Blekinge Institute of Technology
Department of Computer Science

COURSE SYLLABUS

Nätverks- och systemsäkerhet

Network and System Security

7,5 ECTS credit points (7,5 högskolepoäng)

Course code: ET2595
Educational level: Second cycle
Course level: A1N
Field of education: Technology
Subject group: Electrical Engineering

Subject area: Electrical Engineering
Version: 5
Applies from: 2017-08-01
Approved: 2017-03-01
Disused: 2023-08-28

1 Course title and credit points
The course is titled Network and System Security/Nätverks- och systemsäkerhet 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 Dean 2016-06-07. The course syllabus was revised by Head of Department of Computer Science and Engineering and applies from 2017-08-01. The course is replaced with ET2540, Nätverkssäkerhet.
Reg.no: BTH-4.1.1-0217-2017.
Replaces ET2540.

3 Objectives
The aim of the course is for students to learn how data, computer systems and networks can be protected against unauthorized access.

4 Content
The key elements of the course are:
• Overall description of computer hacking, malicious software (malware) and denial-of-service attacks
• Introduction to applied cryptography, key management and digital certificates
• Vulnerabilities and security functions for applications and operating systems
• Firewalls
• Authentication for data, users and systems
• Security for wireless networks
• IP security
• Virtual private network (VPN) systems
• Security for e-mail, web, and other applications
• Cloud security
• Introduction to intrusion detections systems (IDSs)

5 Aims and learning outcomes
Knowledge and understanding
After course completion, the student should be able to:
• Elaborate on different security threats against network equipment
• Describe different encryption methods and cryptography algorithms
• Elaborate on different types of VPN systems, such as IPsec
Competence and skills
After course completion, the student should be able to:
• Configure a firewall
• Create and administrate digital certificate
• Install and operate a VPN system
• Install and operate an IDS system
Judgement and approach
After course completion, the student should be able to:
• Evaluate different security solutions for systems and networks that protect against specific threats

6 Learning and teaching
The course contains lectures and seminars where theoretical aspect of the course are presented, and lab work where practice applying the theory. The course contains also an assignment (assignment 1) and a project (assignment 2) that are independently done by the students on their own.
English

7 Assessment and grading
Examination of the course

Code	Module	Credit	Grade
1710	Exam[1]	3 ECTS	A-F
1720	Laboration 1	1 ECTS	G-U
1730	Laboration 2	1 ECTS	G-U
1740	Laboration 3	1 ECTS	G-U
1750	Assignment 1	0.5 ECTS	G-U
1760	Assignment 2	1 ECTS	G-U

[1] Determines the final grade for the course, which will only be issued when all components have been approved.
The course will be graded A Excellent, B Very good, C Good, D Satisfactory, E Sufficient, FX Fail, supplementation required, F Fail.

8 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.

9 Prerequisites
Passed/completed courses in Data- and Telecommunications or Data communication 7,5 hp.
Passed/completed course in Programming 7,5 hp

10 Field of education and subject area
The course is part of the field of education and is included in the subject area Electrical Engineering.

11 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.

12 Course literature and other teaching material
■