GÖTEBORGS UNIVERSITET

DATA- OCH INFORMATIONSTEKNIK

DIT071 Network Security, 7,5 högskolepoäng

Network Security, 7.5 credits

Avancerad nivå / Second Cycle

Fastställande

Kursplanen är fastställd av IT-fakultetsnämnden 2006-11-17 och senast reviderad 2017-06-07 av Institutionen för data- och informationsteknik. Den reviderade kursplanen gäller från och med 2017-08-20, höstterminen 2017.

Utbildningsområde: Naturvetenskapligt 100 %
Ansvarig institution: Data- och informationsteknik

Inplacering

The course is a part of the Computer Science Master's Programme and is also an elective course at the University of Gothenburg.

Kursen kan ingå i följande program: 1) Datavetenskapligt program (N1COS), 2) Computer Science, Master's Programme (N2COS), 3) Datavetenskapligt program (NDATM) och 4) Applied Data Science masterprogram (N2ADS)

Huvudområde	*Fördjupning*
Datavetenskap	A1F, Avancerad nivå, har kurs/er på avancerad nivå som förkunskapskrav
Computer Science-Networks and Distributed Systems	A1F, Avancerad nivå, har kurs/er på avancerad nivå som förkunskapskrav

Förkunskapskrav

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.

Lärandemål

5.1 Knowledge and understanding

- describe how applications can communicate securely and what possible tools and protocols exist in order to offer different levels of security,
- evaluate new protocols and the level of security they may offer,
- analyze what makes systems vulnerable and be able to predict new attack methods before they become a reality,
- impact different protocols and security architectures can have to an application or to a system.

5.2 Skills and abilities

- analyze and design secure networks, applications and systems,
- evaluate the security needs for networked systems and applications,
- communicate efficiently with professionals working in the field.

5.3 Judgment and approach

- judge what is required by a sound security architecture,
- evaluate the security needs for networked systems and applications.

Innehåll

Why is it possible to break into networked computer systems? What weaknesses are used? And what makes one protocol more secure than another? This course answers these questions and many more. We begin the course by looking at weaknesses that have plagued networked systems for years. We then continue with 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.

Delkurser

1. **Laboration** *(Laboratory work),* 1,5 hp
   Betygsskala: Godkänd (G) och Underkänd (U)

2. **Tentamen** *(Written exam),* 6 hp
   Betygsskala: Väl godkänd (VG), Godkänd (G) och Underkänd (U)

Former för undervisning

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.

Undervisningsspråk: engelska

Former för bedömning

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

A student who has failed a the same examination twice has to 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 without 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.

Betyg

På kursen ges något av betygen Väl godkänd (VG), Godkänd (G) och Underkänd (U). The course is graded with the following marks: 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.

Kursvärdering

The course is evaluated through meetings both during and after the course between teachers and student representatives. Further, an anonymous questionnaire can be 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.