IV1013 Introduction to Computer Security 7.5 credits

Introduktion till datasäkerhet

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

Course syllabus for IV1013 valid from Spring 2024

Grading scale

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

Education cycle

First cycle

Main field of study

Technology

Specific prerequisites

Knowledge and skills in Java programming, 6 credits, corresponding to completed course ID1018/DD1337 or alternatively a completed course in basic programming such as DD1310-DD1319/DD1321/DD1331/DD100N combined with a completed course in Java programming corresponding to DD1380.

Knowledge of low-level programming, 6 credits, corresponding to completed course IS1200/IS1500/EP1200.

Knowledge in networks and communication, 6 credits, corresponding to completed course IK1203/EP1100.

Knowledge in discrete mathematics, 6 credits, corresponding to completed course IX1500/SF1610/SF1630/SF1662/SF1679/SF1688.

Active participation in a course offering where the final examination is not yet reported in Ladok is considered equivalent to completion of the course. Registering for a course is counted 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 should be able to

- explain basic mechanisms in, and the structure of, secure communications protocols
- describe weaknesses in computer systems, software, networks, and communications protocols as well as explain attacks that utilise such weaknesses
- explain and compare advantages and disadvantages with common cryptographic technologies
- design and implement simple cryptographic applications
- account for and recognise threats against information security: confidentiality, integrity, and availability. as well as choose appropriate methods to protect against threats
- design, implement, and evaluate security in networks

in order to receive an introduction to the basics of cryptography, security in computer systems and network security.

Course contents

- Basic cryptography: symmetric and asymmetric cryptography.
- Cryptographic hashing and digital signatures.
- Security in protocols and services of the Internet.
- Certificates and infrastructures for open key encryption.
- Security in network systems: routers, firewalls, and systems to detect intrusion.
- Security in operating systems.
- Software security: vulnerability, attacks, and defence mechanisms.

Examination

- PRO1 - Project Assignment, 6.0 credits, grading scale: A, B, C, D, E, FX, F
- TENT - Digital examination, 1.5 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.

TENT is carried out as continuous, digital examination and is given in English. Solutions may be given in Swedish or English.

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.