Computer Security

(EDA263 / DIT 641)

Lecture 1: Course introduction

Magnus Almgren

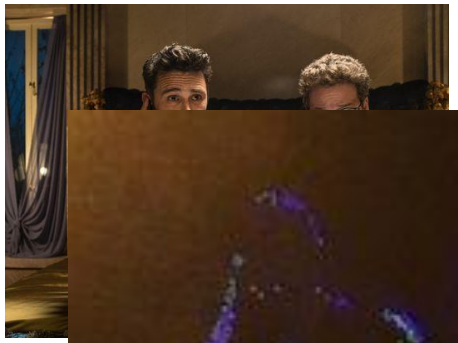
Department of Computer Science and Engineering

Chalmers University of Technology

Sweden

Trailer for movie …

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



No
"H

http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/

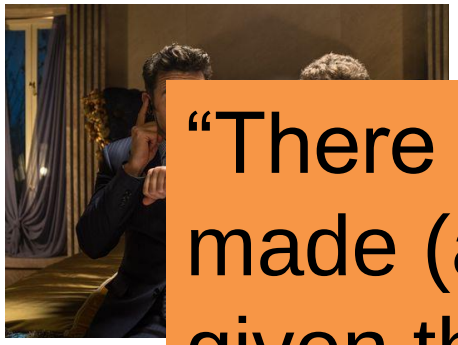
Dec 3:
Diplomat denies

Nov 24:
"Hacked by #GOP

Dec 1: FBI confirms investigation

Dec 7: A righteous deed

http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/



Nov 24:
"Hacke

Dec 1: F
investig

Dec
dee

"There is no movie of Cleopatra to be made (and how that is a bad thing given the insanity and rampaging ego of this woman and the cost of the movie is beyond me)," referring to **Jolie**. "Watch how you talk to me," he says to Pascal, prompting her response: "Don't fucking threaten me."

http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/

Nov 24:
"Hacked by #GOP

Dec 1: FBI confirms investigation

Dec 7: A righteous deed

Dec 3:
Diplomat denies

Dec 7:
Premiere + apologies

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

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

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

Jan 2: U.S. sanctions against North Korea

http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/


Democrats Confront F.B.I. Chief at Closed-Door Intelligence Briefing


A President Who Inspired Big Dreams, and Big Smiles, in a Young Generation


Jolted by Deaths, Obama Found His Voice on Race


Head of Ethics Office Speaks Out. Some Republicans Ask, Was It Ethical?

POLITICS

Obama Strikes Back at Russia for Election Hacking

By DAVID E. SANGER DEC. 29, 2016


The Obama administration was riven for months by an internal debate about how much of its evidence to make public. Al Drago/The New York Times

Russian Hacking in the U.S. Election
Complete coverage of Russia's campaign to disrupt the 2016 presidential election.

C.I.A. Nominee Says He Won't Balk at Seeking Russian Intelligence JAN 12
N.S.A. Gets More Latitude to Share Intercepted Communications JAN 12
Fact Check: Trump's News Conference JAN 12
How a Sensational, Unverified Dossier Became a Crisis for Donald Trump JAN 11
Trump, Sessions, Tillerson: Your Wednesday Evening Briefing JAN 11
See More »

WASHINGTON — President Obama struck back at Russia on Thursday for


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

EUROPE

Britain Says North Korea Was Behind Cyberattack on Health Service

By DAN BILEFSKY OCT. 27, 2017

The Royal London Hospital in London. North Korea was behind the cyberattack on the National Health System in May, a British minister said. Niklas Halle'N/Agence France-Presse — Getty Images

Britain believes "quite strongly" that North Korea was behind the "WannaCry" cyberattack in May that wreaked havoc on the National Health Service's computer systems and spread to more than 150 countries, a senior official said on Friday.

The minister of security, Ben Wallace, told the BBC that several other countries had concluded the same thing: North Korea unleashed "ransomware" that buffeted institutions including universities in China, rail

RELATED COVERAGE

Victims Call Hackers' Bluff as Ransomware Deadline Nears MAY 19, 2017

The World Once Laughed at North Korean Cyberpower. No More. OCT. 15, 2017

Global Ransomware Attack: What We Know and Don't Know JUNE 27, 2017

Hacking Attack Has Security Experts Scrambling to Contain Fallout MAY 13, 2017

Symantec Official Blog

+5
5 Votes

IoT devices being increasingly used for DDoS attacks

Malware is infesting a growing number of IoT devices, but their owners may be completely unaware of it.

By: **Symantec Security Response** SYMANTEC EMPLOYEE

Created 22 Sep 2016 | 0 Comments | : 繁體中文, 日本語, 한국어

Malware targeting the Internet of Things (IoT) has come of age and the number of attack groups focusing on IoT has multiplied over the past year. 2015 was a record year for IoT attacks, with eight new malware families emerging. More than half of all IoT attacks originate from China and the US. High numbers of attacks are also emanating from Russia, Germany, the Netherlands, Ukraine and Vietnam.

Poor security on many IoT devices makes them soft targets and often victims may not even know they have been infected. Attackers are now highly aware of lax IoT security and many pre-program their malware with commonly used and default passwords.

IoT attacks have long been predicted, with plenty of speculation about possible hijacking of home automation and home security devices. However, attacks to date have taken a different shape. Attackers tend to be less interested in the victim and the majority wish to hijack a device to add it to a botnet, most of which are used to perform distributed denial of service (DDoS) attacks.

Just this month the security vendor Sucuri reported on a large DDoS attack launched from 3 different types of botnets (CCTV botnet, home router botnet and compromised web servers). While

Your Community Manager: RGMDonaldson

Welcome to the Security Community on Symantec Connect.

The Security Community covers many different security products from Symantec and provides valuable technical information for each.

