



Computer Security (EDA263 / DIT 641)

Lecture 1: Course introduction

Magnus Almgren
Department of Computer Science and Engineering
Chalmers University of Technology
Sweden



<https://www.youtube.com/watch?v=KpyVENBPj5c>

Dec 3:
Diplomat denies

Dec 17:
Will not release
movie.
U.S.: North Korea
responsible (Dec 19)

Nov 24:
"Hacked by #GOP"

Dec 7:
Premiere + apologies

Dec 1: FBI confirms
investigation

Dec 16: 9/11
attacks on any
theatre that shows
movie

Dec 24: Movie
available on for
online streaming + a
few cinemas

Dec 7: A righteous
deed

Jan 2: U.S. sanctions
against North Korea





No
"H

Hacked By #GOP

Warning :

We've already warned you, and this is just a beginning.

We continue till our request be met.

We've obtained all your internal data including your secrets and top secrets.

If you don't obey us, we'll release data shown below to the world.

Determine what will you do till November the **24th, 11:00 PM(GMT)**.

Data Link :

<https://www.sonypicturesstockfootage.com/SPEData.zip>

<http://dmiplaewh36.spe.sony.com/SPEData.zip>

<http://www.ntcnt.ru/SPEData.zip>

<http://www.thammasatpress.com/SPEData.zip>

<http://moodle.universidadebomatech.com.br/SPEData.zip>



Motivation

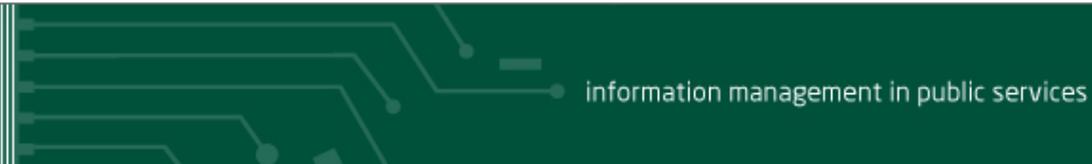
Course in Computer Security:

- 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:



Return to: [CBR Home](#) | [News](#)

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

News

Select a Technology sector

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 Yahoos 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 Computer Business Review

Register now and collect your FREE Report worth £1500

CBR Free Newsletter

Submit

Sign up for the latest CBR news and features as well as other industry newsletters.



Related News and Insight



The operation discovered cyber crime rings linked to Yahoo's **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 Yahoo's 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'.

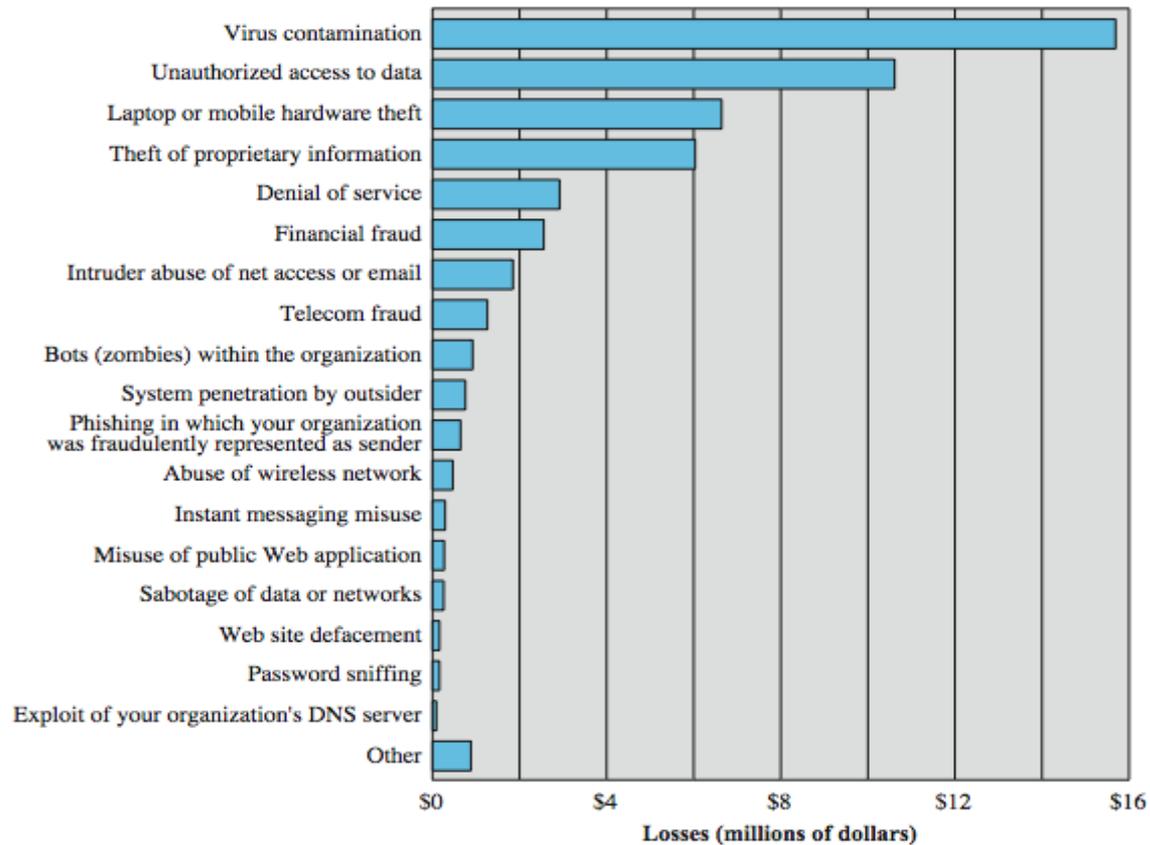
Botnets can be used by cyber criminals to perform DDoS (distributed denial of

