1 Course title and credit points
The course is titled Software Security/Programvarusäkerhet and awards 7.5 ECTS credits. One credit point (högskolepoäng) corresponds to one credit point in the European Credit Transfer System (ECTS).

2 Decision and approval
This course is established by School of Computing 2013-06-17. The course syllabus was revised by School of Computing and applies from 2013-09-02. Reg.no: BTH 4.1.1-0442-2013

3 Objectives
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.

4 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.

5 Aims and learning outcomes
Knowledge and understanding
On completion of the course the student will:
- 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
On completion of the course the student will:
- 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.

6 Generic skills
The following generic competences are trained in the course:
- Problem solving
- Planning and time management
- Information search

7 Learning and teaching
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.
The teaching language is English.

8 Assessment and grading
Examining of the course

-----------------------------------------------
<table>
<thead>
<tr>
<th>Code Module</th>
<th>Credit</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>1310 Web-/Client server</td>
<td>1.5 ECTS</td>
<td>G-U</td>
</tr>
<tr>
<td>1320 Source code analysis</td>
<td>3 ECTS</td>
<td>A-F</td>
</tr>
<tr>
<td>1330 Binary file analysis</td>
<td>1.5 ECTS</td>
<td>A-F</td>
</tr>
<tr>
<td>1340 Identification and management of software vulnerabilities</td>
<td>1.5 ECTS</td>
<td>A-F</td>
</tr>
</tbody>
</table>

The course will be graded A Excellent, B Very good, C Good, D Satisfactory, E Sufficient, FX Insufficient, supplementation required, F Fail. The final grade is a weighted average. Rounded down.

**9 Course evaluation**
The course coordinator is responsible for systematically gathering feedback from the students in course evaluations and making sure that the results of these feed back into the development of the course.

**10 Prerequisites**
Admission to the course requires passing the course, 'Programming in UNIX environment'.

**11 Field of education and subject area**
The course is part of the field of education and is included in the subject area Computer Science.

**12 Restrictions regarding degree**
The course cannot form part of a degree with another course, the content of which completely or partly corresponds with the contents of this course.

**13 Additional information**
Replaces DV2409 and DV2513.

**14 Course literature and other teaching material**
1. Gray Hat Hacking, Third Edition Reviews
   Author: Harris, S., Harper, A., Eagle, C., & Ness, J. 
   Publisher: McGraw-Hill
   Published: 2011
2. The Web Application Hacker's handbook
   Author: Dafydd Stuttard, Marcus Pinto
   Publisher: John Wiley & Sons
   Published: 2011