IL1333 Hardware Security 7.5 credits

Hårdvarusäkerhet

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

Establishment

Course syllabus for IL1333 valid from Spring 2023.

Grading scale

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

Education cycle

First cycle

Main field of study

Technology

Specific prerequisites

Knowledge in digital design, 6 credits, corresponding to completed course IE1204/IE1205.

Language of instruction

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

Intended learning outcomes

Having passed the course, the student shall be able to

- describe state-of-the-art hardware security techniques and justify their applications and limitations
- describe how the safety is guaranteed in an illustrating application
- describe the threats against a system from hardware perspective and available counter-measures and apply the knowledge to choose an appropriate set of countermeasures for a certain threat assessment.
- analyse and make a critical balance between the performance, cost and safety of the system and illustrate compromises that are available for design engineers of electronic and embedded systems
- explain the need of hardware security primitives and justify advantages and disadvantages with the different primitives and choose an appropriate primitive for a specific application
- use the knowledge to build a small electronic or embedded system for increased safety and explain how the safety is guaranteed in the system.

Course contents

- Physical attacks and "tamper resistance"
- Side-channel attacks and countermeasures
- Introduction to lightweight cryptography
- Security for smart card and radio frequency identification tags (RFID-tags)
- Design for physical unclonable functions (PUFs) and true random number generators
- Personal integrity in the Internet-of-Things era

Examination

- LABA - Laboratory work, 2.5 credits, grading scale: P, F
- PROA - Project, 1.0 credits, grading scale: P, F
- TENA - Written exam, 4.0 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.

Transitional regulations

Students who have taken but not completed the course are offered to complete those missing course components.

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.