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

Course syllabus for EP2790 valid from Autumn 2019

Grading scale

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

Education cycle

Second cycle

Main field of study

Computer Science and Engineering

Specific prerequisites

Completed course in Programming equivalent DD1315 Programming technique and Matlab, DD1316 Programming technique, C, DD1337 Programming and ID1018 programming I or the equivalent.

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 students should be able to:

- model threats in large-scale computer systems (including software, networks etc),
- simulate attacks in large-scale computer systems
- carry out risk analysis based on a model and simulation
- describe which defence mechanisms computer system can have
- report and present models, simulation, risk analysis, and defense strategy for a given 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 the right defence to decrease risk.

Course contents

Companies today have thousands of software based computer systems that all are depending on one another in a large complex network, a system-of-systems. That IT attacks succeed to a large extent due to this complexity. A company needs to understand the whole system while an attacker only needs find one way in. At the same time, there is a large set of attack types that are utilised and plenty of proposed defence mechanisms. This course main content aims to develop students' understanding of:

- the complex IT landscape of today by creating models of such.
- which attacks that are utilised today to cause harm and how these can propagate through a large network.
- what defences there are and when they are best suited against different attack types.
- how risk can be calculated and used to prioritise security work.

Course literature

Information about the course literature will be announced in the course memo.

Equipment

Own computer.

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.

Other requirements for final grade

The examiner decides, in consultation with KTH's coordinator for disabilities (Funka), about possible adapted examination for students with documented, permanent disabilities. The examiner may permit other examination format for re-examination of 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.