Collect your FREE Report worth £1500

Related News and Insight

Money....

Computer Security Losses



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



ABOUT SYMANTEC

Add +

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 costs¹ associated with global consumer cybercrime at US \$110 billion² over the past twelve months.

Every second, 18 adults become a victim of cybercrime³, 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 costs⁴, cybercrime costs consumers more than a week's worth of nutritious food necessities for a family of four⁵. In the past twelve months, an estimated 556 million⁶ 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 devices⁸ - 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.

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 costs¹ associated with global consumer cybercrime at **US \$110 billion²** over the past twelve months.

Every second, 18 adults become a victim of cybercrime³

* **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 devices⁸ - 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.

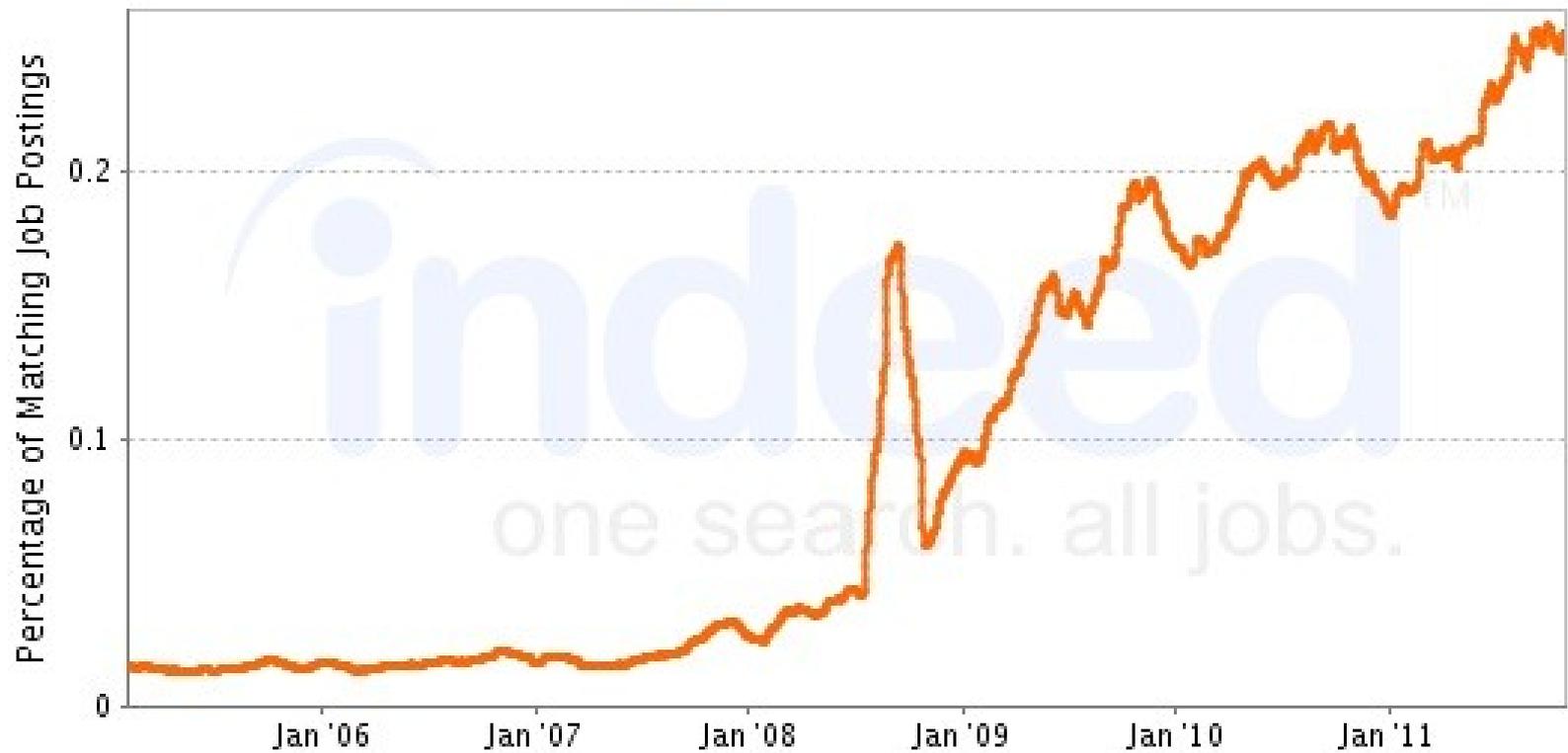
For every second that goes by, 19 people worldwide fall victim to some form of online crime, most commonly social network hacking and credit card fraud.

