DD2510 Cybersecurity in a Socio-Technical Context 7.5 credits

Cybersäkerhet i sociotekniskt sammanhang

This is a translation of the Swedish, legally binding, course syllabus.

If the course is discontinued, students may request to be examined during the following two academic years

Establishment

This official course syllabus is valid from the autumn semester 2022 in accordance with decision by the head of school: J-2021-1998.Decision date: 14/10/2021

Grading scale

A, B, C, D, E, FX, F

Education cycle

Second cycle

Main field of study

Computer Science and Engineering

Specific prerequisites

Knowledge in computer security, 6 higher education credits, equivalent to completed course DD2391/DD2395.

Active participation in a course offering where the final examination is not yet reported in LADOK is considered equivalent to completion of the course.

Being registered for a course counts as active participation.

The term 'final examination' encompasses both the regular examination and the first re-examination.

Language of instruction

The language of instruction is specified in the course offering information in the course catalogue.

Intended learning outcomes

After passing the course, the student shall be able to

- describe fundamental legislation in the cybersecurity area and in a broad stroke describe how this legislation should be interpreted in different scenarios
- describe different types of threat actors and the threats that they direct against different types of digital systems
- describe and analyse commonly occurring work processes for development and administration of secure digital systems and relate this to diversity, gender equality, equal rights and ethical aspects
- describe and analyse how individuals and organisations constitute attack surfaces and potential security vulnerabilities in digital systems and relate this to diversity, gender equality, equal rights and ethical aspects

in order to

- understand and be able to convey the importance of cybersecurity in society
- create and be able to maintain a good understanding of how the properties of threat actors influence how secure digital systems should be created
- understand and be able to identify the balance between technical and non-technical properties to create secure digital systems
- facilitate action within the boundaries of the law.

Course contents

This course intends to give an introduction and overview of how technical and non-technical aspects of cybersecurity influence one another. The course concerns the actors that influence, how cybersecurity is designed in digital systems. Human use of digital systems can in many ways be considered as a part of the system itself and has a clear impact on the security of the system. People and their actions form both the basis for the threats to which digital systems are exposed, and how we choose to defend these systems. This action is also influenced by the laws of the society.

The course consists of four separate modules that cover these different actors and their relation to cybersecurity :

1. legal aspects
2. threat actors
3. processes and organisation
4. vulnerabilities in the use of systems

Examination

- UPP1 - Oral and written assignments, 2.0 credits, grading scale: A, B, C, D, E, FX, F
- UPP2 - Oral and written assignments, 2.0 credits, grading scale: A, B, C, D, E, FX, F
- UPP3 - Oral and written assignments, 2.0 credits, grading scale: A, B, C, D, E, FX, F
- UPP4 - Oral and written assignments, 1.5 credits, grading scale: A, B, C, D, E, FX, F

Based on recommendation from KTH's coordinator for disabilities, the examiner will decide how to adapt an examination for students with documented disability.

The examiner may apply another examination format when re-examining individual students.

Other requirements for final grade

Active participation in all compulsory activities.

Ethical approach

- All members of a group are responsible for the group's work.
- In any assessment, every student shall honestly disclose any help received and sources used.
- In an oral assessment, every student shall be able to present and answer questions about the entire assignment and solution.