Computer Security (EDA263 / DIT 641)

Lecture 1:
Course introduction

Magnus Almgren (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:

- interest
- understand risk and tools in society
  (like driving with bad breaks …)
- money
- jobs

Motivation for NOT taking the course:

Facebook helps FBI nab cyber criminals who caused $850m in losses

Tineka Smith

Published 12 December 2012

Facebook's security team assisted the FBI in identifying cyber crime rings responsible for compromising more than 11 million computer systems.

The FBI and the Department of Justice (DOJ) arrested 10 individuals from several countries; including the UK, US, New Zealand, Peru, Bosnia and Herzegovina, Croatia and Macedonia.

The operation discovered cyber crime rings linked to Yahos malware which compromised over 11m computers and caused losses up to $850m.

The suspected individuals stole money using the Butterfly Botnet, which steals credit card, and bank account information from computer users'.

Botnets can be used by cyber criminals to perform DDoS (distributed denial of

CBR Home

Log in or Register for enhanced features | Forgotten Password?

Software | Systems & Networks | Communications | Services | The CIO Agenda | Cloud | Blogs | White Papers | Suppliers | Dining Club | Events | Reports | Companies | Videos

CBR Computer Business Review

All Computer Business Review

Search

The operation discovered cyber crime rings linked to Yahos malware which compromised over 11m computers and caused losses up to $850m.

The suspected individuals stole money using the Butterfly Botnet, which steals credit card, and bank account information from computer users'.

Botnets can be used by cyber criminals to perform DDoS (distributed denial of service) attacks, distribute malware and send spam emails.

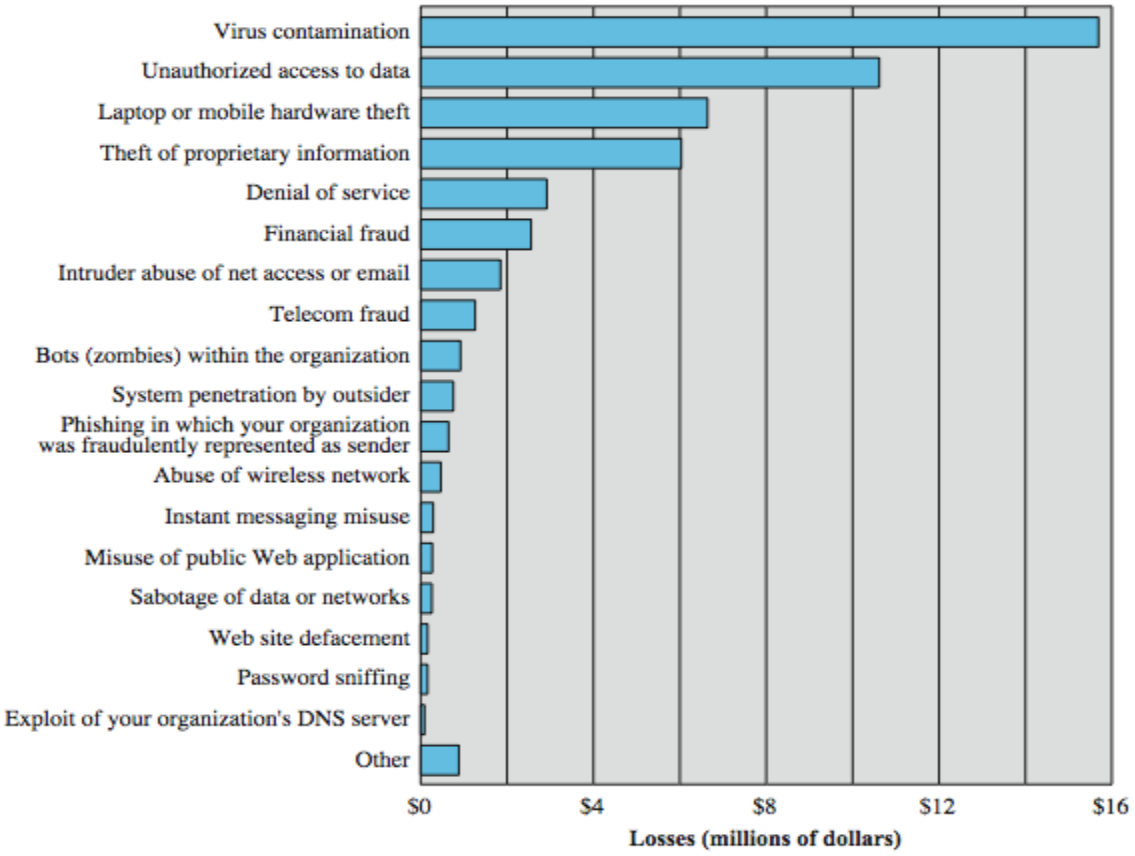
The FBI and the Department of Justice (DOJ) arrested 10 individuals from several countries; including the UK, US, New Zealand, Peru, Bosnia and Herzegovina, Croatia and Macedonia.