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



And not only traditional systems ...

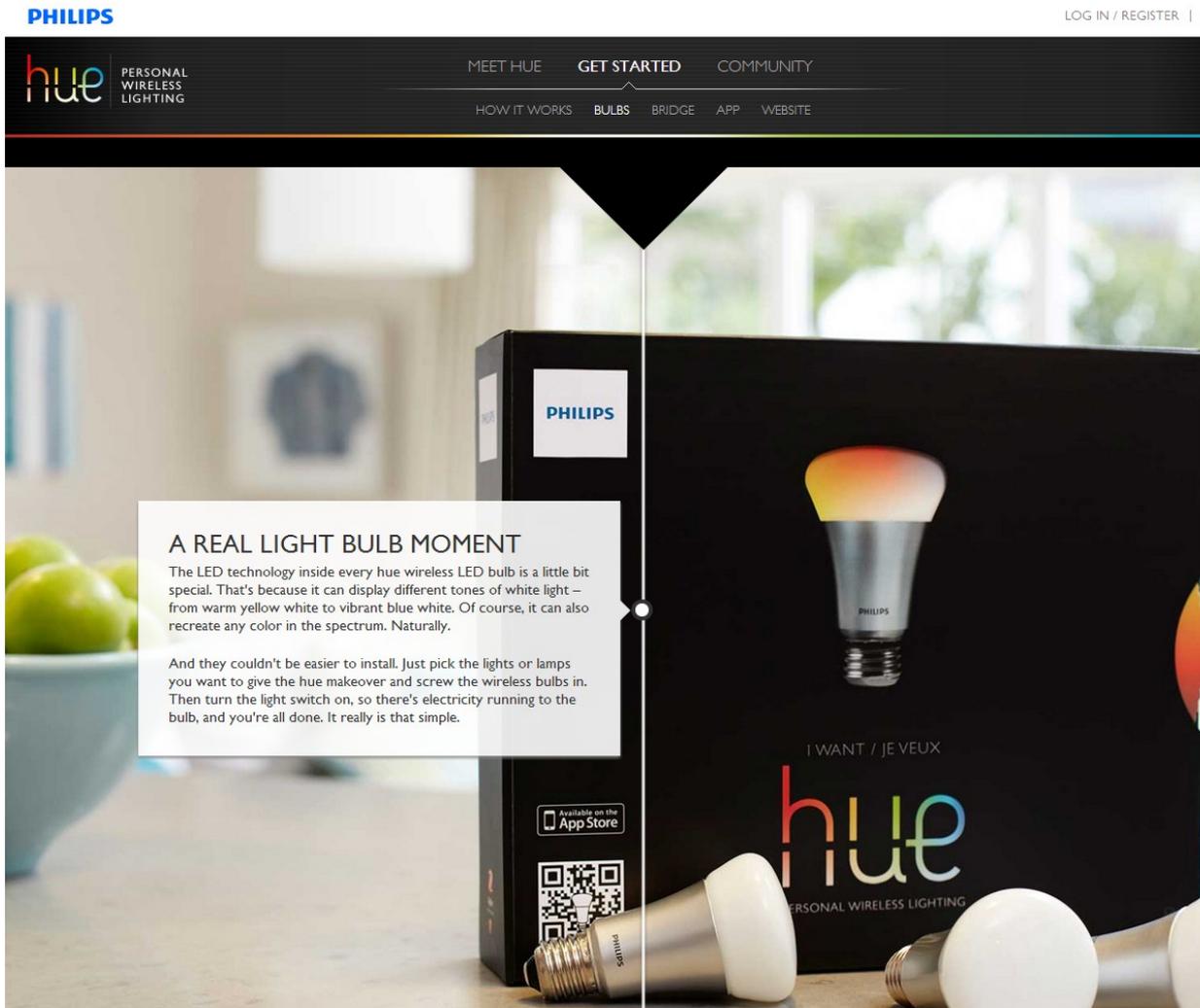
- Critical Infrastructures are dependent on IT and IT security
 - Banking and Finance
 - Transportation
 - Power
 - Water purification plants
 - Communication and Information exchange
 - Trade and Business
 - Manufacturing and Companies
 - etc, etc
- Thus, we need **CIP**:
Critical Infrastructure Protection







