EP2790 Security Analysis of Large-Scale Computer Systems 7.5 credits

Säkerhetsanalys av storskaliga datorsystem

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

Establishment

The course syllabus is valid from autumn 2025 according to faculty board decision: HS-2025-2310.

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 DD1310-DD1318/DD1331/DD1337/DD100N/ID1018.

Knowledge in cybersecurity, 6 credits, equivalent to completed course DD2391/DD2395/IK2206/IV1013
or

knowledge and skills in ethical hacking, 7,5 credits, equivalent to completed course EN2720
or
knowledge in secure network systems, 7,5 credits, equivalent to completed course EP2500/EP2520.

Intended learning outcomes

After passing the course, the student should be able to

- model in detail the architectures of large-scale computer systems (including software, networks, etc.)
- carefully and well balanced describe and evaluate threats and attacks in large-scale computer systems
- clearly describe defense mechanisms for computer systems and how these relate to vulnerabilities and attacks
- carry out qualified and well balanced risk analyses based on system models
- in a professional manner report and present models, a cybersecurity risk analysis, and defense strategies for a computer system

in order to

- understand and explain which threats a specific system can have
- understand and explain how attacks work and propagate through a system architecture
- argue why certain risks should be prioritised
- choose an effective defense to decrease risk.

Course contents

This course teaches a threat modeling-based method for analyzing cybersecurity risks for systems-of-systems. It includes developing and combining models for computer system resilience, threat actor capabilities, and business impacts of realized threats into an overall cyber risk assessment. Moreover the course addresses how cyber risk analysis is used for identifying and arguing for cost efficient defense mechanism selection for protecting the analyzed system-of-systems.

Examination

- PRO1 - Project work, 6.0 credits, grading scale: A, B, C, D, E, FX, F
- SEM1 - Seminars, 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.

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.