

Software Security

Software Security
6 credits

Programme course

TDDC90

Valid from: 2024 Spring semester

Determined by	Main field of study	
Board of Studies for Computer Science and Media Technology	Information Technology, Computer Science and Engineering, Computer Science	
Date determined	Course level	Progressive specialisation
2023-08-31	Second cycle	A1X
Revised by	Disciplinary domain	
	Technology	
Revision date	Subject group	
	Informatics/Computer and Systems Sciences	
Offered first time	Offered for the last time	
Autumn semester 2007		
Department	Replaced by	
Institutionen för datavetenskap		

Course offered for

- Master of Science in Computer Science and Engineering
- Master of Science in Industrial Engineering and Management
- Master of Science in Information Technology
- Master of Science in Computer Science and Software Engineering
- Master of Science in Industrial Engineering and Management - International
- Master's Programme in Computer Science
- Master's Programme in Cybersecurity

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 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

Other information

About teaching and examination language

The teaching language is presented in the Overview tab for each course. The examination language relates to the teaching language as follows:

- If teaching language is “Swedish”, the course as a whole could be given in Swedish, or partly in English. Examination language is Swedish, but parts of the examination can be in English.
- If teaching language is “English”, the course as a whole is taught in English. Examination language is English.
- If teaching language is “Swedish/English”, the course as a whole will be taught in English if students without prior knowledge of the Swedish language participate. Examination language is Swedish or English depending on teaching language.

Other

The course is conducted in such a way that there are equal opportunities with regard to sex, transgender identity or expression, ethnicity, religion or other belief, disability, sexual orientation and age.

The planning and implementation of a course should correspond to the course syllabus. The course evaluation should therefore be conducted with the course syllabus as a starting point.

The course is campus-based at the location specified for the course, unless otherwise stated under “Teaching and working methods”. Please note, in a campus-based course occasional remote sessions could be included.

Common rules

Plagiarism

For examinations that involve the writing of reports, in cases in which it can be assumed that the student has had access to other sources (such as during project work, writing essays, etc.), the material submitted must be prepared in accordance with principles for acceptable practice when referring to sources (references or quotations for which the source is specified) when the text, images, ideas, data, etc. of other people are used. It is also to be made clear whether the author has reused his or her own text, images, ideas, data, etc. from previous examinations, such as degree projects, project reports, etc. (this is sometimes known as “self-plagiarism”).

A failure to specify such sources may be regarded as attempted deception during examination.

Attempts to cheat

In the event of a suspected attempt by a student to cheat during an examination, or when study performance is to be assessed as specified in Chapter 10 of the Higher Education Ordinance, the examiner is to report this to the disciplinary board of the university. Possible consequences for the student are suspension from study and a formal warning. More information is available at [Cheating, deception and plagiarism](#).

Linköping University has also produced a guide for teachers and students' use of generative AI in education (Dnr LiU-2023-02660). As a student, you are always expected to gain knowledge of what applies to each course (including the degree project). In general, clarity to where and how generative AI has been used is important.

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 <https://styrdokument.liu.se/Regelsamling/Innehall>.