And even lamps need security



PHILIPS LOG IN / REGISTER | EN

hue PERSONAL WIRELESS LIGHTING MEET HUE **GET STARTED** COMMUNITY

HOW IT WORKS **BULBS** BRIDGE APP WEBSITE

A REAL LIGHT BULB MOMENT

The LED technology inside every hue wireless LED bulb is a little bit special. That's because it can display different tones of white light – from warm yellow white to vibrant blue white. Of course, it can also recreate any color in the spectrum. Naturally.

And they couldn't be easier to install. Just pick the lights or lamps you want to give the hue makeover and screw the wireless bulbs in. Then turn the light switch on, so there's electricity running to the bulb, and you're all done. It really is that simple.

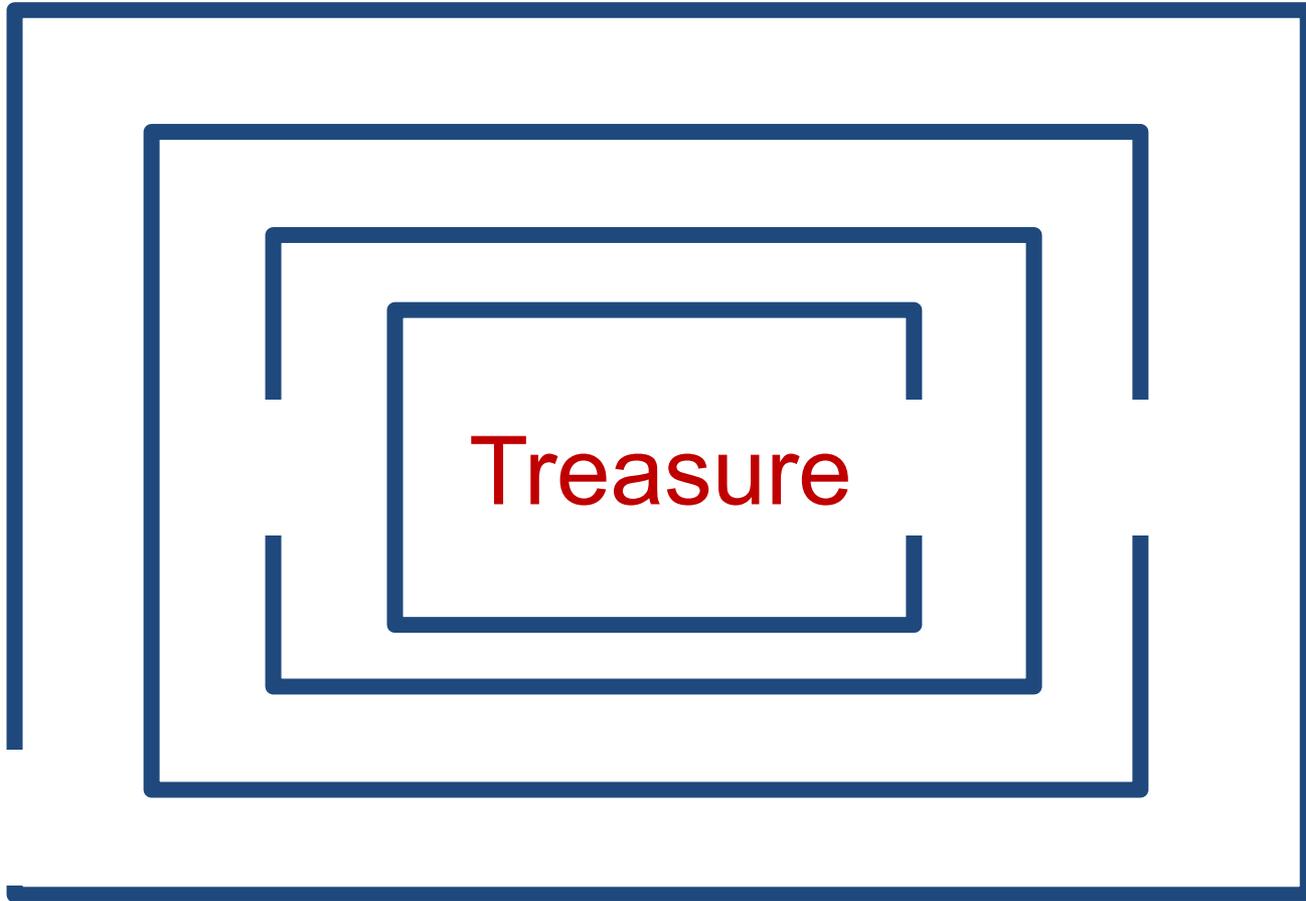
Available on the App Store

I WANT / JE VEUX

hue PERSONAL WIRELESS LIGHTING



Explanation of Attacks



Security specialization at Chalmers and Gothenburg University

CHALMERS



UNIVERSITY OF GOTHENBURG

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.



EDA263 (DIT641 for GU) Computer Security for the International Masters Program in Secure and Dependable Computer Systems, 7.5 credits - Study period 3, 2014/2015

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.almgren¹

Responsible for laborations

M.Sc Valentin Tudor, email: tudor¹

Laboratory supervisors

M.Sc Aljoscha Lautenbach, email: aljoscha¹

M.Sc Fatemeh Ayatollahi, email: fatemeh.ayatollahi¹

Contents

Part 1: Lectures

Part 2: Laboratory exercise

There are four lab exercises in the course. They will start in course week 2.

All information on the lab exercises are found on the course homepage.