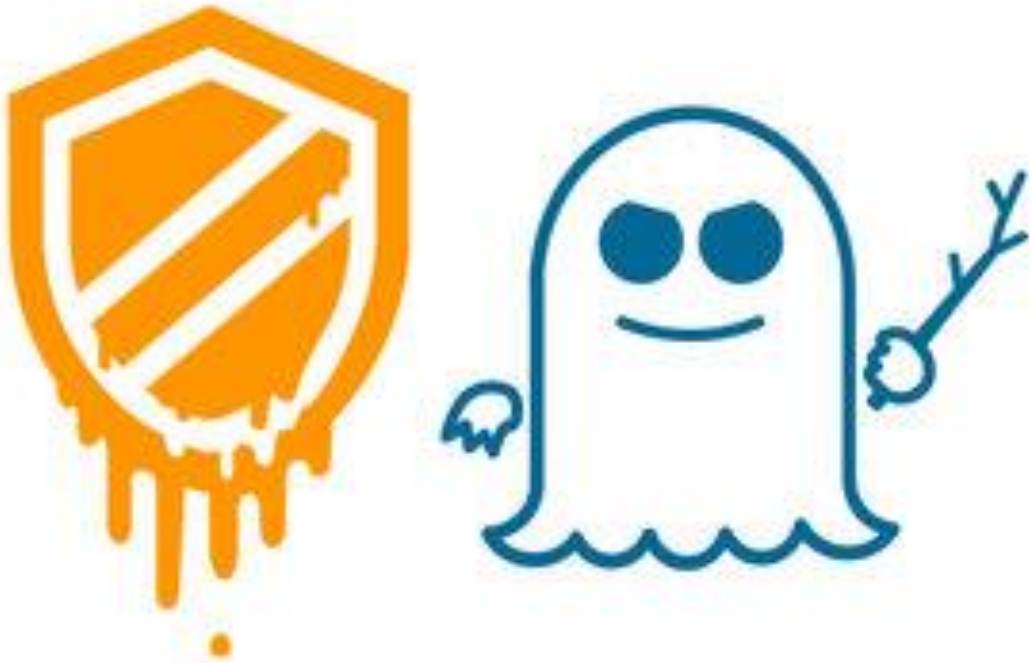
Please feel free to contact me via private message with any questions you may have.

I look forward to hearing from you and answering any questions about the Community.

Send a private message to the Community Manager

Top 5 Contributors: All Time

MEMBER	REWARD POINTS
Brian	135801
Vikram Kumar-SAV to SEP	77376
Mithun Sanghavi	74670



Hacking Team Leak Shows ×

www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work/

WIRED Hacking Team Leak Shows How Secretive Zero-Day Exploit Sales W

BUSINESS CULTURE DESIGN GEAR SCIENCE

SHARE

SHARE 143

TWEET

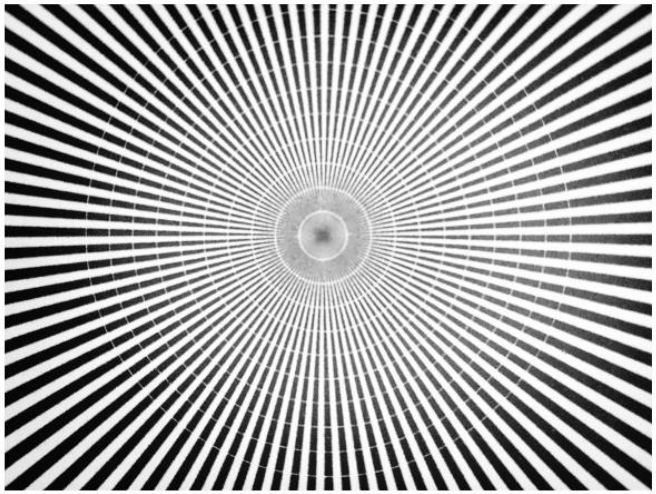
PIN 3

COMMENT 4

EMAIL

KIM ZETTER SECURITY 07.24.15 7:00 AM

HACKING TEAM LEAK SHOWS HOW SECRETIVE ZERO-DAY EXPLOIT SALES WORK

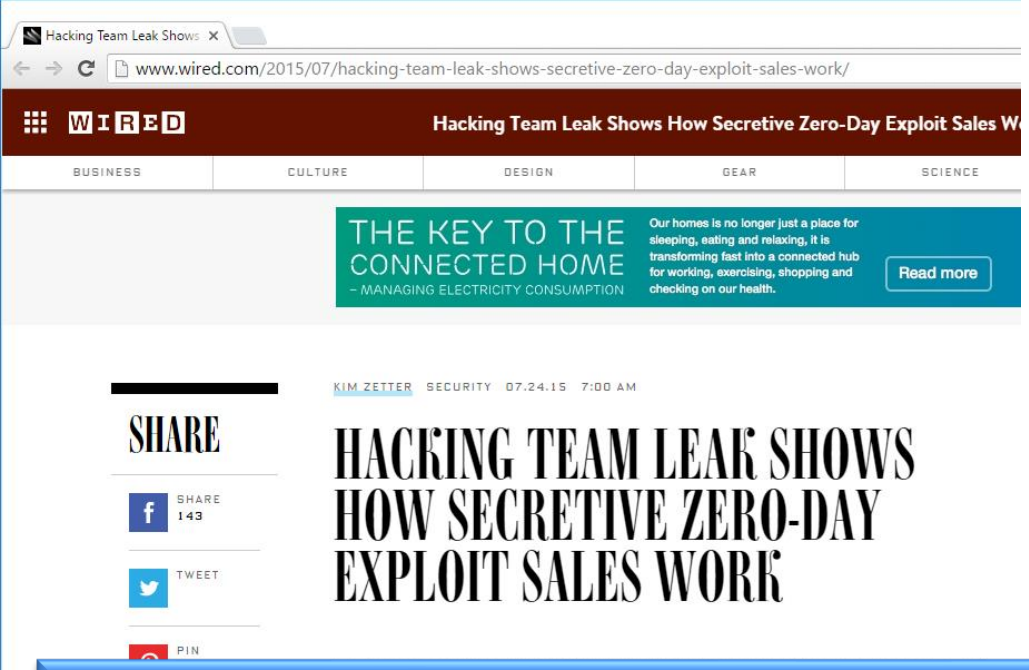


GETTY IMAGES

THE UNDERGROUND MARKET for zero-day exploit sales has long been a hidden dark alley to anyone but the hackers and sellers who call it home. But the recent hack of the Italian spyware maker Hacking Team, and the subsequent dump of 400 gigabytes of its internal emails, has shone a bright light on the nature of exploit sales, how they're negotiated, and

THE UNDERGROUND MARKET for zero-day exploit sales has long been a hidden dark alley to anyone but the hackers and sellers who call it home. But the **recent hack of the Italian spyware maker Hacking Team**, and the subsequent dump of 400 gigabytes of its internal emails, has shone a bright light on the nature of exploit sales, how they're negotiated, and how they've been kept in check by security protections.

