ID2008 Software Engineering and Security Architecture 7.5 credits

Software Engineering and Security Architecture

This is a translation of the Swedish, legally binding, course syllabus.

Establishment

Course syllabus for ID2008 valid from Spring 2010

Grading scale

A, B, C, D, E, FX, F

Education cycle

Second cycle

Main field of study

Specific prerequisites

120 university credits (hp) in engineering or natural sciences and documented proficiency in English corresponding to English A.

Language of instruction

The language of instruction is specified in the course offering information in the course catalogue.

Intended learning outcomes

Having completed this course the student will be able to participate in, and cooperate with, software development teams with a goal to achieving appropriate levels of security for that team's software products.

To this end the student will be able to:
* identify common software vulnerabilities, their causes, symptoms, and remedies.
* understand the roles and activities in project management that promote secure software development.
* apply secure software design principles, and methods and tools for the secure implementation of those designs.
* apply suitable security architectures.
* relate to standards of relevance for the area of secure software engineering, in particular to understand the advantages, roles, mechanisms, and difficulties involved in methods for evaluating assurance in security software.

Course contents

With the starting point of studies into the problem in terms of known software vulnerabilities, the course then relates the different stages of the software development cycle to measures that can suitably alleviate software vulnerabilities.
Assurance criteria evaluation methods are primarily represented by The Common Criteria. In order to gain a broad understanding of the method it is presented through several complementary perspectives. Apart from an historical view over its development it is studied from the point of view of several of the primary beneficiaries of the method.

Disposition

Lectures and practical assignment
Emphasis is placed on active study of the subject matter, both individually and in groups, i.e., the students are expected to research the subject matter through studies of the course literature and the Internet. This research is shared during the course through group discussion, additions to the course web pages, and active participation at lectures.
Students will be required to actively participate in practical project work where several of the above mentioned methods, tools and principles are applied in a fictitious software development project. The results from this work are presented in a written report and active seminar participation toward the end of the course.

Course literature

Preliminary:

Gary McGraw: Software Security, Addison-Wesley, 2006, ISBN: 0-321-35670-5

Examination

- PRO1 - Project, 3.8 credits, grading scale: P, F
- TEN1 - Examination, 3.7 credits, grading scale: A, B, C, D, E, FX, F

Based on recommendation from KTH's coordinator for disabilities, the examiner will decide how to adapt an examination for students with documented disability.

The examiner may apply another examination format when re-examining individual students.

If the course is discontinued, students may request to be examined during the following two academic years.

Examination is comprised of a written exam and a practical project. The written exam contains a number of questions which require essay answers. It is graded according to the scale A,B,C,D,E,Fx,F. The practical project is completed in student groups and is graded pass, fail, or complementary work required. A pass for the course requires a pass mark on both the written exam and for the project work. The student's grade for the course is based on the grade for the written exam.
Each exam question is given one of the following grades:
A The answer is a complete and comprehensive solution to the question and is clear indication that the student has the ability to critically reason around the course subject matter.
B The answer is a complete and comprehensive solution to the question.
C The answer shows a complete understanding of the question and the ability to relate a well balanced solution.
D The answer shows a good understanding of the question and the ability to communicate the most salient parts of the solution.
E The answer shows a motivateable interpretation of the question and the ability to correctly describe relevant concepts and terms.
F The answer fails to meet any of the above criteria.
In order to pass the exam all the answers must achieve at least an E grade. Beyond that, the grade for the exam is calculated as an average of the two highest grades for the exam answers. Where that average is half-way between two grades, the lower grade is applied unless there is evidence of an individual contribution to course work that would support the higher grade. A practical implication for this rule is that it will be to the students advantage to make explicit what they contribute and accomplish during the course, including their individual contribution to group work. The motivation for the two-grade average strategy is that the student must meet the basic requirements for all the course goals, but thereafter may specialise their deeper studies to two or more of the course goals.
If a student receives an F grade on a maximum of one exam question, and an average grade of at least C for two questions then the exam will be awarded an Fx grade. Students who are awarded an Fx grade on the written exam are given the opportunity to complete complementary tasks. If such complementary assignments meet the requirements set for them the exam grade will be converted to a pass. In such cases the exam will not be awarded higher than an E grade.

Ethical approach

- All members of a group are responsible for the group's work.

- In any assessment, every student shall honestly disclose any help received and sources used.
- In an oral assessment, every student shall be able to present and answer questions about the entire assignment and solution.