Computer Security (EDA263 / DIT 641)

Lecture 1:
Course introduction

Erland Jonsson
Department of Computer Science and Engineering
Chalmers University of Technology
Sweden

Motivation

Course in Computer Security:

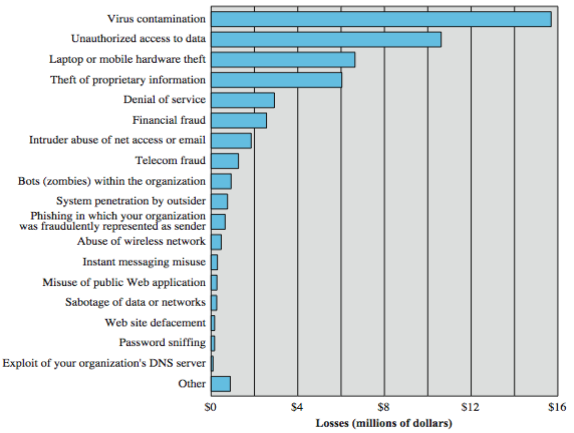
- relates to the **future**
- exhibits many **problems** related to the "IT revolution"
- security is **multi-disciplinary**
- requires a **holistic** approach

Motivation for taking the course:

- money
- jobs
- eggs

Motivation for NOT taking the course:

Money….
Computer Security Losses



Source: Computer Security Institute/FBI 2006 Computer Crime and Security Survey

Money….

Cybercrime costs $338bn to global economy; Mor... http://www.zdnet.com/blog/btl/cybercrime-costs-...

Between the Lines

Cybercrime costs $338bn to global economy; More lucrative than drugs trade

By Zack Whittaker | September 7, 2011, 12:01pm PDT

Summary: Cybercrime is costing more than the drugs trade, according to new research by Symantec. But this criminologist argues that some crime cannot be measured in financial losses.

Source: Symantec

Norton reports that cybercrime is costing the global economy $338 billion a year, overtaking a still a lucrative trade in the underground drugs market.

For every second that goes by, 19 people worldwide fall victim to some form of online crime, most commonly social network hacking and credit card fraud.

The Norton Cybercrime Report 2011 outlines the cost of cybercrime worldwide, with 74 million in the United States alone falling victim to online scams, phishing attacks and exploitative malware; costing the U.S. economy an estimated $32 billion.

Jobs…..

Eggs....

Critical Infrastructures – are dependent on IT and IT security

- Banking and Finance
- Transportation
- Power
- Water purification plants
- Communication and Information exchange
- Trade and Business
- Manufacturing and Companies
- etc, etc

Thus, we need Critical Infrastructure Protection (CIP)

CHALMERS UNIVERSITY OF TECHNOLOGY
Department of Computer Science and Engineering
Maskingränd, level 4, Ph. 031 772 1008 (department's student office) ***Rev. A***

EDA263 (DIT641 for GU) Computer Security for the International Masters Program in Secure and Dependable Computer Systems, 7.5 credits - Study period I, 2011/2012

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 unau-thorized use of the system's services. The course covers threats and vulnerabilities in the com-puter 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 cov-ered. 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

Professor Erland Jonsson, ph. 031 772 1698, email: erland.jonsson[1]
PhD Magnus Almgren, ph. 031 772 1702, email: magnus.almgren[1]

Responsible for laborations

Lecturer Arne Dahlberg, email: dahlberg[1]

Laboratory supervisors

M.Sc Pierre Kleberger, email: pierre,kleberger[1]
M.Sc Laleh Pirzadeh, email: laleh.pirzadeh[1]

Contents

Part 1: Lectures
Part 2: Laborations
There are three laborations in the course. They will start in course week 2 and continue until course week 5.
All information on the laborations are found on the course homepage.

CHALMERS UNIVERSITY OF TECHNOLOGY
Department of Computer Science and Engineering
Maskingränd, level 4, Ph. 031 772 1008 (department's student office) ***Rev. A***
EDA263 (DIT641 for GU) Computer Security for the International Masters Program in Secure and Dependable Computer Systems, 7.5 credits - Course period I, 2009/2010
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 unau-thorized use of the system's services. The course covers threats and vulnerabilities in the com-puter 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 cov-ered. 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
Professor Erland Jonsson, ph. 031 772 1698, email: erland.jonsson[1]
PhD Magnus Almgren, ph. 031 772 1702, email: magnus.almgren[1]
Responsible for laborations
Lecturer Arne Dahlberg, email: dahlberg
M.Sc Pierre Kleberger, email: pierre,kleberger[1]
M.Sc Laleh Pirzadeh, email: laleh.pirzadeh[1]
M.Sc Farnaz Moradi, email: moradi[1]
Contents
There are three laborations in the course.
n course week 2 and continue until course week 5.
All information on the laborations are found on the course homepage.

