HI1023 Network Security 7.5 credits

Nätverkssäkerhet, grundkurs

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

Establishment

On 2020-04-17, the Head of School of CBH has decided to establish this official course syllabus to apply from the spring semester 2021 C-2020-0764.

Grading scale

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

Education cycle

First cycle

Main field of study

Technology

Specific prerequisites

HE1033 Communication Networks

Language of instruction

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

Intended learning outcomes

After completing the course, the student will be able to:

- Analyze an organization's need for IT-security and to follow a fundamental method for this
- Prepare and secure a computer network at both the network level and the application level
- Search for and detect typical security vulnerabilities in IT systems and computer networks and be able to state how to deal with them
- Plan and carry out a literature study of a limited topic within IT or computer network security and compile and present the results thereof
- Give an account for how a few security technologies, included in the course, work and can be used
- Give an account for how a few social, societal, and ethical aspects affect IT and computer network security.

Course contents

The course aims at theoretical and applied knowledge in securing computer networks, including servers, computers, and their software as well as securing the organization wherein they reside. The course deals with securing data communications at the network and transport levels (firewalls, ports, IP tunnels, IPSec etc.) and the application level (authentication, encryption etc.). The course also deals with non-technical aspects of IT- and communication security. Included are societal and economical aspects, but also ethical aspects.

The following is included in the course:

- General overview of IT security
- How to work with IT security
- Management within companies and organisations
- Encryption methods
- Authentication and access control
- IPSec and virtual private networks (VPN)
- Firewalls and intrusion detection system (IDS)
- Protection against malicious software, such as anti-virus software
- Personal integrity
- Web security
- Typical security vulnerabilities
- Other current topics in IT security

Examination

- LAB1 - Laboratory Work, 1.5 credits, grading scale: P, F

- RED2 - Report, 2.0 credits, grading scale: A, B, C, D, E, FX, F
- TEN1 - Written exam, 4.0 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.

RED2 is examined by hand ins, seminars, and oral presentation.

Other requirements for final grade

Passed lab assignment (LAB1; 1,5 cr.)
Passed account (RED2; 2 cr.)
Passed exam (TEN1; 4 cr.)
Final grade, grading scale A-F. Final grade is based on the lower grade of RED2 and TEN1.

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.