It provides both the exploits and RCS to government intelligence and law enforcement agencies around the world, **and has come under attack for selling to repressive regimes, who've used them to target political activists and dissidents.**



THE UNDERGROUND MARKET for zero-day exploit sales has long been a hidden dark alley to anyone but the hackers and sellers who call it home. But the **recent hack of the Italian spyware maker Hacking Team**, and the subsequent dump of 400 gigabytes of its internal emails, has shone a bright light on the nature of exploit sales, how they're negotiated, and how they've been kept in check

It's long been known that zero-days can sell for anywhere between **$5,000 to half a million or more,** but seeing the price negotiations in writing provides new insight into the fluid value of zero-days.

Exclusive iOS exploits could cost as much as **half a million**, according to one of Hacking Team's sellers.

WikiLeaks - The Hackingte

https://wikileaks.org/hackingteam/emails/

WikiLeaks

Search Keywords

Shop | Donate | Submit

Hacking Team

Today, 8 July 2015, WikiLeaks releases more than 1 million searchable emails from the Italian surveillance malware vendor Hacking Team, which first came under international scrutiny after WikiLeaks publication of the SpyFiles. These internal emails show the inner workings of the controversial global surveillance industry.

Search by Terms in Email | Search by Attached Filename | Search by Email-ID

You must fill at least one of the fields below.

Search terms throughout whole of email:

You can use boolean operators to search emails.
For example **sudan rcs** will show results containing both words. **sudan | rcs** will show results with either words, while **sudan !rcs** will show results containing "sudan" and not "rcs".

Mail is From:

Mail is To:

Enter characters of the sender or recipient of the emails to search for.

Advanced Search

Archives 2006-2010

- Afghanistan
- Albania
- Algeria
- Andorra
- Angola
- Antigua
- Antigua and Barbuda
- Argentina

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

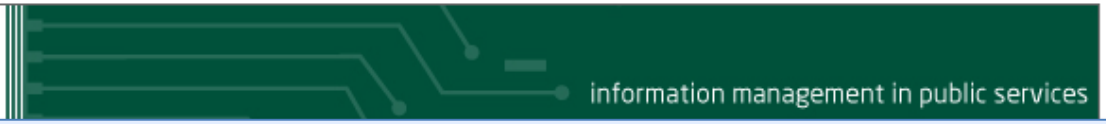
Log in or Register for enhanced features | Forgotten Password?

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.

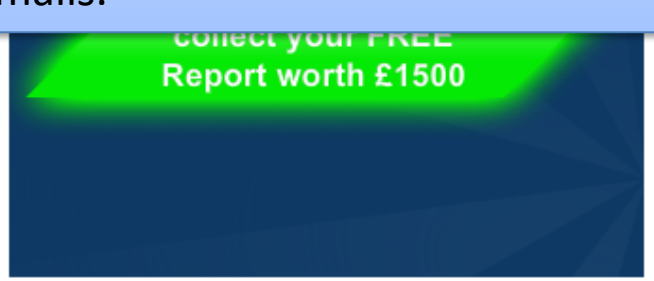
The suspected individuals stole money using the Butterfly **Botnet**, which steals credit card, and bank account information from computer users'.

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

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

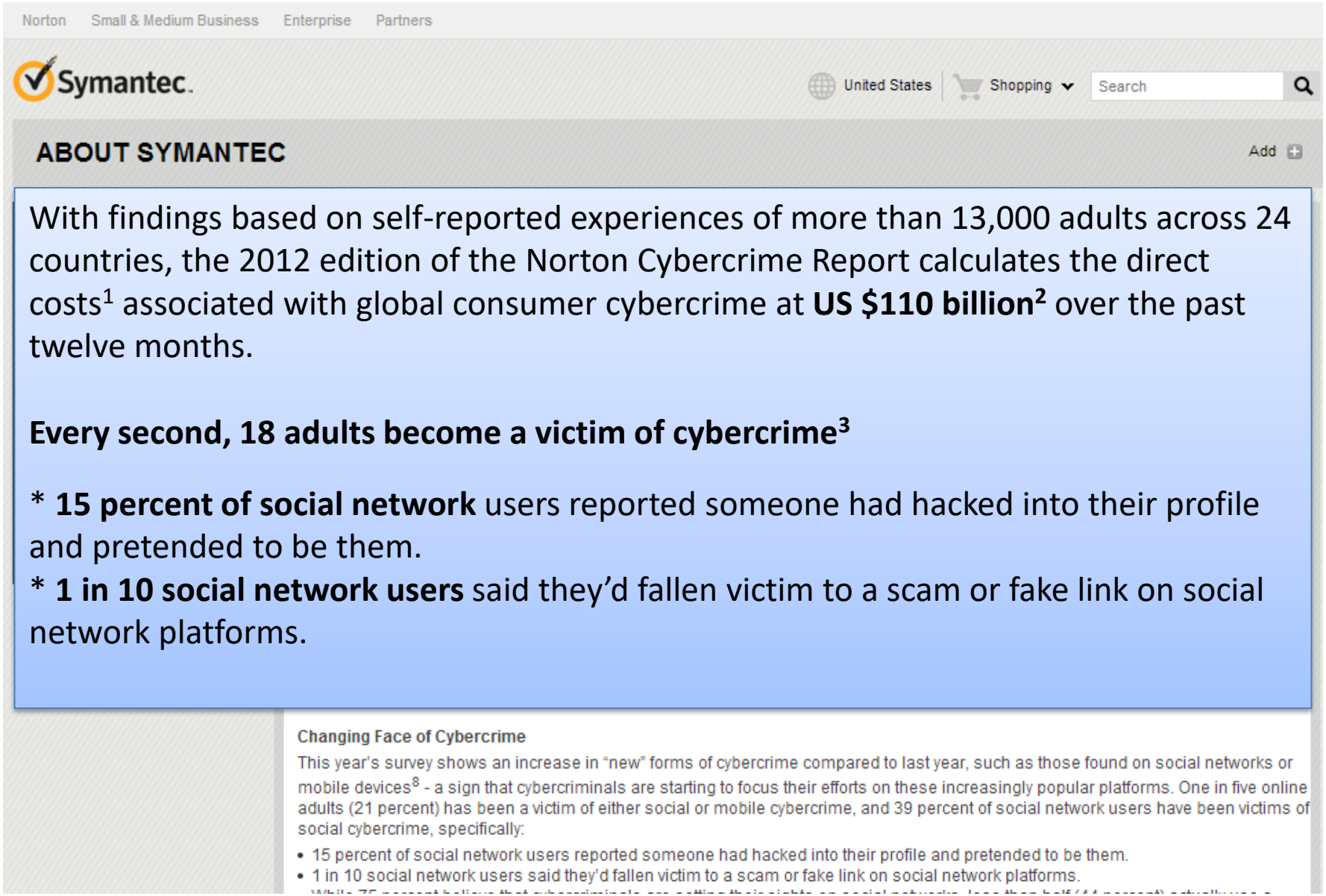
Mountain View, CA – Sept. 5, 2012 – Norton by Symantec (NASDAQ:SYMC) today released the findings of its annual Norton Cybercrime Report, one of the world's largest consumer cybercrime studies. The study is aimed at understanding how cybercrime affects consumers, and how the adoption and evolution of 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.

