CHALMERS UNIVERSITY OF TECHNOLOGY
Department of Computer Science and Engineering
Maskingränd, 4th floor, Ph. 031 772 1008 (CSE department's student office)

EDA263 (DIT641 for GU) Computer Security for the International Masters Program in Computer Systems and Networks (MPCSN), 7.5 credits - Course period III, 2017/2018

Aim
The course gives basic knowledge in the security area, i.e. how to protect your system against intentional 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 computer systems and networks, as well as rules, methods and mechanisms for protection. Modelling and assessment of security and dependability as well as metrication methods are covered. During a few lectures, a holistic security approach is taken and organizational, business-related, social, human, legal and ethical aspects are treated.

Prerequisites
The course EDA092 Operating systems or equivalent knowledge is recommended.

Teachers
Associate Professor Magnus Almgren, ph. 031 772 1702, email: magnus.almgren[1]

Responsible for laborations
M.Sc Wissam Aoudi, email: wissam.aoudi[1]

Laboratory supervisors
M.Sc Carlo Brunetta, email: brunetta[1]
M.Sc Thomas Rosenstatter, email: thomas.rosenstatter[1]

Contents
Part 1: Lectures, according to the plan on page 2.
Part 2: Laborations
There are four laborations in the course. They will start in course week 2 and continue until course week 6. All information on the laborations are found on the course homepage.

Reading
Text book: Stallings & Brown: Computer Security, Pearson 2012, ISBN: 978-0-273-76449-6,
          e-book at Chalmers library
Offprints (OP): can be downloaded via Ping Pong.
Downloads and links (DL) from the course homepage.

Course homepage
The course homepage is http://www.cse.chalmers.se/edu/course/EDA263/ (and ping pong).

Examination
Three written examination opportunities will be offered:
Sat 2018-03-17 08:30 (am), Wed 2017-06-05 14:00 (am) and Wed 2017-08-29 14:00 (pm)

Marks 3, 4 and 5 are given for a passed examination (GU: Pass and Pass with distinction).
The whole course is passed when the written examination and the laborations are passed.

Lecture plan (preliminary)
Lectures are given according to the schedule in timeedit with the topics as below.
The corresponding course material is listed in a separate document

lecture	contents
L1 - 180115	course introduction, terminology, computer security basics
L2 - 180118	UNIX Security, authentication and access controls, authorization, passwords
L3 - 180122	…, mobile malware
L4 - 180125	malicious software and vulnerabilities
L5 - 180126	buffer overflow attacks
L6 - 180129	introduction to cryptology, signatures, PKI, CA, covert channels, digital watermarking, key escrow
L7 - 180201	database security, injection attacks
L8 - 180202	analysis of Malware, defensive programming, operating systems security basic, malware defences, memory
L9 - 180205,	network security basics, firewalls, deception systems, network attacks , network attacks and controls, network authentication, Kerberos, Denial-of-Service attacks
L10 - 180208,	intrusion detection systems, intrusion tolerance
L11 - 180212,	Common Criteria, spam economics, computer forensics
L12 - 180219,	security and dependability modelling and metrics
L13 - 180222,	risk analysis , human and organisational factors
L14 - 180226,	security policies and models
L15 - 180301,	ethics, course summary, course survey, examination
L16 - 180305,	reserve
L17 - 180308,	reserve