COURSE SYLLABUS

Säkerhet i mjukvaruintensiv produkt- och tjänsteutveckling - en introduktion
Security in Software-intensive Product and Service Development - an introduction
6 credits (6 högskolepoäng)

Course code: PA2582
Main field of study: Software Engineering, Computer Science
Disciplinary domain: Technology
Education level: Second cycle
Specialization: A1N - Second cycle, has only first cycle course/s as entry requirements

Subject area: Computer Technology
Language of instruction: English
Applies from: 2020-08-31
Approved: 2020-03-01

1. Decision
This course is established by Dean 2020-02-07. The course syllabus is approved by Head of Department of Software Engineering 2020-03-01 and applies from 2020-08-31.

2. Entry requirements
Admission to the course requires at least 120 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 areas of: layers of security, development/operations/technology security, security "built-in", architectural security and patterns, ROI on pre-emptive security, Security risk assessment, privacy in relation to security, usability in relation to security. Experience of programming and design of software-intensive products and services are desirable.

3.2 Content
The student will learn to understand the importance of taking security aspects into account already during the planning and development of software-intensive product and service development. During the course, the student will be familiarized with and get practical experience from different methods to evaluate, plan, and prepare for the so-called "secure software engineering." By taking security aspects into account as a part of product design and development, you can use different techniques and methods such as architectural patterns and good practices. Also included is to understand the different phases and aspects that are influenced by, and where good engineering influences, security – where security has to be seen in the three layers of engineering security, operational security, and technology-based security.
The course consist of the following parts:
• Background to security and its' influences 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
• Introduction to how the choice of technologies and languages influences 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:
• Be able to account for the understanding of security aspects in secure software engineering
• Be able to gain a detailed understanding of how to apply different methods to achieve security in software engineering, e.g., secure architectures)

• Be able to account for how to apply initial security analysis and trade-offs in relation to security in the design and development of software-intensive product and service development

4.2 Competence and skills
On completion of the course, the student will be able to:
• 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:
• Be able to evaluate and assess the appropriate applications of the frameworks and methods, models and processes that are presented in the course including the trade-off its 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
2010	Written assignment 1	2 credits	GU
2020	Written assignment 2	2 credits	GU
2030	Written assignment 3	2 credits	GU

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

The course-PM for each course revision should include 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.