JÖNKÖPING UNIVERSITY
School of Engineering

PROGRAMME SYLLABUS

Cybersecurity (one year master), 60 credits

Cybersäkerhet (magister), 60 högskolepoäng

Programme Code:	TACS4	Programmestart:	Autumn 2025
Confirmed:	Feb 01, 2025	Education Cycle:	Second-cycle level

Title of qualification

Degree of Master (60 credits) with a major in Computer Science specialisation in Cybersecurity

Magisterexamen med huvudområdet datavetenskap inriktning Cybersäkerhet

Programme overview

Main field of study

"Computer science (CS) is the study of computers and algorithmic processes, including their principles, their hardware and software designs, their applications, and their impact on society." (Tucker, Allen, ACM, 2006.)

The Computing Sciences Accreditation Board—which is made up of representatives of the Association for Computing Machinery (ACM), and the IEEE Computer Society (IEEE CS)—identifies four areas that it considers crucial to the discipline of computer science: theory of computation, algorithms and data structures, programming methodology and languages, and computer elements and architecture.

In addition to these four areas, CSAB also identifies a large number of fields as being important areas of computer science, e.g., software engineering, artificial intelligence, database systems, parallel and distributed computation, computer networking and communication, operating systems, human–computer interaction, and computer graphics.

The scientific basis for computer science is logic and discrete mathematics. Consequently, mathematical deduction is an important tool. Scientific studies in computer science are usually conducted using quantitative methods from science or engineering. The most typical research approach is controlled experiments, with subsequent statistical analysis and inference; but traditional social science methods like case studies and interviews can be used where appropriate. Another approach is design science, where an IT-artifact is developed to demonstrate how concepts, theories, models and methods work in practice.

Computer science is related to computer engineering, which in turn has a strong connection to electrical engineering. Internationally, computer science is broadly defined, specifically, hardware and computer architectures are usually included, as can also be seen from CSAB’s description above. In Sweden, the distinction is often made that computer engineering mainly studies the design and construction of computers and other hardware, while computer science focuses on software systems. Areas such as hardware programming, internet-of-things, embedded systems and robotics are thus shared between the two subjects.

Computer science is also related to information systems, and the border between the two subjects is not sharp. In computer science, the information technology is usually studied from a scientific or an engineering perspective, typically with a focus on the computer system itself. Information systems, on the other hand, mainly uses methods from social science while emphasizing the business context and processes around the IT systems.

Studies in computer science grants knowledge about, e.g., the theoretical underpinnings of computer science, their implementations in computer systems, methods for software development, and methods for evaluating systems and other deliverables. The student develops skills in analyzing problems, systems, and data, in designing and programming tools and systems, in evaluating technology and its uses, and in doing all of this both independently and in collaboration with others.

At JU, computer science is organized under the discipline Industrial Product Realization. Product realization is defined as including all tasks and activities needed to develop solutions to customer needs, and to realize these solutions through physical products and associated services. Research and education in this discipline can focus on specific parts of the product realization process or apply a holistic perspective. Industrial product realization is characterized by customer adaptation, standardization, flexible production, and automation. The process often includes market- and customer analyses, structured requirements elicitation and management, analyses of production processes and materials, optimization of components, systems, and logistics flows, and development of product lifecycle support services (including usage analyses supporting maintenance, product development, and product recycling). Research and education in computer science support these tasks by way of methods and techniques for scalable data analysis, systems development, and intelligent embedded digital solutions.

Background

Cybersecurity breaches are heavily affecting our society, and the protection of assets has become big business. We see cybersecurity-related issues daily in the news, such as ransomware attacks, identity theft and data breaches. In recent years, we have seen more financially-motivated adversaries and state-sponsored attacks, making it an uneven playing field, especially for smaller organisations with limited resources. Cybersecurity is considered a horizontal market which implies it cuts through vertical sectors, such as manufacturing, automotive, banking, education, healthcare, retail, and more. This means there is a need to protect assets virtually anywhere in society. One prime example is the manufacturing sector which has its aim set at Industry 5.0, where the common theme is digitalisation, connectivity, and automation. With such transformation comes increased dependency on hardware and software that controls and monitors industrial equipment, Operational Technology (OT). Such OT is at the core of production, and their functioning is critical to operation. To fully leverage OT, such systems are often connected to networks and have humans in the loop. With the introduction of OT comes a new range of challenges connected to cybersecurity.

The increased focus and need for cybersecurity solutions have created significant demand for skilled professionals.

This master's programme in cybersecurity helps students acquire the skills required to take on the challenge of protecting our society.

