DD2460 Software Safety and Security 7.5 credits

Programvarusäkerhet

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

Establishment

Course syllabus for DD2460 valid from Autumn 2017

Grading scale

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

Education cycle

Second cycle

Main field of study

Computer Science and Engineering

Specific prerequisites

Single course student:

SF1604 Linear algebra, SF1625 Calculus in one variable, SF1901 Probability theory and statistics, DD1337 Programming, DD1338 Algorithms and Data Structures, SF1630 Discrete Mathematics, DD1352 Algorithms, Data Structures and Complexity, DD2395 Computer Security or corresponding courses

Language of instruction

The language of instruction is specified in the course offering information in the course catalogue.

Intended learning outcomes

After the course the successful student will be able to:

- reason abstractly about safety and security aspects of programs
- use various logics and type systems to specify important safety and security properties of programs
- apply runtime monitoring for enforcing temporal safety properties
- apply various techniques and tools for checking properties
- argue for the soundness of these techniques.

Course contents

- Part I. Security automata and runtime monitoring: security automata, enforcing temporal safety properties, runtime monitoring, monitor inlining.
- Part II. Hoare logic and program correctness: Hoare logic, formal specification of program correctness, verification condition generation.
- Part III. Temporal logic and behavioural correctness: Linear temporal logic, formal specification of behavioural correctness, Büchi automata, model checking.
- Part IV. Information flow analysis and security: information flow analysis, type systems.

Course literature

Michael Huth and Mark Ryan "Logic in Computer Science", Cambridge University Press 2004 (andra utgåven), ISBN 052154310X.

Examination

- INL1 - Hand-in Assignments, 5.0 credits, grading scale: A, B, C, D, E, FX, F
- LAB1 - Laboratory Work, 2.5 credits, grading scale: A, B, C, D, E, FX, 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.

INL1, Hand-in Assignments, grade scale used: A, B, C, D, E, F.
LAB1, Laboratory Work, grade scale used: C, D, E, 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.