



COURSE SYLLABUS

Säkerhet och mjukvaruutveckling Security in Software Engineering 4 credits (4 högskolepoäng)

Course code: PA1468

Main field of study: Software Engineering

Disciplinary domain: Technology

Education level: First cycle

Specialization: GIF - First cycle, has less than 60 credits
in first cycle course/s as entry requirements

Language of instruction: English

Applies from: 2022-01-17

Approved: 2021-09-01

1. Decision

This course is established by Dean 2018-05-22. The course syllabus is approved by Head of Department of Software Engineering 2021-09-01 and applies from 2022-01-17.

2. Entry requirements

Admission to the course requires 12 credits completed from courses in programming and completed course Object-oriented Design, 6 credits and taken the course Software Architecture and Quality, 6 credits.

3. Objective and content

3.1 Objective

The purpose of this course is to introduce security practices that can be applied to the software development process.

3.2 Content

This course explains the base cybersecurity concepts related to the software development process. It covers security practices, methods, tools, threat models and processes that will help to improve the quality of software products in terms of cyber security. You will learn some useful hands-on approaches to guarantee security during the software development lifecycle (SDLC) at the following stages: requirements gathering, design, implementation, test and integration, deployment, maintenance, and incident response. The security practices include trade-off analysis, threat modeling, static and dynamic application security, as well as penetration testing and incident response.

4. Learning outcomes

The following learning outcomes are examined in the course:

4.1 Knowledge and understanding

On completion of the course, the student will be able to:

- Account for the understanding of security aspects in secure software engineering.
- Gain a detailed understanding of security practices in software engineering including methods, tools, threat models and processes.

4.2 Competence and skills

On completion of the course, the student will be able to:

- Understand the security development lifecycle.
- Select appropriate security practices at the given stage of the software development process.

4.3 Judgement and approach

On completion of the course, the student will be able to:

- Evaluate the appropriate security practices, methods, tools, threat models and processes that are presented in the course.

5. Learning activities

The teaching is organised around lectures in campus that will be supplemented with written material, literature, and research literature. The course will have practical exercises to help students build the skills. Throughout the course, communication,

feedback, and discussions with teachers and fellow participants will take place during lectures and through the course's online learning platform.

6. Assessment and grading

Modes of examinations of the course

Code	Module	Credits	Grade
2205	Written assignments 1	2 credits	GU
2215	Written assignment 2	2 credits	GU

The course will be graded A Excellent, B Very good, C Good, D Satisfactory, E Sufficient, FX Fail, supplementation required, F Fail.

The information before a course occasion states the assessment criteria and make explicit in which modes of examination that the learning outcomes are assessed.

An examiner can, after consulting the Disability Advisor at BTH, decide on a customized examination form for a student with a long-term disability to be provided with an examination equivalent to one given to a student who is not disabled.

7. Course evaluation

The course evaluation should be carried out in line with BTH:s course evaluation template and process.

8. Restrictions regarding degree

The course can form part of a degree but not together with another course the content of which, completely or partly corresponds with the contents of this course.

9. Course literature and other materials of instruction

- Ross Anderson. Security Engineering - 3rd edition, 2020 (<https://www.cl.cam.ac.uk/~rja14/book.html>)
- Michael Howard, Steve Lipner. Security Development Lifecycle, 2006.

Materials such as research articles and other course materials, as well as recommendations for additional reading, are provided via the courses' online platform.