DD2391 Cybersecurity Overview 7.5 credits

Cybersäkerhet översiktskurs

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

The official course syllabus is valid from the autumn semester 2022 in accordance with the decision from the head of school: J-2021-2008.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 and skills in programming, 5 credits, equivalent to completed course DD1337/DD1310-DD1318/DD1321/DD1331/DD100N/ID1018.

Knowledge in foundations of computer science, 6 credits, equivalent to DD1320-DD1327/DD1338/ID1020/ID1021.

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

- identify threats against confidentiality, integrity and availability in digital systems
- explain basic terminology and concepts in computer security and use them
- find and use documentation of security related problems and tools
- analyse simple program code and systems (based on given or self-made system descriptions) to identify vulnerabilities and predict corresponding threats
- select countermeasures against identified threats and argue for their suitability
- compare countermeasures and evaluate their side effects,
- apply countermeasures
- present and explain their reasoning to others,

in order to

- be able to develop software and computer systems with security in mind
- be able to move on and specialise in the cybersecurity area
- assess the difficulty of a security problem in relation to their own ability to decide when they can handle it alone and when they need to consult an expert.

Course contents

- introduction to computer security
- introduction to cryptography
- authentication, access control, security models
- intrusion detection, firewalls
- malware: virus/worms/troyans
- web attacks
- system security, buffer overflow attacks, side channels
- human factors, security audits, and social manipulation
- selected current security related problems and technologies

Examination

- LAB1 - Laboratory work, 3.0 credits, grading scale: P, F
- PRO1 - Project work, 1.5 credits, grading scale: P, F

- TEN1 - Written exam, 3.0 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.

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.