EDA263 (DIT641 for GU) Computer Security for the International Masters Program in Secure and Dependable Computer Systems, 7.5 credits - Study period 3, 2014/2015

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.almgren¹

Responsible for laborations

M.Sc Valentin Tudor, email: tudor¹

Laboratory supervisors

M.Sc Aljoscha Lautenbach, email: aljoscha¹

M.Sc Fatemeh Ayatollahi, email: fatemeh.ayatollahi¹

Contents

Part 1: Lectures

Part 2: Laboratory exercise

There are four laborations in the course.

in course week 2.

se homepage.

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 available for download on pingpong. Offprints is some selected extra course material. Some of the offprints are relevant for the laborations.

Lecture slides and notes.

Computer Security

(EDA263, DIT641)

OFFPRINTS

2015

Contents:

1. Stallings: Linux Security
2. Pfleeger: Covert Channels, Steganography, Easter eggs, trapdoors and Salami attacks
3. Pfleeger: Ethics
4. An introduction to cryptography (about PGP)
5. The GNU Privacy Handbook
6. Stallings: Kerberos
7. Powell: Security (Intrusion tolerance, the FRS system)

Revision: 140108-1

Contents:

Stallings: Linux Security

Pfleeger: Covert Channels, Steganography, Easter eggs, trapdoors and Salami attacks

Pfleeger: Ethics

An introduction to cryptography (about PGP)

The GNU Privacy Handbook

Stallings: Kerberos

Powell: Security (Intrusion tolerance, the FRS system)

Reading instructions for Stallings: “Computer Security” and other course material in the course EDA263 – rev140107-1

These notes are reading instructions for the second edition of the text book, which is the officially recommended book. It will be continuously updated during the course so please always download the last version.

