Computer Security

Programme course

6 credits

Datasäkerhet

TSIT02

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
First cycle

Advancement level
G2F

Course offered for
- Computer Science, Master's Programme
- Mathematics, Master's Programme
- Mathematics
- 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
- Information Technology, M Sc in Engineering
- Computer Science and Software Engineering, M Sc in Engineering
- Applied Physics and Electrical Engineering - International, M Sc in Engineering
- Applied Physics and Electrical 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
At least one course in basic computer science, and some knowledge on operating systems and computer communications.

Intended learning outcomes

After completing the course the student should be able to describe safety issues arising from the use of computers and modern network technologies, and the opportunities to protection available today. This means that after completing this course the student is expected to be able to:

- Describe the principles and possibilities of how security can be built into computers and networks, both at the component and system level
- Explain the concept that confidentiality, integrity and availability (CIA) of information and its use in data security
- Describe the common security protocols in network communications
- Describe the usual models of access control and user authentication
- Describe the use of cryptography-based tools

Course content

Structure and terminology of the subject. Authentication of user identity. Theory and practice for access control. Formal security models. Cryptology and its use in security tools. Security problems, tools, protocols and solutions in networks and distributed systems. Security in specific systems such as databases. Security management.

Teaching and working methods

The course consists of lectures, seminars and laboratory work.

Examination

LAB1	Laboratory work	1 credits	U, G
TEN1	Written examination	5 credits	U, 3, 4, 5

Grades

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

Department

Institutionen för systemteknik

Director of Studies or equivalent

Klas Nordberg

Examiner

Guilherme B. Xavier

Course website and other links

http://www.icg.isy.liu.se/courses/tsit02/

Education components

Preliminary scheduled hours: 28 h
Recommended self-study hours: 132 h

Course literature

Additional literature

Books

Ross Anderson, (2008) *Security Engineering* 2nd ed Wiley

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://styrdokument.liu.se/Regelsamling/Innehall/Utbildning_pa_grund-_och_avancerad_niva.