Objectives

The programme is intended for students with a bachelor's degree in computer science, computer engineering, informatics, information systems or similar. By introducing students to core technologies and concepts in the field, the programme will help them understand, use and implement solutions that address cybersecurity-related issues.

The programme aims to provide knowledge that enhances the skills and abilities of students with different IT-related backgrounds by providing broad cybersecurity skills and the possibility to select a focus in several courses that align with personal interests or backgrounds.

Post-graduation employment areas

This master's programme in cybersecurity prepares students for third-cycle courses and research projects or work in the industry. With the experience provided by the programme, students will be able to undertake a variety of roles, such as cybersecurity specialist, cybersecurity engineer, cybersecurity manager, or cybersecurity consultant.

Post-graduation studies

A Master's degree qualifies to apply for further third-cycle education leading to a licentiate or doctoral degree.

Objectives

General learning outcomes

On completion of the programme, the student must fulfil the learning outcomes for the degree of master (60 credits) as laid down in the Higher Education Ordinance:

Knowledge and understanding

1. demonstrate knowledge and understanding in the main field of study, including both an overview of the field and specialised knowledge in certain areas of the field as well as insight into current research and development work, and
2. demonstrate specialised methodological knowledge in the main field of study.

Competence and skills

3. demonstrate the ability to integrate knowledge and analyse, assess and deal with complex phenomena,

issues and situations even with limited information,
4. demonstrate the ability to identify and formulate issues autonomously as well as to plan and, using appropriate methods, undertake advanced tasks within predetermined time frames,
5. demonstrate the ability in speech and writing to report clearly and discuss his or her conclusions and the knowledge and arguments on which they are based in dialogue with different audiences, and
6. demonstrate the skills required for participation in research and development work or employment in some other qualified capacity.

Judgement and approach
7. demonstrate the ability to make assessments in the main field of study informed by relevant disciplinary, social and ethical issues and also to demonstrate awareness of ethical aspects of research and development work,
8. demonstrate insight into the possibilities and limitations of research, its role in society and the responsibility of the individual for how it is used, and
9. demonstrate the ability to identify the personal need for further knowledge and take responsibility for his or her ongoing learning.

Programme-specific learning outcomes
On completion of the programme, the student must also fulfil the following programme-specific learning outcomes:

Knowledge and understanding
10. display knowledge of the area of cybersecurity and its related subject areas, and
11. display knowledge of the definitions, terminology, and concepts of cybersecurity.

Competence and skills
12. demonstrate skills in using tools for penetration testing and cybersecurity operations, and
13. demonstrate the ability to create risk and privacy impact assessments.

Judgement and approach
14. demonstrate an insight into the societal, legal and ethical aspects of cybersecurity operations, and
15. demonstrate the ability to suggest risk-based security controls to counter threats and vulnerabilities.

Contents

Programme principles
Instruction is in the form of lectures, seminars, exercises, laboratory sessions and project work. All courses are held in English. All final course examinations are in English.

The teaching approach in the programme is based, to a large extent, on learning from real-life scenarios and group learning. Lectures and labs often include examples from real projects, which put the theoretical material into a practical context. In course assignments, students work in groups to plan and implement a solution to a problem based on a real-life case. The resulting solution is reported in both written and oral form. This lays the ground for learning communication and leadership within a group.

The programme includes an independent degree project worth 15 higher education credits. Students, individually or in groups of two, prepare and present an assignment in cybersecurity, applying the knowledge accumulated during the programme and demonstrating the acquired skills. The degree project is carried out during the last term of the programme and can be done in close collaboration with a company or an organisation.

Research basis
Within the Department of Computer Science & Informatics, there is a strong focus on research related to cybersecurity. Cybersecurity is a topic that affects all sectors of society. Here, the focus is especially on cybersecurity and privacy in the industrial and public sectors, where most of the cybersecurity research in the department is conducted. Furthermore, there is a particular focus on human aspects among the staff where contributions on, for example, awareness, management, usable security and social engineering have been made.

Cybersecurity is a multi- and interdisciplinary field of study that draws on principles from different subjects, such as computing (e.g., artificial intelligence, privacy, software development), social sciences (e.g., psychology, ethics, economy), and many more.

The programme is also closely connected to the thematic areas of Jönköping University's SPARK Research Environment, especially to the sub-environments 1 (Integrated Product and Production Development for Sustainability and Resilience) and 3 (Human-Centered Industrial AI). In these sub-environments are the core areas of digitalisation and digital transformation of products and services, all utterly dependent on cybersecurity. This also makes cybersecurity a foundation to facilitate research between schools and departments, the industry and the public sector.