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.

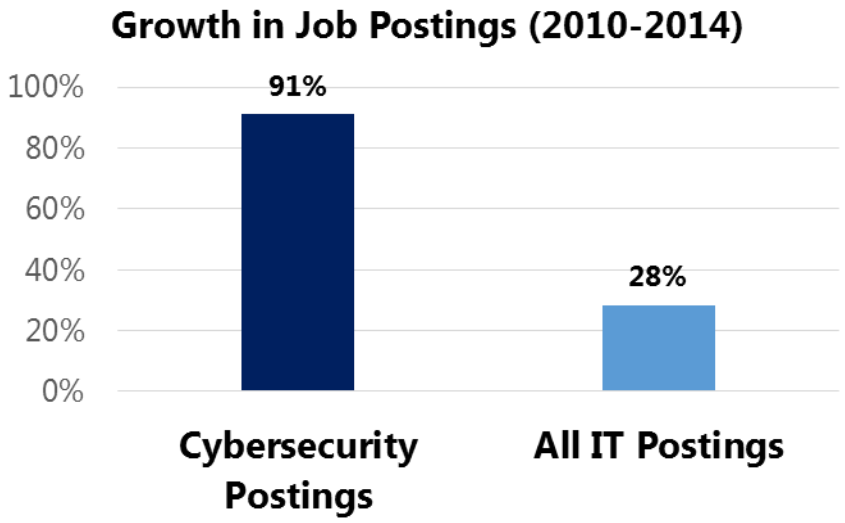
The Norton Cybercrime Report 2011 outlines the cost of cybercrime worldwide, with 74 million in the United States alone falling victim to online scams, phishing attacks and exploitative malware; costing the U.S. economy an estimated $32 billion.

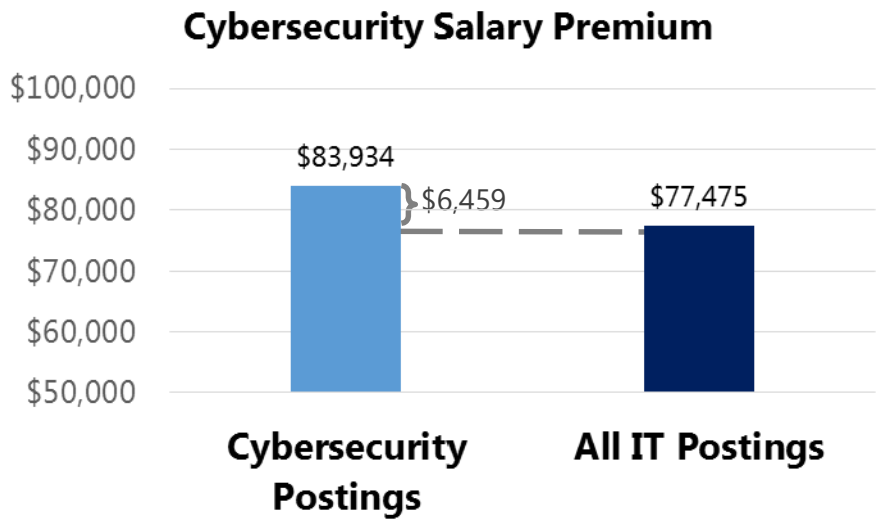
But the report suggests that more than 69 percent, at two-thirds of online adults, have fallen victim to cybecrime; a figure that is still on the rise.

Symantec, the anti-virus maker who issued the report, noted that it takes U.S. authorities nearly twice as long to resolve cybercrime than its British counterparts.

By the Numbers: The Cybersecurity Job Market

- In 2014, there were 238,158 postings for cybersecurity-related jobs nationally. **Cybersecurity jobs account for 11% of all IT jobs.**
- Cybersecurity postings have **grown 91%** from 2010-2014. This growth rate is more than faster than IT jobs generally.
- Cybersecurity posting advertise a 9% salary premium over IT jobs overall.
- Cybersecurity job postings took **8% longer to fill than IT job postings overall.**
- The demand for certificated cybersecurity talent is outstripping supply. In the U.S., employers posted 49,493 jobs requesting a CISSP, recruiting from a pool of only 65,362 CISSP holders nationwide.*





*According to the International Information System Security Certification Consortium, Inc., (ISC)² ® membership counts as of July 14, 2015

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.

