LINKÖPINGS UNIVERSITET

Software Security

Programme course

6 credits

Software Security

TDDC90

Valid from:

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
- Information Technology, M Sc in Engineering
- Computer Science and Software 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

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 security. Students are expected to have knowledge of operating systems, programming languages, and software engineering. Students should be able to develop, test and debug software in a Unix or Linux environments. Some experience with C-programming as well as basic knowledge of web application development are recommended.

Intended learning outcomes

Students taking this course will learn about the issues underlying software security, and develop the skills needed to build secure software. The course covers methods, tools, and best practices for building secure software. Students completing this course should be able to:

- identify and analyze security problems in software;
- formulate security requirements for software;
- devise, evaluate, and explain solutions to software security;
- critically evaluate the effectiveness of methods, state-of-art tools, and best practices, for detecting and preventing vulnerabilities; and
- design and write secure software.

Course content

The course covers:

- vulnerability discovery and analysis, and supporting tools;
- analysis of infamous vulnerabilities and their exploits;
- attack and vulnerability modeling;
- security requirements analysis and design for security;
- principles for secure programming;
- static and dynamic intrusion prevention mechanisms;
- security testing and evaluation; and
- systematic approaches to building secure software.

Vulnerabilities, attacks, and principles for secure programming are studied with an emphasis on programs written in C/C++ and web applications.

Teaching and working methods

The course consists of lectures and laboratory work.

Examination

UPG1	Laboratory work and assignments	3 credits	U, G
TEN1	Written examination	3 credits	U, 3, 4, 5

Grades

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

Department

Institutionen för datavetenskap

Director of Studies or equivalent

Patrick Lambrix

Examiner

Nahid Shahmehri

Education components

Preliminary scheduled hours: 34 h
Recommended self-study hours: 126 h

Course literature

Additional literature

Other
Articles (see the course home page).

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.