FIL3030 Hardware Security 7.5 credits

Hårdvarusäkerhet

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

If the course is discontinued, students may request to be examined during the following two academic years

Establishment

Course syllabus for FIL3030 valid from Spring 2019

Grading scale

P, F

Education cycle

Third cycle

Specific prerequisites

Admitted as doctoral student.

Language of instruction

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

Intended learning outcomes

The aim of this course is to give doctoral students knowledge necessary to develop secure systems. In the era of the Internet-of-Things (IoT) in which physical devices such as sensors and RFID tags are integrated with electronics to provide capabilities of sensing, computing and communication, assuring security of such systems becomes a great challenge. In order to tackle this problem, industry is making efforts across multiple layers involving cryptographic algorithms, protocols, secure integrated circuits, hardware architecture, etc. From the academic side, we have the responsibility to educate and prepare our students - the future engineers, for the security challenges of the IoT era. Specifically, in this course, we aim to make the students aware of potential hardware vulnerabilities and to give them the necessary knowledge and skills required for building trustworthy hardware.

Upon completion, students will be able to:

- Describe state-of-the-art hardware security techniques. Justify their targeted applications and limitations. Describe how security is assured in an exemplary application.
- Describe the threats to a system from the hardware perspective as well as available countermeasures. Apply the knowledge to select a suitable set of countermeasures for a specific threat scenario.
- Analyze and critically assess trade-offs between system performance, cost, and security. Exemplify some of the trade-offs that are available to designers of electronic and embedded systems.
- Explain the need for hardware security primitives. Justify pros and cons of different primitives and select a suitable one for a specific application.
- Apply the knowledge to design a small electronic or embedded system with enhanced security in a group project. Explain how the security is assured in the system.

Course contents

The following is a list of topics to be covered:

- Physical Attacks and Tamper Resistance.
- Side Channel Attacks and Countermeasures.
- Introduction to Lightweight Cryptography.
- Security of Smartcards and Radio-Frequency IDentification (RFID) Tags.
- Design of Physical Unclonable Functions (PUFs) and True Random Number -Generators (TRNGs).
- Personal integrity in the IoT era.

Disposition

The course consists of 12 2-hour lectures, two 4-hour labs, and one group project.

Course literature

M. Tehranipoor and C. Wang. Introduction to Hardware Security and Trust. Springer, 2012.

Equipment

None

Examination

- EXA1 - Examination, 7.5 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.

In the examination part, the following is included:

- two labs (20%, grade pass/fail), 1.5 hp
- a final exam (40%, grade A, B, C, D, E, FX, F), 3 hp
- a forskningsproject and its presentation (40%, grade pass/fail), 3 hp

Other requirements for final grade

To pass, all bullets listed in the examination should be completed.

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.