The operation discovered cyber crime rings linked to Yahos malware which compromised over 11m computers and caused losses up to $850m.

The suspected individuals stole money using the Butterfly Botnet, which steals credit card, and bank account information from computer users'.

Related News and Insight

Money….
Computer Security Losses



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

WELCOME
CORPORATE PROFILE
NEWS ROOM
- Press Releases
  Subscribe to RSS
- Symantec Perspectives
- Social Media Center
- Media Resources
- Media Contacts

INVESTOR RELATIONS
ANALYST RELATIONS
GOVERNMENT AFFAIRS
CAREERS

Press Release

2012 Norton Study: Consumer Cybercrime Estimated at $110 Billion Annually

Cost per Victim Goes Down; Social and Mobile Incidents on the Rise

Mountain View, CA – Sept. 5, 2012 – Norton by Symantec (NASDAQ:SYMC) today released the findings of its annual Norton Cybercrime Report, one of the world's largest consumer cybercrime studies. The study is aimed at understanding how cybercrime affects consumers, and how the adoption and evolution of new technologies impacts people's security. With findings based on self-reported experiences of more than 13,000 adults across 24 countries, the 2012 edition of the Norton Cybercrime Report calculates the direct costs[1] associated with global consumer cybercrime at US $110 billion[2] over the past twelve months.

Every second, 18 adults become a victim of cybercrime[3], resulting in more than one-and-a-half million cybercrime victims each day on a global level. With losses totaling an average of US $197 per victim across the world in direct financial costs[4], cybercrime costs consumers more than a week's worth of nutritious food necessities for a family of four[5]. In the past twelve months, an estimated 556 million[6] adults across the world experienced cybercrime, more than the entire population of the European Union.[7] This figure represents 46 percent of online adults who have been victims of cybercrime in the past twelve months, on par with the findings from 2011 (45 percent).

Changing Face of Cybercrime

This year's survey shows an increase in "new" forms of cybercrime compared to last year, such as those found on social networks or mobile devices[8] - a sign that cybercriminals are starting to focus their efforts on these increasingly popular platforms. One in five online adults (21 percent) has been a victim of either social or mobile cybercrime, and 39 percent of social network users have been victims of social cybercrime, specifically:

- 15 percent of social network users reported someone had hacked into their profile and pretended to be them.
- 1 in 10 social network users said they'd fallen victim to a scam or fake link on social network platforms.

Norton Small & Medium Business Enterprise Partners

Symantec. United States Shopping Search

ABOUT SYMANTEC

Add

With findings based on self-reported experiences of more than 13,000 adults across 24 countries, the 2012 edition of the Norton Cybercrime Report calculates the direct costs[1] associated with global consumer cybercrime at **US $110 billion[2]** over the past twelve months.

Every second, 18 adults become a victim of cybercrime[3]

* **15 percent of social network** users reported someone had hacked into their profile and pretended to be them.
* **1 in 10 social network users** said they'd fallen victim to a scam or fake link on social network platforms.

Changing Face of Cybercrime

This year's survey shows an increase in "new" forms of cybercrime compared to last year, such as those found on social networks or mobile devices[8] - a sign that cybercriminals are starting to focus their efforts on these increasingly popular platforms. One in five online adults (21 percent) has been a victim of either social or mobile cybercrime, and 39 percent of social network users have been victims of social cybercrime, specifically:

- 15 percent of social network users reported someone had hacked into their profile and pretended to be them.
- 1 in 10 social network users said they'd fallen victim to a scam or fake link on social network platforms.

