UNIVERSITY OF AMSTERDAM

FACULTY OF SCIENCE

TEACHING AND EXAMINATION REGULATIONS

PART B: programme-specific section

Academic year 2020-2021

MASTER'S PROGRAMME
SECURITY AND NETWORK ENGINEERING

Contents

Chapter 1. General Provisions

Article B-1.1 – Definitions

In addition to part A, the following definitions are used in part B.

Research Project 1	A component of 6 EC comprising research into the literature and/or contributing to scientific research and/or an internship, always resulting in a written report. Research Project 1 is not considered part of the Master's thesis.
Research Project 2	A component of 6 EC comprising research into the literature and/or contributing to scientific research and/or an internship, always resulting in a written report. Research Project 2 is considered the Master's thesis/graduation project.

Article B-1.2 – Study programme information

1. The Master's programme Security and Network Engineering, CROHO number 60227, is offered on a full-time and part-time basis (part-time means taking the curriculum in two years). The official language is English. This means that the Code of Conduct for Foreign Languages at the UvA applies for this programme (see Code of Conduct Governing Foreign Languages at the University of Amsterdam 2000 at the website: https://www.uva.nl/en/about-the-uva/about-the-university/rules-and-regulations/teaching/teaching.html.
2. The programme consists of a one-year programme with a total study load of 60 EC.

Article B-1.3 – Enrolment

The programme is offered starting in the first semester of the academic year (1 September).

Chapter 2. Programme objectives and exit qualifications

Article B-2.1 – Programme objectives

The Master's programme Security and Network Engineering (SNE) is a scientific, professionally oriented one year study programme with a compulsory curriculum. The objective of the programme is the training of security and network engineers who:

1. have knowledge on an abstract level of the operation of computers and networks with respect to interfaces, protocols and software;
2. are able to translate this abstract knowledge into concrete system and network configurations, independent of underlying vendor technology;
3. are able to acquire knowledge about innovative technologies and evaluate their potential;
4. are able to accommodate those innovations in an evolutionary way into existing systems;
5. are familiar with the philosophy and practice of Open Source Technology and are able to evaluate its strength and possibilities in relation to proprietary technology;
6. are able to build innovative systems using Open Source Components;
7. are able to recognize security aspects of systems on all levels and to take adequate measures to eliminate security problems where needed.
8. are able to become acquainted with research methods in the domain within a short period of time and are able to apply these;
9. are familiar with the ethical and juridical aspects of their research.

Article B-2.2 – Exit qualifications

1. The Exit qualifications of the Master's programme Security and Network Engineering are defined as follows: graduates of the Master's programme in Security and Network Engineering should
   1. have insight into the most important technological developments and related scientific results in the field of security and network engineering.
   2. have the capacity to apply this insight in the interests of the innovation and modernisation of systems and networks.
   3. have participated in active scientific research as is being performed in the Informatics Institute of the University of Amsterdam or in comparable scientific research groups or R&D divisions of companies.
   4. have the capacity to address security and network engineering problems using abstraction and model formation, and they should be capable of formulating solutions in general, mathematical and technical terms.
   5. have the capacity to communicate clearly, both orally and in writing; they should be skilled in giving presentations to groups and should know how to explain problems and solutions at the appropriate level of abstraction.
   6. be able to function well in teams. They should be capable of discussing technical topics in both small and large groups, and they should be well equipped to distribute and coordinate technical tasks among group members.
   7. be aware of the societal, ethical and social aspects of security and network engineering.
   8. be skilled in exploring (searching, reading and evaluating) the many forms of documentation and literature concerning security and network engineering, with regard to both content and medium. They should be familiar with the Internet Society (ISOC), the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C) and other international bodies that develop standards and publish in the area of computer systems and networks.
   9. be highly familiar with the usual configurations and procedures for the regular and crisis administration of a variety of current systems and networks, middleware and applications.
   10. have knowledge about methods and principles of systems based on Open Technology, which consists of Open Standards, Open Software (including Open Source) and Open Security. Graduates should be able to apply this knowledge in existing, complex environments and to integrate Open Technology with (partly) proprietary solutions.
   11. be highly familiar with the security functions of systems and networks, and they should be capable of contributing actively to the architecture and the configuration of systems and networks that conform to current security standards. Graduates should also be able to determine whether systems or networks conform to particular security standards.
   12. have the technical knowledge of communication protocols, network components and business systems that they will need to accurately justify choices and steps relating to administration and security, including those regarding configuration, procedures and security architecture.
   13. have a good understanding of the world of Internet Service Providers and routing issues in local networks and the global Internet.
   14. have sufficient insight into the organisational contexts within which systems and networks function, to channel the needs of organisations and users, and to translate them into appropriate technical support.
   15. have sufficient technical knowledge and intellectual capacity to assume positions of leadership in the field of security and network engineering within a few years. They should have the capacity to develop their own vision of the field of security and network engineering, thus contributing to evolution and innovation in concrete system environments.
   16. understand methods for gathering digital traces from a computer system and have the knowledge to assure that information gathered is suited for forensic or security analysis.