Equal terms, gender equality and diversity

The School of Engineering (JTH) strives in all its activities to ensure that all individuals are given equal opportunities and treated equally. At both the JU and JTH levels, this is reflected in governing documents concerning organizational and personnel matters, the establishment and delivery of programmes and courses, as well as the monitoring of educational quality. At JTH, student influence is also ensured through student representation in various educational and industry councils.

Courses in the programme that address gender equality aspects include *Digital Ethics and Privacy* (7.5 credits), *Ethical Hacking and Penetration Testing* (7.5 credits) and *Cybersecurity Operations and Incident Response* (7.5 credits). Gender aspects are considered by identifying and analysing different people's perspectives, conditions and needs.

Programme progression

The course *Cybersecurity Overview* gives a holistic view of cybersecurity and its relation to other subject areas, such as information security and privacy. Also, an overview of general and industry-specific standards and frameworks within the area is given as a frame of reference. Cybersecurity denotes a specific focus on risks and vulnerabilities associated with critical infrastructures and related systems used for connecting them. Hence, a parallel course on*Critical Infrastructure* introduces the fundamentals in that area. More specifically, threats, vulnerabilities and security controls related to industrial control systems (e.g. SCADA and operational technology) and networks (e.g. Industrial Internet of Things).

Following are two courses with two distinct aims, *State-of-the-art and Research Methods in Cybersecurity* and *Ethical Hacking and Penetration Testing*. The concept of red team/blue team is central in *Ethical Hacking and Penetration Testing*, where the focus is on the red team, i.e., focus on offensive aspects of cybersecurity. Such aspects include hacking and penetration testing and the tools and methodologies associated. *State-of-the-art and Research Methods in Cybersecurity* have two main parts. One aims to provide knowledge in state-of-the-art and emerging knowledge areas in cybersecurity. The other aims to introduce quantitative scientific methods in cybersecurity, focusing on descriptive statistics, sampling and survey design and regression analysis. The spring term starts with a course in *Digital Ethics and Privacy* and the *Final Project Work in Computer Science*. *Digital Ethics and Privacy* focuses on legal and societal aspects of cybersecurity with topics including, but not limited to, human values, vulnerabilities, or intersectionality, engaging students in critique-based thinking and analysis. Moreover, the course considers privacy, including legal and professional frameworks (e.g., privacy by design, or privacy impact assessment).

The spring term ends with a *Cybersecurity Operations and Incident Response* course. In this course, there is a focus on the blue team, i.e. the defensive aspects of cybersecurity. Such concepts include network security (including intrusion detection/prevention, firewalls, network admission control, and virtual private networks), standards and frameworks for incident response, digital forensics and digital evidence and monitoring.

During their *Final Project Work*, the students are expected to enhance and deepen their knowledge of modern trends and discoveries in cybersecurity and contribute their own results to this area. The *Final Project Work* requires students to exercise their ability to understand a problem, identify different solutions to the problem, and choose an appropriate solution.

Courses

Course changes can occur, as long as they do not substantially affect the programme’s content and learning goals.

Teaching and examination

The academic year is divided into two semesters, and the semesters into two study periods. In each study period two courses are generally taken in parallel. Assessment is part of each course or module. Modes of assessment and grades are shown in each course syllabus.

Entry requirements

The applicant must hold a minimum of a bachelor's degree (i.e., the equivalent of 180 ECTS credits at an accredited university) with at least 90 credits in Computer Science, Informatics, Information Systems, Computer Engineering, or the equivalent. Proof of English proficiency is required.

Qualification Requirements

To obtain a Degree of Master (60 credits) with a major in Computer Science, specialisation in Cybersecurity, students must complete a minimum of 60 credits in accordance with the current programme syllabus.

In addition, a Degree of Bachelor of Science in Engineering/Degree of Bachelor of Science or an equivalent Swedish or foreign qualification is required.

Quality Development

At JTH, systematic quality assurance is carried out within JU's established quality system. This system, based on the requirements of the Higher Education Act, the Higher Education Ordinance, and the Standards and Guidelines for Quality Assurance in the European Higher Education Area, has been reviewed and approved by the Swedish Higher Education Authority.

Active and continuous course evaluation, including student feedback through course surveys, forms one of the cornerstones of this system. Annual programme evaluations and student representation in JTH's various educational and industry councils are two additional examples.

Other Information

Admission is under ‘Admission regulations for first- and second cycle courses and study programmes at Jönköping University (Admission regulations)’.

This syllabus is based on ‘Regulations and guidelines for first-, second- and third-cycle education at Jönköping University’.