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.

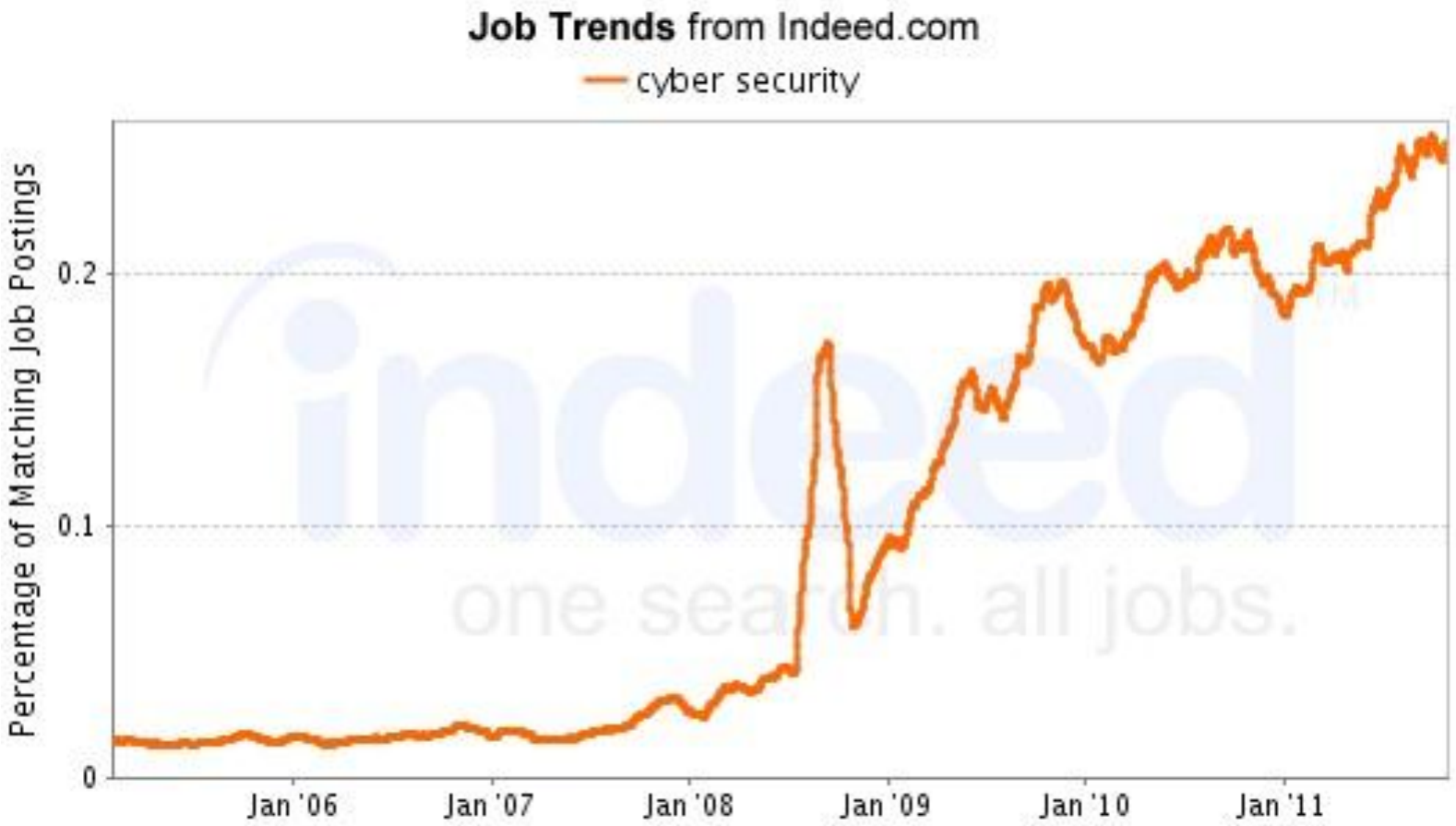
Source: Symantec

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…..


Job Trends from Indeed.com
cyber security
Percentage of Matching Job Postings
0.2
0.1
0
Jan '06
Jan '07
Jan '08
Jan '09
Jan '10
Jan '11
indeed
one search. all jobs.