Reading

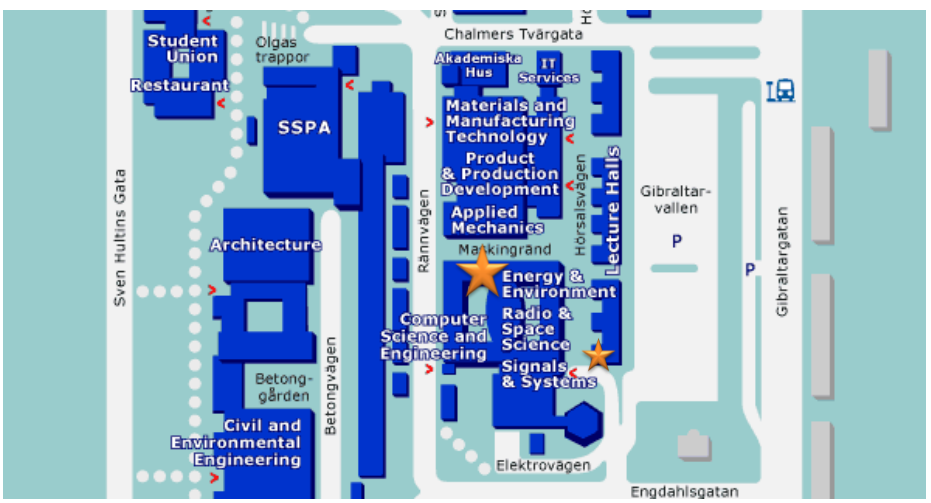
Text book:
Stallings & Brown: Computer Security,
Pearson 2008, ISBN: 978-0-13-513711-6.

Downloads and links (**DL**) from the course homepage.

Offprints (**OP**): will be sold at DC.
Offprints is some selected extra coursematerial. Some of the offprints are relevant for the laborations.

Lecture slides and notes.

Where is DC?

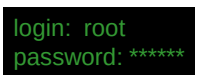


Course outline

- problems, definitions, concepts, taxonomies, ref to dependability
- threats, vulnerabilities, attacks, intrusions
- malicious software (viruses, worms, trojans, etc)
- defences and countermeasures
- security models and mechanisms
- security policies, risk analysis, certification, evaluation
- forensics, ethics

- laboratory exercises

Lab information for EDA263



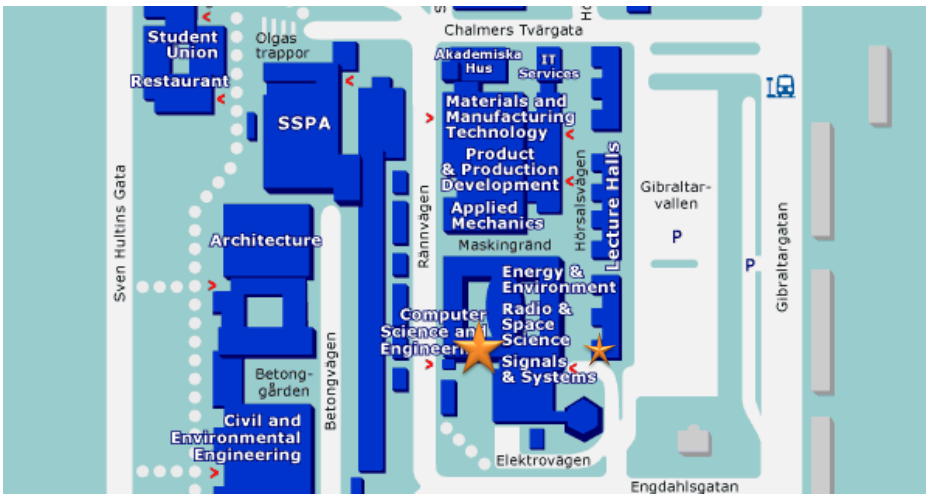
Secure programming (I&A)

GNU Privacy Guard

Vulnerability scanning

- Accounts and passwords:
  - To do the labs, you need to **book a lab group**.
  - **Booking** of lab groups is made **on-line in Chalmers student portal** (for CTH, SDCS, NDS and GU students)
  - For students that for some reason are unable to book lab groups in the student portal, a booking list will be available later this week.
  - Form groups of two students before you book!
  - Remember your group name, it will be used for reporting.
  - For login, your Chalmers account will be used.

Where is the course lab?



On the 4th floor

Lab information (cont'd)

- **Respect deadlines!**
  - Following the deadline guarantees that you get a timely notification of your result on the lab (at most 5 working days from hand-in day)!
  - Keeping the deadlines also generates less confusion regarding whether you are approved!
  - Late submissions will not be considered for correction until the re-exam week in December.
- Remote login: **ssh –X –Y <CID>@remoteXX.student.chalmers.se**
- Information regarding deadlines and hand-in instructions can be found in the labPM or at the course lab page: http://www.cse.chalmers.se/edu/course/EDA263/labs/index.html
- Results will get published at course lab result page: http://www.cse.chalmers.se/edu/year/2012/course/EDA263/labs/lab-res-12.html
- Cheating, e.g. copying code, lab report content or text found elsewhere is **plagiarism** and **will be subject to disciplinary action**.
  - so DON'T CHEAT!

Lab information (cont'd)

- **Respect deadlines!**
  - Following the deadline guarantees that you get a timely notification of your result on the lab (at most 5 working days from hand-in day)!
  - Keeping the deadlines also generates less confusion regarding whether you are approved!
  - Late submissions will not be considered for correction until the re-exam week in December.
- Remote login: **ssh –X –Y <CID>@remoteXX.student.chalmers.se**
- Information regarding deadlines and hand-in instructions can be found in the labPM or at the course lab page: http://www.cse.chalmers.se/edu/course/EDA263/labs/labinfo.html
- Results will get published at course lab result page: http://www.cse.chalmers.se/edu/course/EDA263/labs/lab-res-10.html
- Cheating, e.g. copying code, lab report content or text found elsewhere is **plagiarism** and **will be subject to disciplinary action**.

Cheating, e.g. copying code, lab report content or text found elsewhere is **plagiarism** and **will be subject to disciplinary action**.
- so DON'T CHEAT!