



COURSE SYLLABUS

Introduktion till säkerhet för mjukvaruutveckling Introduction to Security in the Software Development Lifecycle 6 credits (6 högskolepoäng)

Course code: PA2585

Main field of study: Software Engineering

Disciplinary domain: Technology

Education level: Advanced level

Specialization: A1N - Second cycle, has only first-cycle course/s as entry requirements

Language of instruction: English.

Applies from: 2021-08-30

Approved: 2021-03-01

1. Decision

This course is established by Dean 2021-02-25. The course syllabus is approved by Head of Department of Software Engineering 2021-03-01 and applies from 2021-08-30.

2. Entry requirements

Admission to the course requires at least 120 completed credits, of which at least 90 credits are in a technical area, and a minimum of 2 years professional experience within an area related to software-intensive product and/or service development (shown by, for example, a work certificate from an employer).

3. Objective and content

3.1 Objective

The purpose of this course is to introduce security practices within the Software Development Lifecycle (SDLC) at the requirements, design, implementation, verification, and after release stages of software development.

This course is the guide to the cybersecurity issues arising throughout the entire development process. We consider the development from the security perspective from the beginning stage until the final release and beyond. The course is adapted to give a solid introduction to non-security-experts mainly and addresses both how professionals (developers, managers, decision-makers) can utilize security to improve (software-based) products/services, and how they are affected by security issues and challenges.

Whether you are a software developer in a bank or telecom company, or you are a product manager in a gaming company, this course will be relevant for you.

3.2 Content

This course covers trade-off analysis, investment decisions into security, requirements selection and prioritization, and risk assessment approaches. The student will learn the hands-on approaches for trade-off analysis, requirements prioritization methods, risk assessment approaches, and other security aspects at all stages of the software development lifecycle (SDLC). By taking security aspects into account as a part of product design and development, the student can use different techniques and methods along with the best practices.

The course consists of the following parts:

- Background to security and its impact on software engineering
- Secure software engineering
- Secure architectures and design
- ROI and trade-offs between security and other quality aspects such as usability
- Risk analysis
- Introduction of infrastructure choices in relation to security

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:

- Discuss security aspects in secure software engineering
- Explain how to apply different methods to achieve security in software engineering, e.g., secure architectures, initial security analysis.

4.2 Competence and skills

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

- Apply frameworks and methods, models and processes that are presented in the course with the purpose of engineering so-called “secure software”.

4.3 Judgement and approach

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

- Evaluate the appropriate applications of the frameworks and methods, models and processes that are presented in the course including the trade-off their application entails.

5. Learning activities

The teaching is organised around online lectures, pre-recorded videos, together with written material, literature, and research literature. Throughout the course, communication, feedback, and discussions with teachers and fellow participants will take place through email and the course’s online learning platform.

6. Assessment and grading

Modes of examinations of the course

| Code | Module | Credits | Grade |
|------|----------------------|-----------|-------|
| 2110 | Written assignment 1 | 2 credits | GU |
| 2120 | Written assignment 2 | 2 credits | GU |
| 2130 | Written assignment 3 | 2 credits | GU |

The course will be graded G Pass, UX Fail, supplementation required, U 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

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

10. Additional information

This course replaces the course PA2582