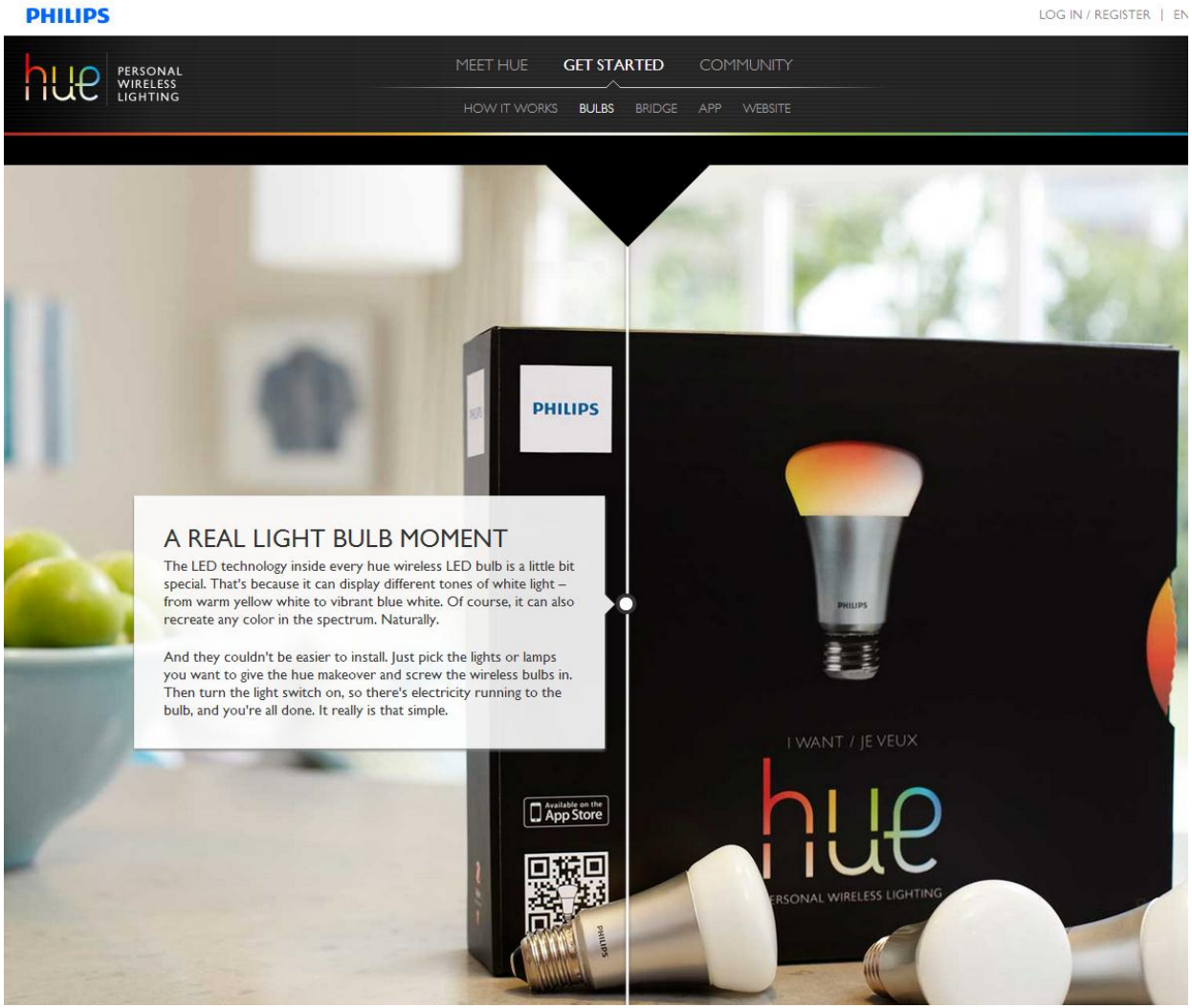
And not only traditional systems …

- 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 **CIP**:
  Critical Infrastructure Protection


