Linnæus University

Course syllabus

Faculty Board of Science and Engineering
School of Computer Science, Physics and Mathematics

2DV404 Nätverkssäkerhet fördjupning, 7,5 högskolepoäng
Network Security, Advanced, 7.5 credits

Main field of study
Computer Science

Subject Group
Informatics/Computer and Systems Sciences

Level of classification
First Level

Progression
G2F

Date of Ratification
Approved by the Board of the School of Computer Science, Physics and Mathematics
2009-11-19

Revised 2011-05-13. Revision made for English translation of the syllabus, expected
learning outcomes, content, examination, literature list and course evaluation.

The course syllabus is valid from autumn semester 2011

Prerequisites
60 credits in Computer Science and the course 1DV425 Network security, 7.5 credits or
equivalent.

Expected learning outcomes
The student should be able to use advanced security technologies and discuss the
functions and what problems they solve. The student is expected to address these
security issues through critical thinking, the study of literature and scientific materials.

After completing this course the student should be able to:

- explain different concepts of system security and network-based security,
- identify, describe and analyze security-related issues in an IT environment,
- identify, describe, analyze, and implement security mechanisms in network
  devices, operating systems and software,
- evaluate and analyze security-related changes in an IT environment,
- discuss and analyze security mechanism's impact on humans and the organization
  from an information security perspective.

Content
The course consists of two modules.

Module 1 Project 4.5 credits
Planning, implementation, analysis and presentation of results from the study of applied problem. The work is carried out in groups.

Module 2 Seminars 3 credits
Discuss and analyze security mechanism's impact on humans and the organization from an information security perspective.

Type of Instruction
Teaching is conducted in the form of project work and seminars.

Examination
The course is assessed with the grades U,3,4 or 5.
For grade 3, the expected learning outcomes must be achieved.

Attendance and performance in seminars and project presentations are evaluated and graded.

Module 1 and 2 are examined through assessment of written assignments, oral and written presentations. Grades are U, 3, 4.

To obtain the grade 5, students must also carry out a individual depth task within each module.

On request, students may have their credits translated to ECTS-marks. Such a request must be sent to the examiner before the grading process starts.

Students not achieving satisfactory results in examination are permitted a second attempt within 6 weeks — during regular semester periods. The number of examinations is limited to five times.

Course Evaluation
A course evaluation will be carried out at the end of the course in accordance with the guidelines of the University. The result of the course evaluation will be filed at the department.

Required Reading and Additional Study Material
Required Reading
Goodrich, T. M. & Tamassia, R. 2011. Introduction to Computer Security. Pearson. ISBN 0321702018.
Schneier, B. 2004. Secrets and Lies: Digital Security in a Networked World. John Wiley & Sons. ISBN 0471453803.

Scientific papers which are downloaded via the Internet or the course website.

Reference Literature
Schneier, B. 2003. Beyond Fear: Thinking Sensibly about Security in an Uncertain World. Springer. ISBN 0387026207.