

Information Security, Second Course

Programme course

6 credits

Informationssäkerhet, fk

TDDD17

Valid from: 2017 Spring semester

Determined by

Board of Studies for Computer Science
and Media Technology

Date determined

2017-01-25

Main field of study

Information Technology, Computer Science and Engineering, Computer Science

Course level

Second cycle

Advancement level

A1X

Course offered for

- Computer Science and Engineering, M Sc in Engineering
- Industrial Engineering and Management - International, M Sc in Engineering
- Industrial Engineering and Management, M Sc in Engineering
- Computer Science, Master's programme
- Information Technology, M Sc in Engineering
- Computer Science and Software Engineering, M Sc in Engineering

Entry requirements

Note: Admission requirements for non-programme students usually also include admission requirements for the programme and threshold requirements for progression within the programme, or corresponding.

Prerequisites

Basic course in computer security. Basic understanding of operating system concepts and TCP/IP networks is recommended. Students are expected to be able to produce written reports of high quality.

Intended learning outcomes

The course provides deeper studies in selected topics in the area of information security. After passing the course, a student should be able to:

- General goals:
 - Explain and use the security terminology and security principles presented at the course.
 - Identify and explain in detail the security threats against a certain system, in a given context; identify vulnerabilities of systems, and formulate security requirements.
 - Analyze and structure a given security problem.
 - Find, evaluate, and explain in detail solutions to security problems, in general and in specific contexts.
 - Synthesize partial solutions towards addressing given security problems.
 - Generalize and synthesize information from multiple types of sources in the information security area to find structure, internal and external connections, and draw original and well-motivated conclusions.
 - Map abstract concepts and models to real security problems and mechanisms, and vice versa.
- Project specific goals:
 - Identify, motivate, analyze, and structure the problems to be addressed in the project.
 - Find, evaluate, and explain solutions to problems identified in the project.
 - Use and understand the equipment (hardware and software) needed to perform the project. Apply existing security tools to address a given problem, and develop new tools and mechanisms.
 - Find, synthesize, and present information from multiple types of sources in the information security area to find structure, internal and external connections, and make original and well-motivated conclusions.
 - Present project results to an audience with similar general background in information security.
 - Plan, follow up, and document the project work.

Course content

- Part 1: This part deals with theory and is based on lectures and a literature study. The detailed contents can vary from year to year based on the current research in the field and the ongoing research at LiU. Topics may include: security mechanisms for modern communication systems (e.g. fingerprinting and watermarking), network security (e.g. security in IEEE 802.11), system and software integrity (e.g. covert channels, buffer overflow, and viruses), modern identification and authentication mechanisms (e.g. biometric authentication), security standards (e.g. Common Criteria) and analysis methodologies (e.g. Fault Tree Analysis), and standards and common implementations in the field (e.g. access control in Radio Access Networks).
- Part 2: In this part students will perform projects, which can be of theoretical or practical nature. The subjects of the projects will be from the topics studied in part 1 or other topics within the field.

Teaching and working methods

The course consists of two parts, an overview part and an individual deeper studies part. The overview consists mainly of lectures and a study of literature. The deeper studies consist of a project in a sub-field of information security. For the project, students will work in teams. The course runs over the entire spring semester.

Examination

LAB2 Laboratory work and written assignments	1 credits U, G
UPG2 Written report. Ends with a common seminar day.	2 credits U, G
TEN2 Written examination	3 credits U, 3, 4, 5

LAB1 gives bonus points on TEN1 during the same year

Grades

Four-grade scale, LiU, U, 3, 4, 5

Department

Institutionen för datavetenskap

Director of Studies or equivalent

Patrick Lambrix

Examiner

Nahid Shahmehri

Course website and other links

<http://www.ida.liu.se/~TDDD17/>

Education components

Preliminary scheduled hours: 55 h

Recommended self-study hours: 105 h

Course literature

M. Bishop, "Computer Security: Art and Science" samt artikelsamling (se kurshemsidan).

Common rules

Regulations (apply to LiU in its entirety)

The university is a government agency whose operations are regulated by legislation and ordinances, which include the Higher Education Act and the Higher Education Ordinance. In addition to legislation and ordinances, operations are subject to several policy documents. The Linköping University rule book collects currently valid decisions of a regulatory nature taken by the university board, the vice-chancellor and faculty/department boards.

LiU's rule book for education at first-cycle and second-cycle levels is available at http://stydokument.liu.se/Regelsamling/Innehall/Utbildning_pa_grund-_och_avancerad_niva.