Hackad dator

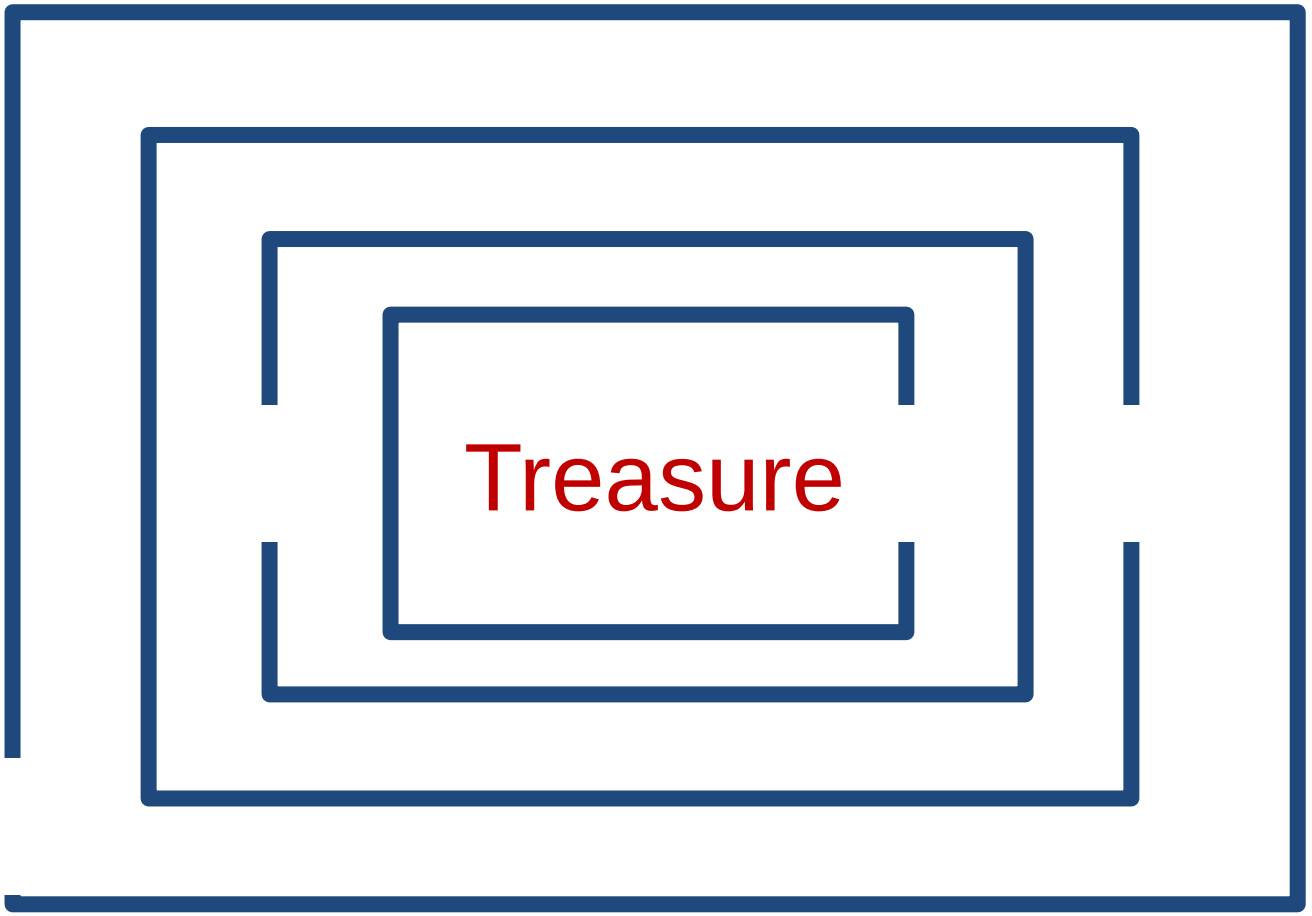

kWh

And even lamps need security



http://www.meethue.com/en-US

Explanation of Attacks



http://www.cse.chalmers.se/edu/master/secspec/

We are proud to possess multifaceted security expertise at Chalmers University of Technology and Gothenburg University, home to a world-leading research environment on computer and network security.

