Blekinge Institute of Technology
Department of Software Engineering

Revision: 1
Reg.no: BTH-4.1.14-0941-2023

COURSE SYLLABUS

Säker mjukvaruarkitektur
Secure Software Architecture
6 credits (6 högskolepoäng)

Course code: PA2594
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

Language of instruction: English
Applies from: 2024-01-15
Approved: 2023-09-01

1. Decision
This course is established by Dean 2022-12-06. The course syllabus is approved by Head of Department of Software Engineering 2023-09-01 and applies from 2024-01-15.

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

3. Objective and content

3.1 Objective
The course aims to equip students with a deep understanding of software security architecture principles, enabling them to design, implement, and maintain secure software systems. By the end of the course, students will possess the knowledge and skills to identify security risks, employ industry-standard security practices, and create robust software architectures that safeguard against a wide range of threats.

3.2 Content
The course covers fundamental principles of software security, emphasizing secure design patterns and delivery practices. It delves into usage threat modeling and risk assessment for designing software security controls and overall security architecture covering Zero Trust and secure-by-design. The course describes industry best practices and standards for designing secure software architectures.

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:
• Comprehend the fundamental principles of software security architecture, including threat modeling, secure design patterns, and cryptographic techniques.
• Understand various authentication and authorization methods.
• Ensure data confidentiality and system integrity on an architectural level.

4.2 Competence and skills
On completion of the course, the student will be able to:
• Design and implement secure software architectures, incorporating principles like least privilege and defense in-depth.
• Identify and mitigate common security vulnerabilities.

4.3 Judgement and approach
On completion of the course, the student will be able to:
• Critically assess and prioritize potential security threats, applying risk assessment techniques to make informed decisions in mitigating vulnerabilities.

• Approach software development with a security-conscious mindset, demonstrating the ability to analyze and address security challenges holistically.

5. Learning activities

The teaching is organized around online lectures and pre-recorded videos together with written material and research literature. Throughout the course, communication, feedback and discussions with teachers and fellow participants will take place through the course's online learning platform, via e-mail, and online meetings.

6. Assessment and grading

Modes of examinations of the course

Code	Module	Credits	Grade
2405	Written assignment 1	2 credits	GU
2415	Written assignment 2	2 credits	GU
2425	Laboratory Session	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

• Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and Default. Publication: April 13, 2023. Cybersecurity and Infrastructure Security Agency
• CISSP All-in-One Exam Guide, Ninth Edition. Shon Harris.
• Cloud Security Handbook. Find out how to effectively secure cloud environments using AWS, Azure, and GCP, Eyal Estrin, 2022
• DevSecOps in Kubernetes, Wei Lien Dang and Ajmal Kohgadai, 2021