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, 2013/2014

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.
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 2015-03-21 am, Sat 2015-04-18 am and Wed 2014-08-26 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 - 150119, 13-15, HC4	course introduction, terminology, computer security basics
L2 - 150122, 10-12, HC4	UNIX Security, malicious software and vulnerabilities I
L3 - 150123, 15-17, HC4	malicious software and vulnerabilties II, buffer overflow attacks
L4 - 150126, 13-15, HC4	authentication and access controls, authorization, passwords
L5 - 150129, 10-12, HC4	introduction to cryptology, signatures, PKI, CA
L6 - 150130, 15-17, HC4	malware defences, network security basics, firewalls, deception systems, network attacks, operating systems security basics
L7 - 150202, 13-15, HC4	network attacks and controls, network authentication, Kerberos Denial-of-Service attacks
L8 - 150205, 10-12, HC4	intrusion detection systems, intrusion tolerance
L9 - 150209, 13-15, HC4	security policies and models
L10 - 150212, 10-12, HC4	database security, injection attacks, defensive programming
L11 - 150216, 13-15, HC4	security and dependability modelling, risk analysis
L12 - 150219, 10-12, HC4	security metrics, human and organisational factors
L13 - 150223, 13-15, HC4	Guest lecture: Common Criteria by Magnus Ahlbin and Emilie Barse from Combitech AB spam economics, computer forensics, key escrow
L14 - 150226, 10-12, HC4	ethics, course summary, examination
L15 - 150305, 13-15, HC4	reserve
L16 - 150306, 15-17, HC4	reserve