CHALMERS UNIVERSITY OF TECHNOLOGY - rev. A
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, 2015/2016

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

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

Responsible for laborations

M.Sc Valentin Tudor, email: tudor[1]

Laboratory supervisors

M.Sc Fatemeh Ayatolahi, email: fatemeh.ayatolahi[1]
M.Sc Aljoscha Lautenbach, email: aljoscha [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/ .

Examination

Three written examination opportunities will be offered:
Sat 2016-03-19 08:30 (am), Sat 2016-04-09 14:00 (pm) and Wed 2014-08-24 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 below.
The corresponding course material is listed in a separate document

lecture	contents
L1 - 150118, 13-15, HA4	course introduction, terminology, computer security basics
L2 - 150121, 10-12, HB4	UNIX Security, authentication and access controls, authorization, passwords
L3 - 150122, 15-17, HA4	authentication and access controls, authorization, passwords, mobile malware
L4 - 150125, 13-15, HA4	Guest lecture by Peter Magnusson from Fingerprint; introduction to cryptology, signatures, PKI, CA
L5 - 150128, 10-12, HB4	covert channels, digital watermarking, key escrow malicious software and vulnerabilities
L6 - 150129, 15-17, HA4	malicious software and vulnerabilities, buffer overflow attacks
L7 - 150201, 13-15, HA4	database security, injection attacks
L8 - 150204, 10-12, HB4	defensive programming, operating systems security basic, malware defences, memory
L9 - 150208, 13-15, HA4	network security basics, firewalls, deception systems, network attacks , network attacks and controls, network authentication, Kerberos, Denial-of-Service attacks
L10 - 150211, 10-12, HB4	intrusion detection systems, intrusion tolerance
L11 - 150215, 13-15, HA4	Guest lecture: Common Criteria by Magnus Ahlbin and Emilie Barse from Combitech AB spam economics, computer forensics
L12 - 150218, 10-12, HB4	security and dependability modelling and metrics
L13 - 150222, 13-15, HA4	risk analysis , human and organisational factors
L14 - 150225, 10-12, HB4	security policies and models
L15 - 150307, 13-15, HA4	ethics, course summary, examination
L16 - 150310, 15-17, HB4	reserve