DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

DIT642 Computer Security, 7.5 credits

Datasäkerhet, 7,5 högskolepoäng

Second Cycle

Confirmation

This course syllabus was confirmed by Department of Computer Science and Engineering on 2022-12-16 and was last revised on 2023-11-20 to be valid from 2024-01-15, spring semester of 2024.

Field of education: Science 100%
Department: Department of Computer Science and Engineering

Position in the educational system

The course is a part of the Computer Science Master´s Programme and a single subject course at University of Gothenburg.

The course can be part of the following programmes: 1) Computer Science, Master's Programme (N2COS), 2) Applied Data Science Master's Programme (N2ADS) and 3) Computer Science, Bachelor's Programme (N1COS)

Main field of studies	*Specialization*
Computer Science	A1N, Second cycle, has only first-cycle course/s as entry requirements

Entry requirements

To be eligible for the course students should have successfully completed courses corresponding to 60 hec within the subject Computer Science or equivalent.
A 7.5 hec course in Programming is required.

Applicants must prove knowledge of English: English 6/English B or the equivalent level of an internationally recognized test, for example TOEFL, IELTS.

Learning outcomes

After completing the course the student is expected to be able to:

Knowledge and understanding
- explain the fundamental goals of computer security,
- describe several security vulnerabilities and possible protection mechanisms,
- describe common methods for security assessment and evaluation as well as problems with current security metrication

Competence and skills
- analyze the security of different types of systems and suggest improvements
- use a few methods for security modeling
- demonstrate his or her skill in technical writing

Judgement and approach
- assess the advantages and disadvantages between different protection mechanisms
- judge the consequences of insecurity
- Keep an informed argument of the ethical and social aspects of computer security

Course content

The course gives basic knowledge in the security area, i.e. how to protect your system against intrusions and attacks. The purpose of intrusions can be to change or delete resources (data, programs, hardware, etc), to get unauthorized access to confidential information or unauthorized use of the system's services. The course covers threats and vulnerabilities in the computer systems and networks, as well as rules, methods and mechanisms for protection. Modeling and assessment of security and dependability as well as metrication methods are covered. A holistic security approach is taken and organizational, business-related, social, human, legal and ethical aspects are treated. The following topics will be covered, among others.

- Introduction to computer security
- Overview of security threats
- Introduction to cryptography.
- Security in operating systems
- Security mechanisms including authentication, authorization, and access control

- Introduction to Network Security and Intrusion detection systems
- Security Models: Bell-LaPadula, Biba, Chinese wall etc.
- Security management, organization and ethics

Sub-courses

1. **Laboratory Experiment** *(Laboration),* 1.5 credits
   Grading scale: Pass (G) and Fail (U)
2. **Assignments** *(Inlämningsuppgifter),* 6 credits
   Grading scale: Pass with distinction (5), Pass with credit (4), Pass (3) and Fail (U)

Form of teaching

The course consists of a series of lectures and exercises in a laboratory. Normally, one or two lectures are given by lecturers from industry, who give an application perspective on security. The exercises in the laboratory focus on a few common security mechanisms.

Language of instruction: English

Assessment

The course is examined by laboratory exercises done in groups and through individual mandatory assignments, where a voluntary test is included.

If a student, who has failed the same examined component twice, wishes to change examiner before the next examination, a written application shall be sent to the department responsible for the course and shall be granted unless there are special reasons to the contrary (Chapter 6, Section 22 of Higher Education Ordinance).

In cases where a course has been discontinued or has undergone major changes, the student shall normally be guaranteed at least three examination occasions (including the ordinary examination) during a period of at least one year from the last time the course was given.

Grades

The grading scale comprises: Pass with distinction (5), Pass with credit (4), Pass (3) and Fail (U).
In order to be awarded the grade 3 for the whole course, the student must pass the laboratory exercises and the mandatory assignments.

In order to be awarded the grade 4 or 5 for the whole course, the student must get the grade 4 respective 5 on the sub-course assignments and pass the other sub-courses.

Course evaluation

The course is evaluated through meetings both during and after the course between teachers and student representatives. Further, an anonymous questionnaire is used to ensure written information. The outcome of the evaluations serves to improve the course by indicating which parts could be added, improved, changed or removed.

Additional information

The course is a joint course together with Chalmers.

Course literature to be announced the latest 8 weeks prior to the start of the course.

The course replaces the course DIT641, 7.5 credits. The course cannot be included in a degree which contains DIT641. Neither can the course be included in a degree which is based on another degree in which the course DIT641 is included.