enterprise security
  - Models of software security
  - IT security regulation and governance

Skills

- Must have skills in monitoring and analysing network activity and traffic, including techniques for detection of anomalies and malicious activities.
- Must have skills in configuring and operating secure test environments for e.g. malware analysis and data generation.
- Must be able to choose the most relevant theory/model and perform a security analysis and evaluation of a system/network.
- Must be able to use various state-of-the-art frameworks for identifying adversaries as well as for developing/deploying attacks
- Must be able to identify the research and development challenges for a cyber-security engineering project and propose/develop relevant solutions
- Must have skills in communicating cyber security challenges and solutions to non-experts.
- Must be able to
  - select and apply relevant machine learning algorithms and techniques for detection of cyber-attacks or anomalous behaviour in cyber systems
    OR
  - select and apply relevant technologies and frameworks for identity and access management to implement strong authentication and access control

Competencies

- Must have the competency to assess and select relevant scientific and technical literature within the various subject areas of cyber security
- Must have the competency to connect research challenges and questions within cyber security to real world problems and products that will have an impact on society
- Must have the competency to analyse cyber risks and identify cyber security needs of an organization
- Must have the competency to compare and assess the potential of different technologies, methods and approaches to make proper security design choices
- Must have the competency to combine a wide range of technologies and devices to realize advanced and non-trivial cyber-security applications and solutions

- Must have the competency to assess, choose and apply methods for securing and/or security testing systems, and to evaluate and reflect on the results achieved

§ 17: STRUCTURE AND CONTENTS OF THE PROGRAMME

The programme is structured in modules and organised as a problem-based study. A module is a programme element or a group of programme elements, which aims to give students a set of professional skills within a fixed time frame specified in ECTS credits, and concluding with one or more examinations within specific exam periods. Examinations are defined in the curriculum.

The programme is based on a combination of academic, problem-oriented and interdisciplinary approaches and organized based on the following work and evaluation methods that combine skills and reflection:

- lectures
- classroom instruction
- project work
- workshops
- exercises (individually and in groups)
- self-study
- teacher feedback
- reflection
- portfolio work

In total, 90 ECTS out of 120 ECTS are common for all students. The common part consists of:

- All courses and projects on the 1st semester
- 2 mandatory courses and a semester project on the 2nd semester
- 1 mandatory course on “Advanced topics in cyber security” (5 ECTS) on the 3rd semester, and
- The thesis project on the 4th semester

Electives: The remaining 30 ECTS can be obtained by choosing elective courses and projects on the 2nd and 3rd semester as described below. Note that elective courses might not be offered if less than 10 students register for the course during the registration period. Students will be offered other options if a chosen course is not offered.

§ 18: OVERVIEW OF THE PROGRAMME

All modules are assessed through individual grading according to the 7-point scale or Pass/Fail. All modules are assessed by external examination (external grading) or internal examination (internal grading or by assessment by the supervisor only).

Offered as: 1-professional						
Module name	Course type	ECTS	Applied grading scale	Evaluation method	Assessment method	Language
1 SEMESTER						
Distributed Systems Security (ESNCYSK1P1)	Project	10	7-point grading scale	Internal examination	Oral exam based on a project	English
Fundamentals of Security and Cryptography (ESNCYSK1K1)	Course	5	Passed/Not Passed	Internal examination	Written or oral exam	English

Network Security (ESNCYSK1K2)	Course	5	7-point grading scale	Internal examination	Written or oral exam	English
Secure Software Development (ESNCYSK1K3)	Course	5	7-point grading scale	Internal examination	Written or oral exam	English
Security in IoT and Cloud Architectures (ESNCYSK1K4)	Course	5	7-point grading scale	Internal examination	Written or oral exam	English
2 SEMESTER						
Secure Systems: Attack and Defence (ESNCYSK2P1)	Project	15	7-point grading scale	External examination	Oral exam based on a project	English
Hacker Space (ESNCYSK2K1)	Course	5	7-point grading scale	Internal examination	Written or oral exam	English
Advanced Software Security (ESNCYSK2K2)	Course	5	7-point grading scale	Internal examination	Written or oral exam	English
Elective course 2nd Semester Choose 1 course module	Course	5				
3 SEMESTER Option A						
Elective Project 3rd Semester Choose 1 project	Project	15				
Advanced Topics in Cyber Security (ESNCYSK3K1)	Course	5	7-point grading scale	Internal examination	Written or oral exam	English
Elective course 3rd Semester Choose 2 course Module	Project	10				
3 SEMESTER Option B						
Project-Oriented Study in an External Organisation (ESNCYSK3P3)	Project	25	Passed/Not Passed	Internal examination	Oral exam based on a project	English
Advanced Topics in Cyber Security (ESNCYSK3K1)	Course	5	7-point grading scale	Internal examination	Written or oral exam	English
3-4 SEMESTER Option A						
Master's Thesis (ESNCYSK4P2)	Project	45	7-point grading scale	External examination	Master's thesis/final project	English
Advanced Topics in Cyber Security (ESNCYSK3K1)	Course	5	7-point grading scale	Internal examination	Written or oral exam	English
Elective course 3rd Semester Choose 2 course Module	Course	10				
3-4 SEMESTER Option B						
Master's Thesis (ESNCYSK4P3)	Project	50	7-point grading scale	External examination	Master's thesis/final project	English
Advanced Topics in Cyber Security (ESNCYSK3K1)	Course	5	7-point grading scale	Internal examination	Written or oral exam	English
Elective course 3rd Semester Choose 1 course module	Course	5				