Based on this expertise, we offer a security specialization that consists of the following course package*

Computer Security

The course provides basic knowledge in the security area, i.e. how to protect systems against attacks. Attacks may change or delete resources (data, programs, hardware, etc), get unauthorized access to confidential information or make unauthorized use of the system's services. The course covers threats and vulnerabilities, as well as rules, methods and mechanisms for protection. Modeling and assessment of security and dependability as well as metrication methods are covered. A holistic security approach is presented and organizational, business-related, social, human, legal and ethical aspects are treated.

Runs in study period 3

Cryptography

The course covers cryptographic primitives such as private-key and public-key ciphers, hash functions, MAC's and signatures and how to embed these in cryptographic protocols to achieve basic goals such as confidentiality, authentication and non-repudiation, but also more elaborate services, such as key management, digital cash and electronic voting. Many examples of broken protocols are also discussed to enhance understanding of the engineering difficulties in building secure systems.

Runs in study period 2

Language-based Security

The course covers the principles of programming language-based techniques for computer security. The goal is understanding such application-level attacks as races, buffer overruns, covert channels, and code injection as well as mastering the principles behind such language-based protection techniques as static analysis, program transformation, and reference monitoring. The dual perspective of attack vs. protection is threaded through the lectures, laboratory assignments, and projects.

Runs in study period 4.

Network security

Why is it possible to break into networked applications and computer systems? What weaknesses are used? And what makes one protocol more secure than another? This course answers these questions and many more. We look at weaknesses that have plagued wired and wireless networked systems for years and investigate the security of countermeasures like firewalls and security protocols such as SSL, SSH and IPsec. Knowledge about possible threats and countermeasures is important for understanding what level of security a system and an application can offer.

Runs in study period 4

Security is becoming increasingly important for system design and development. System architects and designers must have security expertise, so that the systems they design do not fall victims to attacks. Software developers and engineers must have security expertise, so that the code they produce cannot be exploited. Security and network specialists must have critical knowledge of security principles and practice, in order to ensure the security of the systems they are responsible for.

Strong ties with industry

OWASP We have tight relations with the Open Web Application Security Project (OWASP). We are actively involved in both the Stockholm and Gothenburg OWASP chapters.

Cutting edge research

Crisalis is an EU project on security analysis for critical infrastructures in collaboration with eight academic and industrial partners across Europe.

CRISALIS
SECURING CRITICAL INFRASTRUCTURES

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 3, 2012/2013

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 the computer systems and networks, as well as rules, methods and mechanisms for protection. Modeling 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]
Professor Erland Jonsson, ph. 031 772 1698, email: erland.jonsson[1]

Responsible for laborations

M.Sc Pierre Kleberger, email: pierre,kleberger[1]

Laboratory supervisors

M.Sc Valentin Tudor, email: tudor[1]
M.Sc Fatemeh Ayatolahi, email: fatemeh.ayatolahi[1]

Contents

Part 1: Lectures
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.

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 3, 2012/2013

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 the computer systems and networks, as well as rules, methods and mechanisms for protection. Modeling 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]
Professor Erland Jonsson, ph. 031 772 1698, email: erland.jonsson[1]

Responsible for laborations
M.Sc Pierre Kleberger, email: pierre,kleberger[1]

sors
, email: tudor[1]
olahi, email: fatemeh.ayatolahi[1]

Contents

Part 1: Lectures
Part 2: Laborations

course week 2 and continue until course week 6.
e homepage.

There are four laborations in the course.