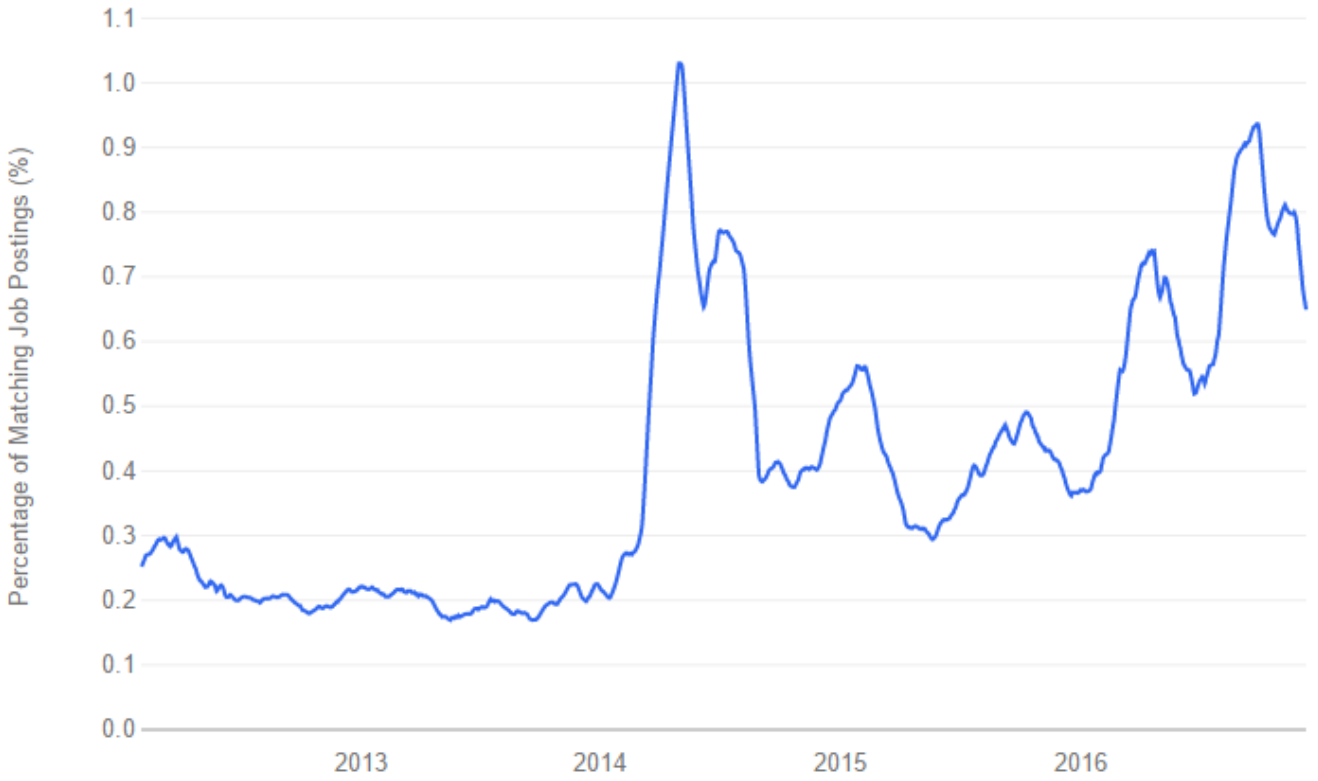
indeed Find Jobs Find Resumes Employers / Post Job Upload your resume Sign in

