Blekinge Institute of Technology
Department of Computer Science

Revision: 9,1
Reg.no: BTH-4.1.14-0268-2020

COURSE SYLLABUS

Programvarusäkerhet

Software Security

7.5 credits (7,5 högskolepoäng)

Course code: DV2546
Main field of study: 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
Discontinued: 2023-04-04

1. Decision

This course is established by School of Computing 2013-06-17. The course syllabus is approved by Head of Department of Computer Science 2020-03-01 and applies from 2020-08-31.

2. Entry requirements

Admission to the course requires passing the course," Programming in UNIX environment ".

3. Objective and content

3.1 Objective

The main objective of this course is to teach students to understand and how to address various software security problems in a secure and controlled environment. During this course the students will gain knowledge (both theoretical and practical) in various kinds of software security problems, and techniques that could be used to protect the software from security threats. The students will also learn to understand the ”modus operandi” of adversaries; which could be used for increasing software dependability.

3.2 Content

The course comprises the following:
• Software security background: historical overview, why software needs to be protected, traditional techniques used.
• Detailed analysis of different groups of software vulnerabilities, their characteristics, how adversaries can exploit them, and how to protect against them.
• Specific problems relating to software security within a Web context in terms of threats and countermeasures.
• Source code analysis, different methods used, and introduction to existing tools.
• Software security research: motivation, goals, state-of-the-art, and related areas.

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 reason about software security problems and protection techniques on both an abstract and a more technically advanced level.
• be able to explain how software exploitation techniques, used by adversaries, function and how to protect against them.

Skills and abilities
• be able to individually review executing software systems and its source code in search for security flaws.
• be able to correctly address identified common security flaws relating to software in both web applications and client/server systems.
• use the repositories of vulnerabilities to investigate and keep updated about current threats.

5. Learning activities

The course consists of:
• Lectures where the students are introduced to theories within a software security context

• Seminars where the students in groups implement the theories, resulting in a more profound understanding of core concepts
• Assignments with tasks about source code analysis, binary file analysis, web security and client-server security problems.

6. Assessment and grading

Modes of examinations of the course

Code	Module	Credits	Grade
1310	Web-/Client server	1.5 credits	GU
1320	Source code analysis	3 credits	AF
1330	Binary file analysis	1.5 credits	AF
1340	Identification and management of software vulnerabilities	1.5 credits	AF

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

The final grade is a weighted average. Rounded down.

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

1. Gray Hat Hacking: The Ethical Hacker's Handbook, Fifth Edition
Author: Allen Harper, Daniel Regalado, Shon Harris, Chris Eagle, Jonathan Ness, Branko Spasojevic, Ryan Linn and Stephen Sims
Publisher: McGraw-Hill Education
Published: 2018
ISBN: 9781260108415

2. The Web Application Hacker's handbook
Author: Dafydd Stuttard, Marcus Pinto
Publisher: John Wiley & Sons
Published: 2011

10. Additional information

Replaces DV2409 and DV2513.