UNIVERSITY OF GOTHENBURG

COMPUTER SCIENCE AND ENGINEERING

DIT071 Network Security, 7.5 credits

Network Security, 7,5 högskolepoäng

Second Cycle

Confirmation

This course syllabus was confirmed by The IT Faculty Board on 2006-11-17 and was last revised on 2017-06-07 by Department of Computer Science and Engineering to be valid from 2017-08-20, autumn semester of 2017.

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

Position in the educational system

The course is a part of the Computer Science Master's Programme and is also an elective course at the 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), 3) Computer Science, Bachelor´s Programme (N1COS) and 4) No translation available (NDATM)

Main field of studies	*Specialization*
Computer Science	A1F, Second cycle, has second-cycle course/s as entry requirements
Computer Science-Networks and Distributed Systems	A1F, Second cycle, has second-cycle course/s as entry requirements

Entry requirements

The requirement for the course is to have successfully completed two years studies within the subject Computer Science or equivalent.

Specifically, the course DIT420 Computer Communication or equivalent is required. A course in Computer security such as DIT641 is recommended but not 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 cmpletion of the course the student should be able to :

5.1 Knowledge and understanding

- Describe and state how applications can communicate securely and what possible tools and protocols exist in order to offer different levels of security
- Show knowledge about how to evaluate new protocols and the level of security they may offer
- Show skills to draw own conclusions and understand what makes systems vulnerable and be able to predict new attack methods before they become a reality
- Describe what impact the selection of different protocols and security architectures can have to an application or to a system.

5.2 Skills and abilities

- Critically analyze and design secure networks, applications and systems
- Show skills to evaluate the security needs for networked systems and applications
- Obtained skills to be able to communicate efficiently with professionals working in the field

5.3 Judgment and approach

- Judge what is required by a sound security architecture
- Describe and formulate how to evaluate the security needs for networked systems and applications

Course content

The course begins by looking at weaknesses that have plagued networked systems for years. The course also contains countermeasures like firewalls and security protocols such as SSL, SSH and IPsec and investigate in detail what makes them secure. The course also gives a survey of cryptographic tools and explains how they can be utilized in protocols and applications, for example how to provide secure user authentication over a public network.

Knowledge about possible threats and countermeasures is important not only for the network security specialist but also for application programmers and everyone else who wants to understand what level of security a system and an application can offer. By knowing the problems, future systems can be designed to be much more secure and reliable than today.

The course covers many topics related to communications and network security:

- Network attacks, encryption and random number generation
- Analysis of weaknesses and attacks against common protocols such as TCP, UDP, IP, and ICMP. Denial of service (DOS) attacks. Scanning and operating system fingerprinting.
- Access control, authentication mechanisms, passwords, Radius, AAA, PKI, key distribution, Kerberos
- Identity management, certificates, X.509, revocation, smart cards, LDAP, OCSP
- Security protocols such as IPSec , SSL and SSH
- Security in wireless networks, WEP, WPA, IEEE 802.1x, EAP, TKIP
- Network design, firewalls, packet filters, proxies, NAT, tunnelling, ingress and egress filtering
- Virtual private networks (VPN), tunnelling protocols, segmentation and remote access
- Logs, alarms, syslog, SNMP
- Link level security, VLAN technology, security in ARP, DHCP and DNS.

The course consists of a series of lectures and laborative exercises. The laborative exercises focus on network scanning, building firewalls and study of common security protocols such as SSL.

Sub-courses

1. **Laboratory work** *(Laboration),* 1.5 higher education credits
   Grading scale: Pass (G) and Fail (U)

2. **Written exam** *(Tentamen),* 6 higher education credits
   Grading scale: Pass with Distinction (VG), Pass (G) and Fail (U)

Form of teaching

The course consists of a series of lectures and laborative exercises. The laborative exercises focus on network scanning, building firewalls and study of common security protocols such as SSL.

Language of instruction: English

Assessment

An individual written exam given in an examination hall. Four laboratory exercises, carried out in pairs in the departments laboratory.

A student who has failed the same examination twice has the right to request of the department a change of examiner. The request is to be in writing and submitted as soon as possible. The department is to grant such a request withour undue delay.

In cases where a course has been discontinued or major changes have been made a student should be guaranteed at least three examination occasions (including the ordinary examination occasion) during a time of at least one year from the last time the course was given.

Grades

The grading scale comprises: Pass with Distinction (VG), Pass (G) and Fail (U).
To pass the course the student must pass both the laboratory exercises and the written exam.

The score on the final exam determines whether a Pass with Distinction for the course is awarded. In order to be granted VG, the candidate must have at least 80% of the total number of credit points at the exam. In order to be granted G, the candidate must have at least 50% of the total number of credit points at the exam.

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.