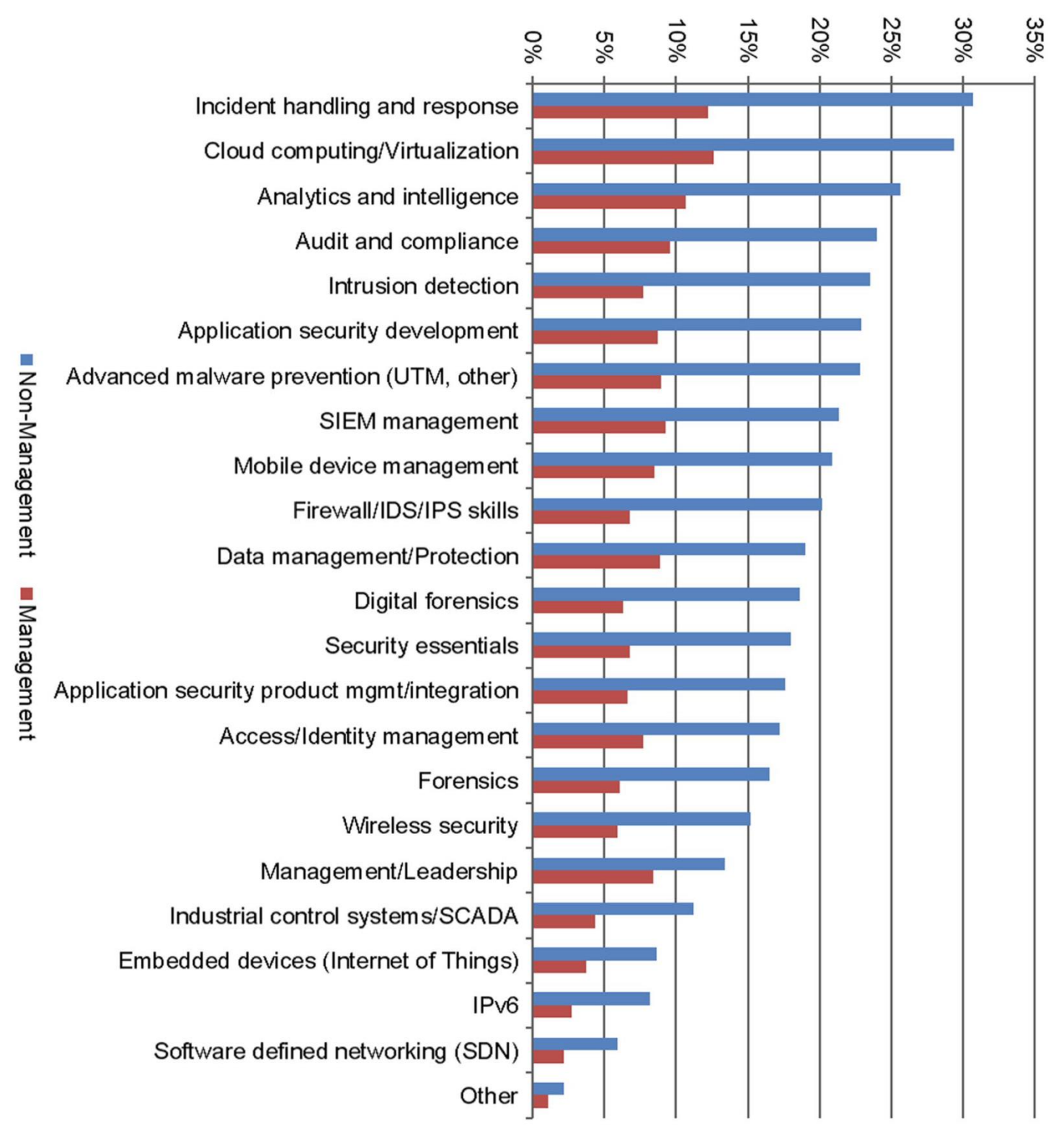
View Job Trends Navigation Menu

cyber security Job Trends

cyber security × + Add Term Find Trends

Job Postings





https://www.sans.org/reading-room/whitepapers/analyst/cybersecurity-professional-trends-survey-34615