Reading

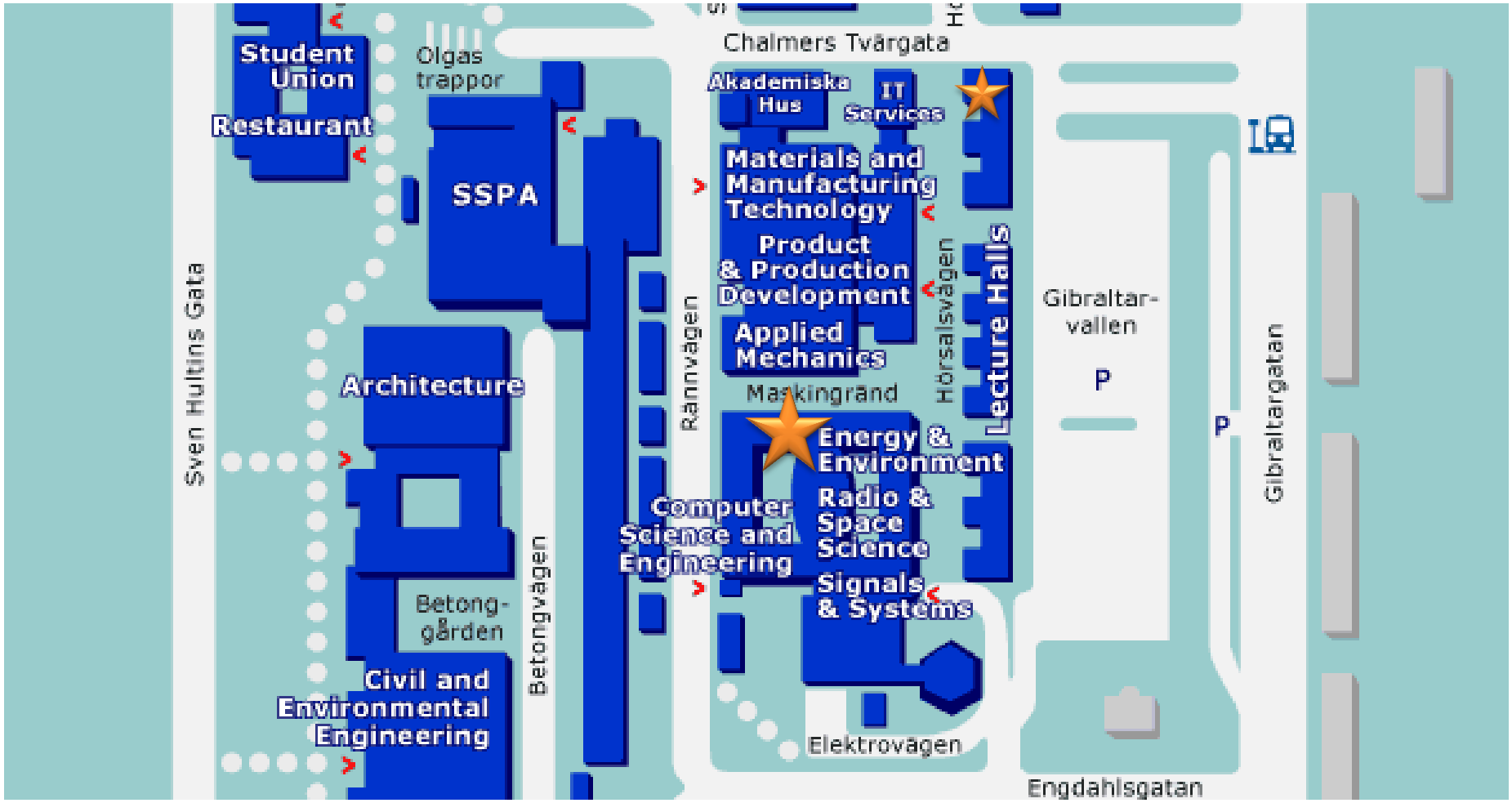
Text book:
Stallings & Brown: Computer Security,
Pearson, second edition, ISBN: 978-0-273-76449-6

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

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

Lecture slides and notes.

Where is DC?


Student Union Restaurant
Olgas trappor
Chalmers Tvärgata
Akademiska Hus
IT Services
SSPA
Materials and Manufacturing Technology
Product & Production Development
Applied Mechanics
Lecture Halls
Gibraltar-vallen
Sven Hultins Gata
Rännvägen
Hörsalsvägen
Maskingränd
Architecture
Energy & Environment
Computer Science and Engineering
Radio & Space Science
Signals & Systems
Betong-gården
Betongvägen
Civil and Environmental Engineering
Elektrovägen
Engdahlsgatan
Gibraltargatan
P
P