4 SEMESTER						
Master's Thesis (ESNCYSK4P1)	Project	30	7-point grading scale	External examination	Master's thesis/final project	English

Elective course 2nd Semester Choose 1 course module						
Module name	Course type	ECTS	Applied grading scale	Evaluation Method	Assessment method	Language
Identity and Access Management (ESNCYSK2K3)	Course	5	7-point grading scale	Internal examination	Written or oral exam	English
Machine Learning (ESNCYSK2K4)	Course	5	7-point grading scale	Internal examination	Written or oral exam	English

Elective Project 3rd Semester Choose 1 project						
Module name	Course type	ECTS	Applied grading scale	Evaluation Method	Assessment method	Language
Secure Systems Development (ESNCYSK3P1)	Project	15	7-point grading scale	Internal examination	Oral exam based on a project	English
IT Security Governance (ESNCYSK3P2)	Project	15	7-point grading scale	Internal examination	Oral exam based on a project	English

Elective course 3rd Semester Choose 2 course Module						
Module name	Course type	ECTS	Applied grading scale	Evaluation Method	Assessment method	Language
Privacy Engineering (ESNCYSK3K2)	Course	5	7-point grading scale	Internal examination	Written or oral exam	English
Models of Security (ESNCYSK3K3)	Course	5	7-point grading scale	Internal examination	Written or oral exam	English
Regulation of IT Security (ESNCYSK3K4)	Course	5	7-point grading scale	Internal examination	Written or oral exam	English
Enterprise Security and Compliance (ESNICTEK3K6)	Course	5	7-point grading scale	Internal examination	Written or oral exam	English

Elective course 3rd Semester Choose 1 course module						
Module name	Course type	ECTS	Applied grading scale	Evaluation Method	Assessment method	Language

Privacy Engineering (ESNCYSK3K2)	Course	5	7-point grading scale	Internal examination	Written or oral exam	English
Models of Security (ESNCYSK3K3)	Course	5	7-point grading scale	Internal examination	Written or oral exam	English
Regulation of IT Security (ESNCYSK3K4)	Course	5	7-point grading scale	Internal examination	Written or oral exam	English
Enterprise Security and Compliance (ESNICTEK3K6)	Course	5	7-point grading scale	Internal examination	Written or oral exam	English

The master's thesis can be conducted as a long master's thesis. If choosing to do a long master's thesis, it has to include experimental work and has to be approved by the study board. The amount of experimental work must reflect the allotted ECTS-credits.

NOTE: Elective courses might not be offered if less than 10 students register for the course during the registration period. Students will be offered other options if a chosen course is not offered.

§ 19: ADDITIONAL INFORMATION

All students who have not participated in Aalborg University's PBL introductory course during their Bachelor's degree must attend the introductory course "Problem-based Learning and Project Management". The introductory course must be approved before the student can participate in the project exam. For further information, please see Department of Electronics Systems's webiste.

§ 20: COMMENCEMENT AND TRANSITIONAL RULES

The curriculum is approved by the dean and enters into force as of 01.09.2020.

§ 21: AMENDMENTS TO THE CURRICULUM AND REGULATIONS

On 26th April 2021 the Vice-Dean of Education has approved, that the competence learning objectives of the Master's Thesis (30, 45 and 50 ECTS respecticely) are revised. The amendment is valid from Spring 2021.

On 7th September 2021 the Vice-Dean of Education has approved, that the assessment in the course module *"Fundamentals of Security and Cryptography"* on the 1st Semester is changed from 7-point grading scale to "Passed/Not Passed". The amendment is valid from Autumn 2021.