DD238U Computer Security 7.5 credits

Datasäkerhet

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

Establishment

Course syllabus for DD238U valid from Spring 2022

Grading scale

P, F

Education cycle

Second cycle

Main field of study

Computer Science and Engineering

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.

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
- KON1 - Partial exam, 3.0 credits, grading scale: P, F
- LAB1 - Laboratory work, 4.5 credits, grading scale: P, F

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.