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

login: root
password: ******

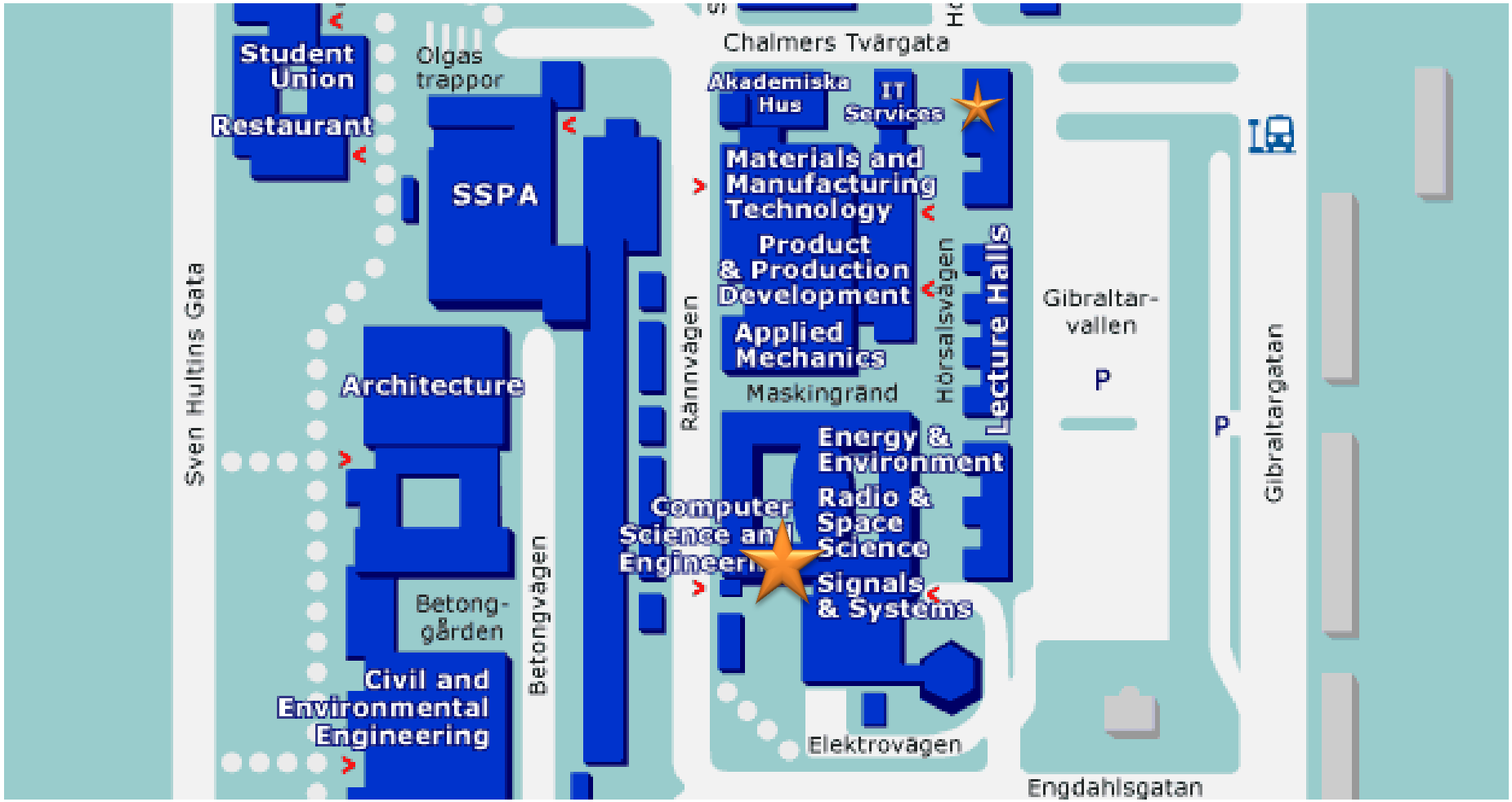
Secure programming (I&A)

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 Ping Pong** (for CTH, SDCS, NDS and GU students)
  - Form groups of two students before you book!
  - For login, your Chalmers account will be used.
- New lab this year: SQL injection

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 August.
  - Each report will only be considered twice = **only one resubmission** until rexam period!!!

- 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 page: http://www.cse.chalmers.se/edu/course/EDA263/ (follow lab link)

- 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 August.
  - Each report will only be considered twice = **only one resubmission** until rexam period!!!
- 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 page: http://www.cse.chalmers.se/edu/course/EDA263/ (follow lab link)
- 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!

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!