17. have the knowledge and capabilities to build systems supporting the forensic or security investigation process with tools enhancing the human capacity to perceive, understand and reason about complex and dynamic data and situations.
18. be able to understand and develop the tools and techniques for analysing and fighting cybercrime.
19. be able to gather and manage the computational resources required to analyse large amounts of complex, dynamic, and distributed data.
20. understand the relation between security processes and cybercrime on the one hand and the security and vulnerability of systems on the other hand.
21. know about current cryptography standards and protocols and their development and be able to make assessments to their proper application.
22. understand the technology and implications of virtualised infrastructure like public and private clouds.
23. understand and be able to implement the trust models needed for secure data sharing.
24. be familiar with wireless technology standards and protocols and be able to make assessments to their proper and secure application.

Chapter 3. Further admission requirements

Article B-3.1 – Admission requirements

1. Admission to the Master's programme Security and Network Engineering is possible, under the conditions as described in paragraph 2, for students with the following qualifications:
    1. A Bachelor Computer Science or a closely related programme from a Dutch university.
    2. A foreign qualification, comparable to B-3.1.1.1, under the condition of sufficient active and passive knowledge of the English language. For details, see Article B-3.5.
    3. A Bachelor Informatics, Technical Informatics or a closely related vocational education (HBO).
2. All students, as mentioned under B-3.1.1. can only be admitted to the Master's programme under the condition of a successful result in an assessment procedure.
   This assessment considers knowledge and motivation and evaluates
   A. General scientific skills:
      1. Writing skills: reading and outlining a technical document
      2. Verbal skills: presenting earlier work
      3. Analytical skills: elementary basic and discrete mathematics, and logic
   B. Specific SNE-skills:
      1. Elementary knowledge of Unix and/or Linux
      2. Elementary knowledge of TCP/IP-networks
      3. Elementary knowledge of Python programming
3. In special cases the Admissions Board may decide to admit a prospective student based on other relevant qualifications, for instance equivalent work experience. The Admissions Board decides on an appropriate assessment for each case.
4. Every submission will be reviewed by the Admissions Board. Admission is only possible with explicit approval from this board.

Article B-3.2 – Pre-Master's programme
Not applicable.

Article B-3.3 – Limited programme capacity
Components within the Master's Programme in Security and Network Engineering, as described under Chapter 4, are exclusively open to students registered in the SNE programme.

Article B-3.4 – Final deadline for registration

1. A request for admission to the Master's programme starting in September must be submitted to Studielink and the Faculty before 1 July in the case of EU/EEA/Swiss students and before 1 February in the case of non-EU/EEA/Swiss students.
2. In exceptional cases, the Admissions Board may consider a request submitted after this closing date

Article B-3.5 – English language requirements

1. The proficiency requirement in English as the official language can be met by the successful completion of one of the following examinations:
    a. IELTS: 7.0, at least 7.0on each sub-score (listening/reading/writing/speaking);
    b. TOEFL paper-based: 590, paper-delivered at least 24 on each sub-score;
    c. TOEFL Internet-based test: 100, at least 24 on each sub-score (listening/reading/writing/speaking);

