Blekinge Tekniska Högskola
Institutionen för programvaruteknik

Revision: 1
Dnr: BTH-4.1.14-0941-2023

KURSPLAN

Säker mjukvaruarkitektur
Secure Software Architecture
6 högskolepoäng (6 credits)

Kurskod: PA2594
Huvudområde: Programvaruteknik, Datavetenskap
Utbildningsområde: Teknik
Utbildningsnivå: Avancerad nivå
Fördjupning: A1N - Avancerad nivå, har endast kurs/er på grundnivå som förkunskapskrav

Undervisningsspråk: Engelska
Gäller från: 2024-01-15
Fastställd: 2023-09-01

1. Beslut
Denna kurs är inrättad av dekan 2022-12-06. Kursplanen är fastställd av prefekten vid institutionen för programvaruteknik 2023-09-01 och gäller från 2024-01-15.

2. Förkunskapskrav
För tillträde till kursen krävs minst 120 hp varav minst 90 hp inom det tekniska området och minst 2 års yrkeserfarenhet inom område som är relaterat till mjukvaruintensiv produkt och/eller tjänsteutveckling (visas exempelvis genom intyg från arbetsgivare).

3. Syfte och innehåll

3.1 Syfte
Syftet med kursen är att ge studenten en djup förståelse av grunderna inom säker mjukvaruarkitektur, som möjliggör att designa, implementera och underhålla säkra mjukvarusystem. Vid kursens slut kommer studenten ha kunskaper och färdigheter för att identifiera säkerhetsrisker, tillämpa tillvägagångssätt som följer säkerhetsbranschens bästa praxis, och skapa robusta mjukvarusystem som skyddar mot ett brett spektrum av hot.

3.2 Innehåll
Kursen omfattar grundläggande metoder inom säker mjukvaruutveckling, med tonvikt på säkra designmönster och leveransmetoder. Studenten kommer även fördjupa sig i processer för hotmodellering och riskbedömning som används för design av säker mjukvara. Detta inkluderar även övergripande säkra arkitekturer som omfattar nolltillit och inbyggt säkerhet. Kursen redogör för befintlig bäst praxis och standarder för design av säkra mjukvaruarkitekturer.

4. Lärandemål
Följande lärandemål examineras i kursen:

4.1 Kunskap och förståelse
Efter genomförd kurs ska studenten kunna:
• Förstå de grundläggande principerna för säker mjukvaruarkitektur, inklusive hotmodellering, designmönster som främjar säkerhet samt tillhörande kryptografiska säkerhetsåtgärder.
• Förstå olika autentiserings- och auktoriseringsmetoder.
• Säkerhetsställa datasekretess och systemintegritet på arkitekturnivå.

4.2 Färdighet och förmåga
Efter genomförd kurs ska studenten kunna:
• Designa och implementera säker mjukvaruarkitektur, som bygger på välkända principer inom säkerhet såsom lägsta behörighet och säkringsstrategi flera steg (djupförsvar).
• Identifiera och reducera vanliga säkerhetssårbarheter.

4.3 Värderingsförmåga och förhållningssätt
Efter genomförd kurs ska studenten kunna:

• Kritiskt bedöma och prioritera potentiella säkerhetshot, använda tekniker för riskbedömning för att fatta välgrundade beslut för att reducera sårbarheter.
• Förhålla sig till mjukvaruutveckling med ett säkerhetsmedvetet tänkesätt, som visar förmågan att analysera och hantera säkerhetsutmaningar ur ett helhetsperspektiv.

5. Läraktiviteter

Undervisningen sker i form av online föreläsningar och inspelat videomaterial, tillsammans med skrivet material och forskningslitteratur. Under kursens gång kommer kommunikation, feedback och diskussioner med lärare och andra kursdeltagare att ske via kursens lärplattform, e-post och online möten.

6. Bedömning och examination

Examinationsmoment för kursen

Kod	Benämning	Omfattning	Betyg
2405	Inlämningsuppgift 1	2 hp	GU
2415	Inlämningsuppgift 2	2 hp	GU
2425	Laboration	2 hp	GU

Kursen bedöms med betygen G Godkänd, UX Underkänd, något mer arbete krävs, U Underkänd.

I kurstillfällets information inför kursstart framgår i vilka examinationsmoment som kursens lärandemål examineras samt gällande bedömningsgrunder.

Examinator kan, efter samråd med högskolans FUNKA-samordnare, fatta beslut om anpassad examinationsform för att en student med varaktig funktionsvariation ska ges en likvärdig examination jämfört med en student utan funktionsvariation.

7. Kursvärdering

Kursvärdering ska göras i enlighet med BTH:s beslut om frågeställning i kursvärderingar och beslut om process för hantering och uppföljning av kursvärderingar.

8. Begränsningar i examen

Kursen kan ingå i examen men inte tillsammans med annan kurs vars innehåll, helt eller delvis, överensstämmer med innehållet i denna kurs.

9. Kurslitteratur och övriga lärresurser

• Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and Default. Publication: April 13, 2023. Cybersecurity and Infrastructure Security Agency. No ISBN. Link: cisa.gov/sites/default/files/2023-06/principles_approaches_for_security-by-design-default_508c.pdf
• CISSP All-in-One Exam Guide, Ninth Edition. Shon Harris. ISBN: 13978-1260467376
• Cloud Security Handbook. Find out how to effectively secure cloud environments using AWS, Azure, and GCP, Eyal Estrin, 2022. ISBN: 13978–1800569195
• DevSecOps in Kubernetes, Wei Lien Dang and Ajmal Kohgadai, 2021. ISBN: 9781098101770