DD2395 Computer Security 6.0 credits

Datasäkerhet

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

Establishment

On 04/21/2020, the Head of the EECS School has decided to establish this official course syllabus to apply from autumn semester 2020, registration number: J-2020-0603.

Grading scale

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

Education cycle

Second cycle

Main field of study

Computer Science and Engineering

Specific prerequisites

Completed courses in programming equivalent to DD1310/DD1311/DD1312/DD1314/DD1315/DD1316/DD1318/DD1331/DD1337/DD100N/ID1018 and computer science equivalent to DD1338/DD1320/DD1321/DD1325/DD1327/ID1020.

Active participation in a course offering where the final examination is not yet reported in LADOK is considered equivalent to completion of the course. This applies only to students who are first-time registered for the prerequisite course offering or have both that and the applied for course offering in their individual study plan.

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 should be able to

- identify threats against confidentiality, integrity and availability in system
- 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 system descriptions to identify vulnerabilities and predict their corresponding threats
- select countermeasures against identified threats and argue for their applicability
- compare countermeasures and evaluate their side effects,
- present and explain their reasoning to others,

in order to

- be able to develop software and computer system with security in mind
- if interested, be able to move on and specialise in computer and network security.

Course contents

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

Examination

- TEN1 - Examination, 3.0 credits, grading scale: A, B, C, D, E, FX, F
- LAB1 - Laboratory Work, 3.0 credits, grading scale: P, 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.

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

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.