    The foregoing examination must have been taken within two years before the student's enrolment.
    d. C1 Advanced (CAE): minimal result 180 (overall B);
    e. C2 Proficiency (CPE): minimal result 170 (overall C)

    Please note that the TOEFL-code for the Faculty of Science of the University of Amsterdam is 9011.
2. An exemption from the English examination referred to in the first paragraph shall be granted to students who:
    a. had previous education in secondary or tertiary education in one of the following English-speaking countries: Australia, Canada (English), New Zealand, Ireland, the United Kingdom or the United States of America;
    b. hold an English-language 'international baccalaureate' diploma;
    c. possessing a Bachelor's degree from a Dutch university satisfy the requirement of sufficient command of the English language;
    d. passed the final examination for the subject of English as part of one of the following diplomas: VWO, Belgian ASO (Flemish).

Chapter 4. Curriculum structure

Article B-4.1 – Composition of the programme

1. The programme consists of compulsory components amounting to 60 EC.
2. Every component will be tested. In the course catalogue this is described per component.
3. Within the programme different types of teaching methods are used. In the course catalogue this is described per component.

Article B-4.2 – Compulsory components

1. Full-time

Component	Code	Study load (EC)	Semester	Teaching method	Assessment
Classical Internet Applications	5384CLIA6Y	6	1	L, PLE	Written
Security of Systems and Networks	5384SESN6Y	6	1	L, PLE, PR	Written, oral
Large Systems	5384LASY6Y	6	1	L, PLE, PR	Written, oral
InterNetworking and Routing	5384INRO6Y	6	1	L, PLE	Written
Research Project 1	53841REP6Y	6	1	PR	Written, oral
Cybercrime and Forensics	5384CYFO6Y	6	2	L, PLE, PR	Written, oral
Advanced Networking	5384ADNE6Y	6	2	L, PLE	Written
Offensive Technologies	5384OFTE6Y	6	2	L, PLE, PR	Written, oral
Advanced Security	5384ADSE6Y	6	2	L, PLE	Written, oral
Research Project 2	53842REP6Y	6	2	PR	Written, oral

L = Lectures, PLE = Practical Lab Exercises, PR = Practical Research

2. Part-time

Year1

Component	Code	Study load (EC)	Semester	Teaching method	Assessment
Security of Systems and Networks	5384SESN6Y	6	1	L, PLE, PR	Written, oral
Large Systems	5384LASY6Y	6	1	L, PLE, PR	Written, oral
Research Project 1	53841REP6Y	6	1	PR	Written, oral
Cybercrime and Forensics	5384CYFO6Y	6	2	L, PLE, PR	Written, oral
Offensive Technologies	5384OFTE6Y	6	2	L, PLE, PR	Written, oral

L = Lectures, PLE = Practical Lab Exercises, PR = Practical Research

Year 2

Component	Code	Study load (EC)	Semester	Teaching method	Assessment
Classical Internet Applications	5384CLIA6Y	6	1	L, PLE	Written
InterNetworking and Routing	5384INRO6Y	6	1	L, PLE	Written
Advanced Networking	5384ADNE6Y	6	2	L, PLE	Written
Advanced Security	5384ADSE6Y	6	2	L, PLE	Written, oral
Research Project 2	53842REP6Y	6	2	PR	Written, oral

L = Lectures, PLE = Practical Lab Exercises, PR = Practical Research

Article B-4.3 – Practical work
In addition to, or instead of, classes in the form of lectures, the elements of the Master's programme often include a practical component as defined in article A-1.2 of part A.

Article B-4.4 – Elective components
Not applicable.

Article B-4.5 – Free curriculum
1. Subject to certain conditions, the student has the option of compiling a curriculum of his/her own choice which deviates from the curricula prescribed by the programme.
2. The concrete details of such a curriculum must be approved beforehand by the most appropriate Examinations Board. Because of the compact program, with a strong focus on collaboration, the Examinations Board will only approve a free curriculum in exceptional cases.
3. The free curriculum is put together by the student from the units of study offered by the University of Amsterdam and must at least have the size, breadth and depth of a regular Master's programme, and is in line with the learning outcomes of the degree programme.
4. The following conditions must at least have been met in order to be eligible for the Master's degree:
    1. at least 48 EC must be obtained from the regular curriculum;
    2. the level of the programme must match the objectives and exit qualifications that apply for the programme for which the student is enrolled.