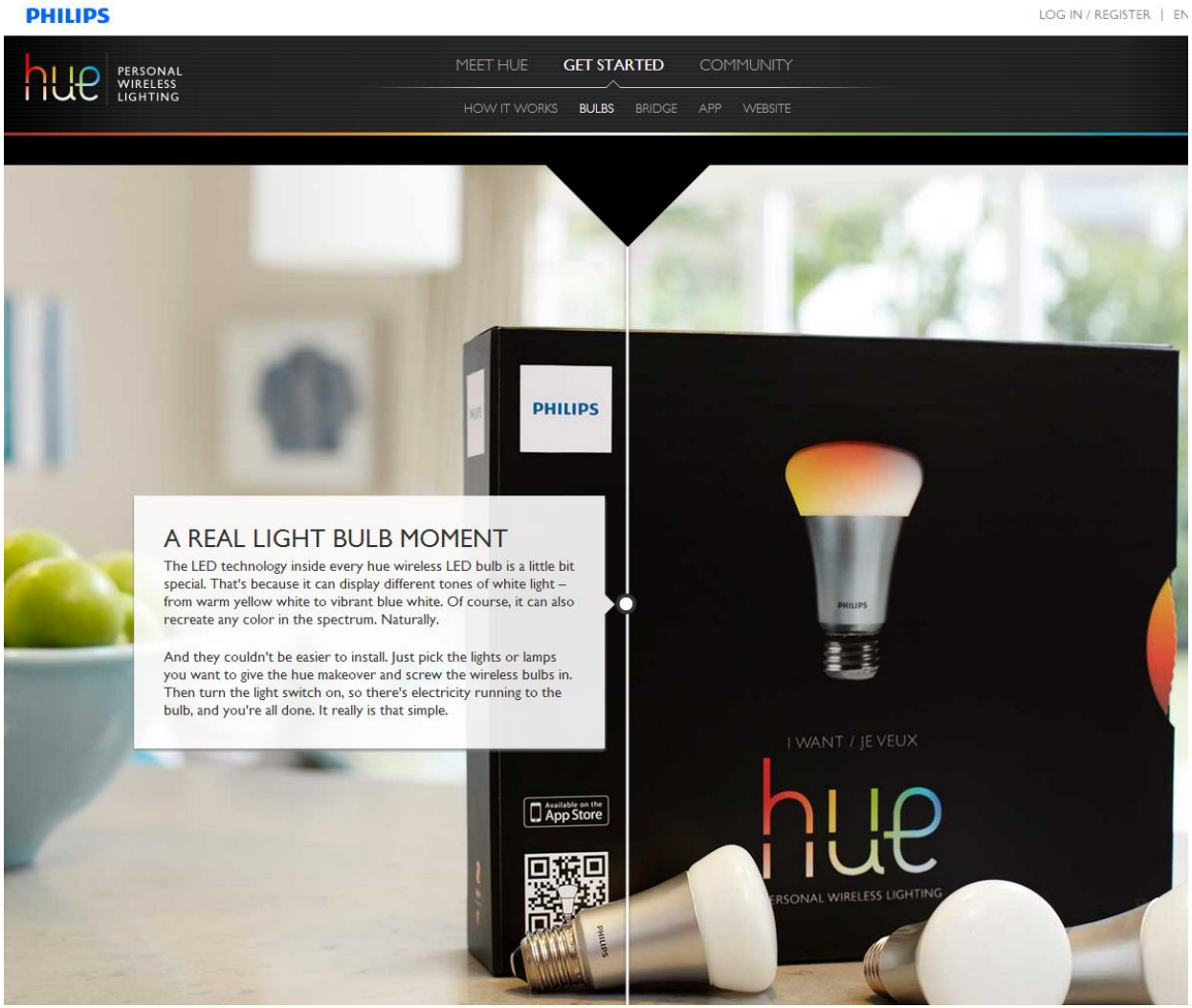
And not only traditional systems …

- 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
Hackad dator


kWh

And even lamps need security



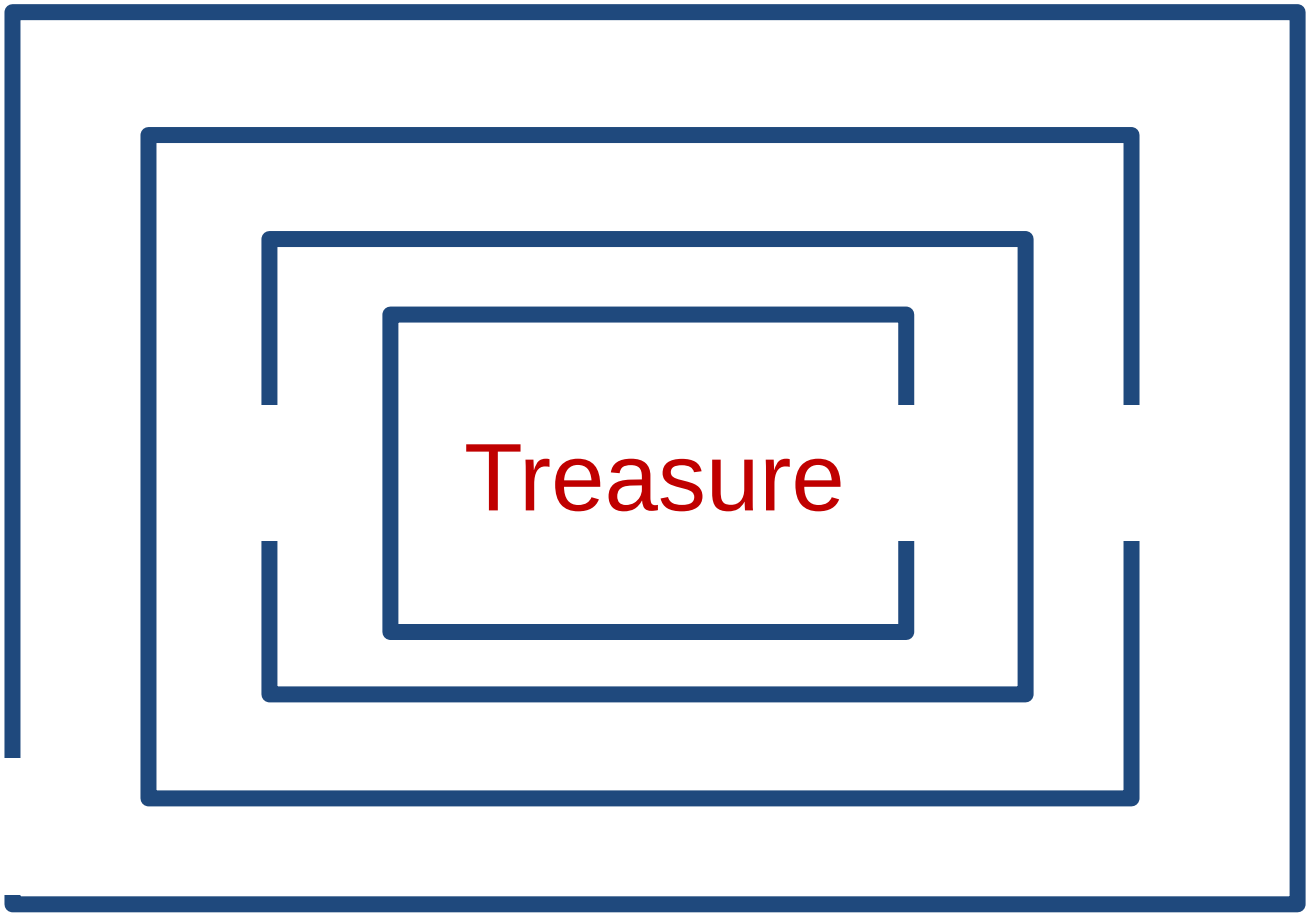
http://www.meethue.com/en-US

Distributed Denial of Service attack from IOT

- Unlike other botnets, which are typically made up of computers, the Mirai botnet is largely made up of so-called "internet of things" (IoT) devices such as digital cameras and DVR players.
- "100,000 malicious endpoints", and the company, which is still investigating the attack, said there had been reports of an extraordinary attack strength of 1.2Tbps.

https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

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 - 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, 2017/2018

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

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

Responsible for laborations

M.Sc Wissam Aoudi, email: wissam.aoudi[1]

Laboratory supervisors

M.Sc Carlo Brunetta, email: brunetta[1]
M.Sc Thomas Rosenstatter, email: thomas.rosenstatter[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,

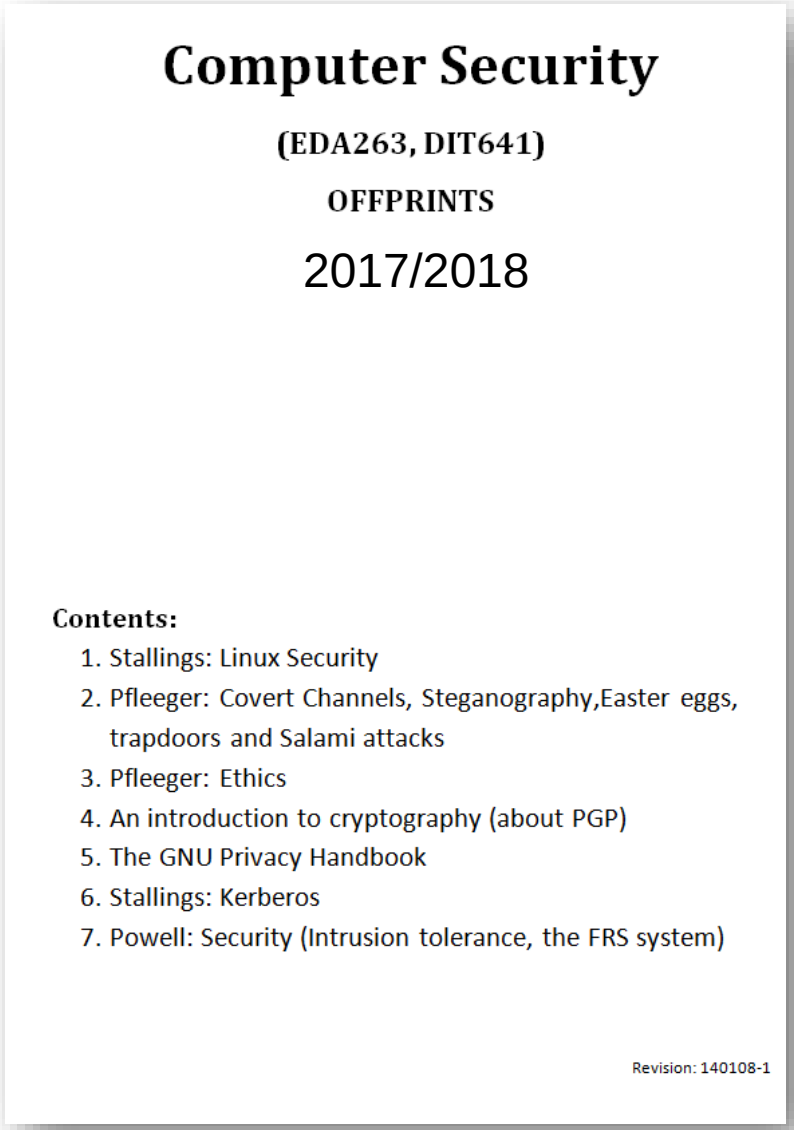
Pearson, second edition, ISBN: 978-0-273-76449-6

E-book at library

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.