Lecture number:

L01: Introduction; Threats, Vulnerabilities, Protection

Chapter 1 (except §1.4, pp.48-52)

Chapter 16 -- Physical security (overviewish)

DL1: Targeted Trojan Email Attacks

L02 - UNIX:

Chapter 4 -- Access Control (UNIX): Only Section 4.4

Ch 25 (online, now available)

DL 2: *UNIX Security 1* (corresponds to parts of online Ch 25)

DL 3: *UNIX Security 2* (corresponds to parts of online Ch 25)

L02 - Malware I (L02) + Malware II (L04):

Chapter 6 -- Malware: (for interested: Digital Immune System)

Chapter 10 -- Buffer Overflows: all

DL 4: Salami attack

L03: Authentication, authorization and access control

Chapter 3 (except: pp. 105-106 and §3.5). (overviewish: §§ 3.7-3.8, pp. 119-123)

Chapter 4 (except: § 4.4 – covered in L02; RBAC Reference Model and The NIST RBAC Model, pp. 146-151)

(overviewish: §4.6, pp. 151-154)

DL2: Testing biometric methods

DL3: Bank card skimming

DL4: Password trading

DL12: Password guessing

L04 Malware I (L02) + Malware II (L04):

Chapter 6 -- Malware: (for interested: Digital Immune System)

Chapter 10 -- Buffer Overflows: all

L05: Introduction to cryptology, signatures, PKI, CA

Chapter 2 Cryptographic Tools

Chapter 20.1 Symmetric Encryption Principles (not: Feistel Cipher Structure)

Chapter 20.2 Data Encryption Standard

(Chapter 20.3 for interested students, read as an overview: AES)

Chapter 20.5 Cipher Block Modes

Chapter 20.7 Key Distribution

Chapter 23.3 Public-Key Infrastructure

OP2-3

L06: Malware defences, Firewalls, Link encryption, Operating Systems Security

DL7: Malware defences principles (p. 1-7)

§§ 9.1-9.5 Firewalls

§ 20.6 Link encryption and end-to-end encryption

§ 13.3 Reference Monitors

**Reading instructions for Stallings: “Computer Security”
and other course material in the course EDA263 – rev140107-1**

These notes are reading instructions for the second edition of the text book, which is the officially recommended book. It will be continuously updated during the course so please always download the last version.

Lecture number:

L01: Introduction; Threats, Vulnerabilities, Protection

Chapter 1 (except §1.4, pp.48-52)
Chapter 16 -- Physical security (overviewish)
DL1: Targeted Trojan Email Attacks

L02 - UNIX:

Chapter 4 -- Access Control (UNIX): Only Section 4.4
Ch 25 (online, now available)
DL 2: *UNIX Security 1 (corresponds to parts of online Ch 25)*
DL 3: *UNIX Security 2 (corresponds to parts of online Ch 25)*

L02 - Malware I (L02) + Malware II (L04):

Chapter 6 -- Malware: (for interested: Digital Immune System)
Chapter 10 -- Buffer Overflows: all
DL 4: Salami attack

L03: Authentication, authorization and access control

Chapter 3 (except: pp. 105-106 and §3.5). (overviewish: §§ 3.7-3.8, pp. 119-123)
Chapter 4 (except: § 4.4 – covered in L02; RBAC Reference Model and The NIST RBAC Model, pp. 146-151)
(overviewish: §4.6, pp. 151-154)
DL2: Testing biometric methods
DL3: Bank card skimming

L05: Introduction to cryptology, signatures, PKI, CA

Chapter 2 Cryptographic Tools
Chapter 20.1 Symmetric Encryption Principles (not: Feistel Cipher Structure)
Chapter 20.2 Data Encryption Standard
(Chapter 20.3 for interested students, read as an overview: AES)
Chapter 20.5 Cipher Block Modes
Chapter 20.7 Key Distribution
Chapter 23.3 Public-Key Infrastructure
OP4-5

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



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 vulnerabilities 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, etc.
L7	-	150202,	13-15,	HC4	network attacks and controls, network authentication, Kerberos
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 I: Common Criteria by Ahlbin and 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