Article B-4.6 – Sequence of examinations
1. The student may participate in examinations of a component only after the student has shown that he/she has the prerequisite knowledge. To that end, a student must have passed the components stated in the course catalogue, that are prerequisite knowledge.
2. The student may start with the master project of the study programme (Research Project 2) only if Research Project 1 has been completed and no more than 12 EC of the complete programme as described in Article B-4.2 have been missed. The final project (Research Project 2) must be approved by the staff members and also by the ethics committee (ECOS3).
3. Resits for practical work are only permitted in special circumstances, which must be approved by the Examinations Board.
4. Written work has to be handed in for assessment in time. In case this condition is not met, the component has to be taken again in the next year. After the first assessment written work can be handed in once more for final improvements.
5. The assessment of projects in which several students have worked on an assignment will only be made at the end of the relevant teaching period. In principle, an individual resit is not possible.
6. At the request of a student, the Examinations Board may deviate from the conditions in paragraphs 1, 2 and 5 for the benefit of the student.

Article B-4.7 – Participation in lectures, practical work and study group sessions
1. All parts and activities of the curriculum are obligatory (presence and participation). This includes lectures, seminars, practical work, colloquia and site visits.
2. Exemptions for activities have to be granted in advance by the examiner.
3. If no exemption has been granted and the conditions as stated in paragraph 1 were not met, the component has to be taken again.

Article B-4.8 – Maximum exemption
Not applicable.

Article B-4.9 – Validity period of examinations

1. The validity period of successfully completed (interim) examinations and exemptions can be limited, as described in part A, article A-4.8.
2. In addition to article A-4.8.2 of part A, all components that are listed in article B 4.2 can be tested on grounds of present-day scientific insights when a student wants to include results of successfully completed examinations and/or granted exemptions older than 3 years in his/her study programme. If the contents of those components no longer correspond to the present-day insights and/or the objects of the master programme, the Programme Director can decide that the results of successfully completed examinations have expired and the Examinations Board will choose replacing components.
3. In addition to article A-4.8.4 of part A results of interim examinations which include theoretical course material are valid throughout the period of the course in question. Results of practical examinations are valid up to and including the end of the academic year in which they were achieved.

Article B-4.10 – Degree

Students who have successfully completed their Master's examination are awarded a Master of Science degree. The degree awarded is stated on the diploma.

Chapter 5. Academic student counselling

Article B-5.1 Academic student counselling

The academic student counselling for this programme consists of individual and group coaching by the core team of lecturers, as well as by the Faculty study adviser.

Chapter 6. Teaching evaluation

Article B-6.1 Teaching evaluation

1. Teaching evaluation is organised both on a per-course and on a per-programme basis.
2. At the end of each regular course each student receives a detailed questionnaire via the UvA Q system.
3. After graduation each student receives a final questionnaire via the UvA Q system.

Chapter 7. Transitional and final provisions

Article B-7.1 - Amendments and periodic review

1. Any amendment to the Teaching and Examination Regulations will be adopted by the dean after taking advice, and if necessary approval by the relevant Programme Committee. A copy of the advice will be sent to the authorised representative advisory body.
2. An amendment to the Teaching and Examination Regulations requires the approval of the authorised representative advisory body as stated in the WHW.
3. An amendment to the Teaching and Examination Regulations is only permitted to concern an academic year already in progress if this demonstrably does not damage the interests of students.

Article B-7.2 – Transitional provisions

Not applicable.

Article B-7.3 - Publication

1. The Dean of the faculty will ensure the appropriate publication of these Regulations and any amendments to them.
2. The Teaching and Examination Regulations will be posted on the faculty website and deemed to be included in the course catalogue.

Article B-7.4 – Effective date

These Regulations enter into force with effect from 31 August, 2020.
Thus, drawn up by the Dean of the Faculty of Science on 10 November, 2020.