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)

Example of reading instructions

2014-01-07

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

Course outline

- problems, definitions, concepts, taxonomies, ref to dependability
- threats, vulnerabilities, attacks, intrusions

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!

- security policies, risk analysis, certification, evaluation
- forensics, ethics

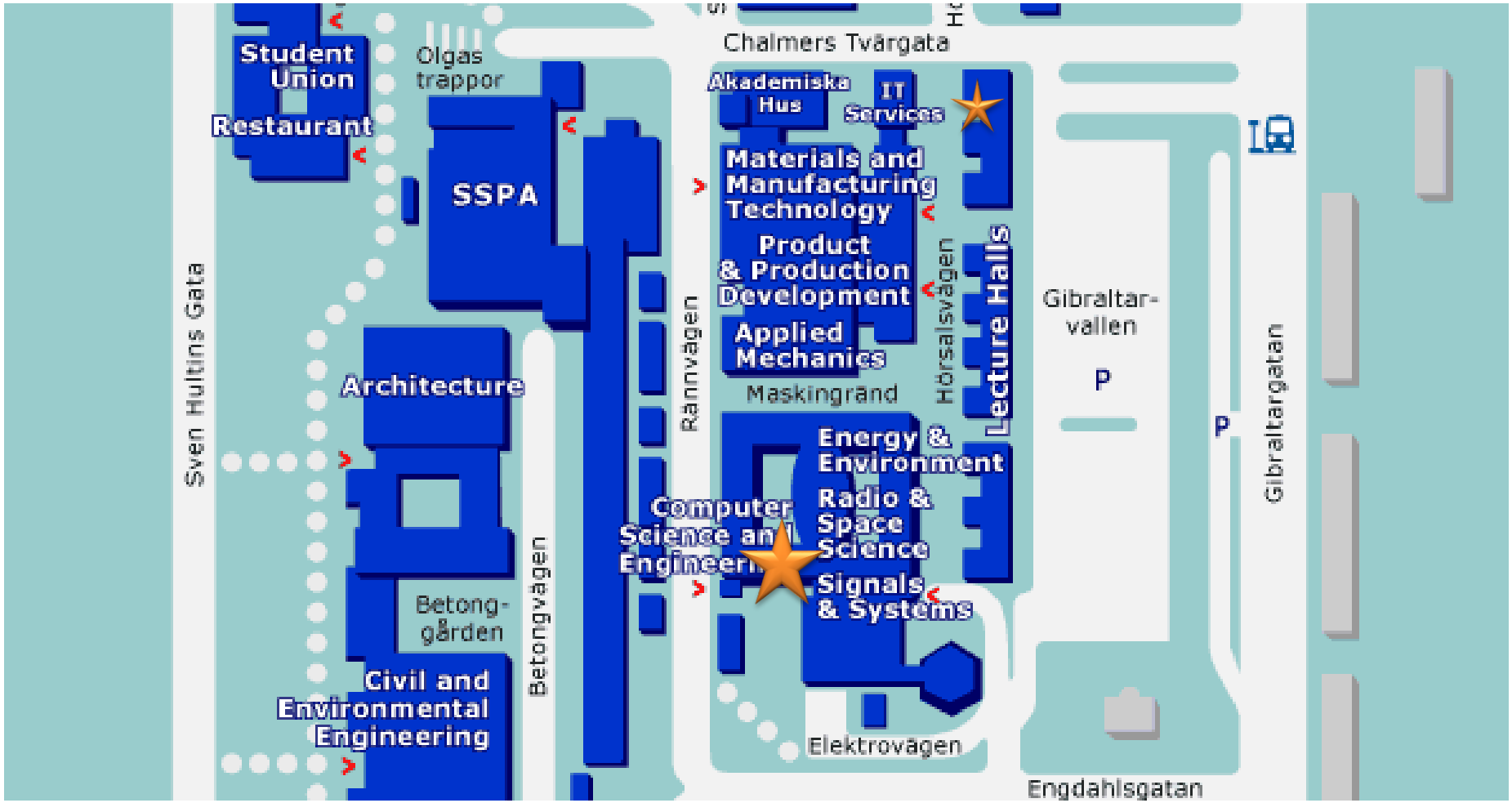
- laboratory exercises

Lecture plan (preliminary)

Lectures are given according to the schedule below.
The corresponding course material is listed in a separate document.

lecture					contents
L1	Mon	180115,	13-15,	HA4	course introduction, terminology, computer security basics
L2	Thu	180118,	10-12,	HA4	UNIX Security, authentication and access controls, authorization
L*	***Fri***	***1801**,***	***15-17,***	***HA4***	***<some Fridays will be used, check pingpong>***
L3	Mon				malicious software and vulnerabilities
L4	Thu				buffer overflow attacks
L6					introduction to cryptology, signatures, PKI, CA
L7					database security, injection attacks
L8					defensive programming, operating systems security basic
L9					network security basics, firewalls, deception systems
L10					intrusion detection systems, intrusion tolerance
L11					Common Criteria spam economics, computer forensics
L12					security and dependability modelling and metrics
L13					risk analysis , human and organisational factors
L14					security policies and models
L15					ethics, course summary, examination
L16					reserve
L17					reserve

Where is the course lab?



On the 4th floor