

Computer Security DD2395

<http://www.csc.kth.se/utbildning/kth/kurser/DD2395/dasakh11/>

Fall 2011

Sonja Buchegger

buc@kth.se

Lecture 14, Dec. 7, 2011

Final Lecture

Outline for Today

- About the course: recap, goals, topics, exam, next steps
- Questions from the first survey
- Relevance in the future

General Goals

- Learn about security concepts
- Have tools and methods to reason about security
- Spot threats, vulnerabilities
- Know and propose counter-measures
- Present concepts to others

Learning Outcomes

The students should be able to:

- recognize threats to confidentiality, integrity, and availability of systems; explain the basic computer security terminology and concepts and use them correctly
 - Throughout + principles
- find and apply documentation of security-related problems and tools Labs
- analyze small pieces of code or system descriptions in terms of their security, identify vulnerabilities of such code or descriptions and predict their corresponding threats
 - Labs, buffer overflows, viruses
- select counter-measures to identified threats and argue their effectiveness, compare counter-measures and evaluate their side-effects; present and explain their reasoning to others, in class e.g. IDS, FW, SW Eng., seminars, labs

Syllabus: Lectures Content

- L1: intro, admin
- L2: cryptography
- L3: authentication
- L4: access control
- L5: web attacks
- L6: malware
- L7: DoS
- L8: firewalls, MLS
- L9: social engineering
- L10: buffer overflows
- L11: models, MLS
- L12: audits
- L13: programming
- L14: recap

Syllabus: Lectures Content

- Concepts: intro, principles
- Prevention:
 - cryptography
 - authentication
 - access control
 - web attacks
 - firewalls, MLS
 - buffer overflows
 - secure programming
- Detection:
 - DoS
 - intrusion detection
 - malware
 - audits
- Response
 - human factors, policies
 - more prevention

Syllabus: Lab Exercises

- PERIOD 3 FOR BACHELOR'S STUDENTS
- See timeedit schema for times and rooms
- 4 different exercises, similar to p2, some changes
 - 1st: on GnuPG, remote or at CSC
 - 2nd: on iptables/firewalls, at CSC
 - 3rd: on web attacks, remote or at CSC
 - 4th: presentation at CSC, report, assess

Exercise 4

- Presentation and demo on computer security topic in a seminar
- Groups of 2-3 students
- Topic distribution on web site
- Group seminars, schedule in schema, signup on course website

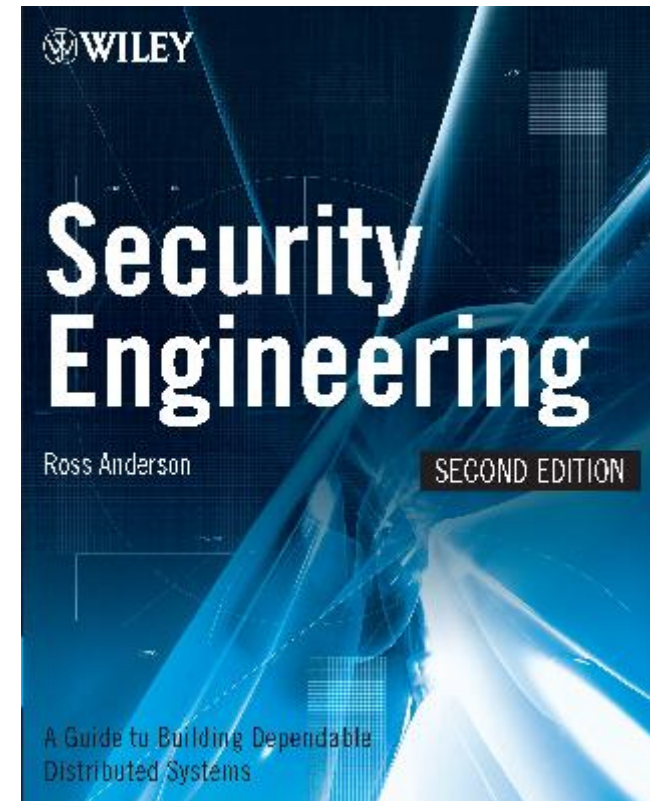
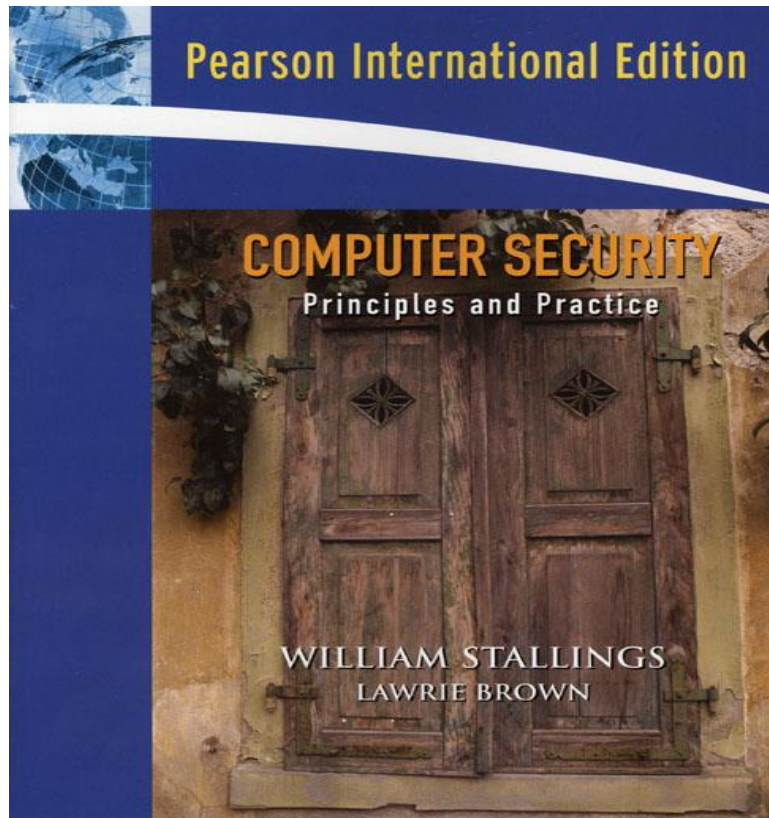
Exam

- January 10, 2012
- Re-exam in June 2012
- No registration needed, just show up

Assessment, Grades

- 6 ECTS in total, that's about 160 hours of work
- 3 ECTS Exam: A-F
- 3 ECTS Labs:
 - pass/fail, no grades
 - bonus points for overall grade (exam points) when handed in early, see lab descriptions

Books: Exam-Relevant Chapters



Next Courses

- Networking Security with Johan Karlander, CSC
- Foundations of Cryptography with Douglas Wikström, CSC
- Software Security with Dilian Gurov, CSC
- Networking and Systems Security with Panos Papadimidratos, EES

Course Analysis

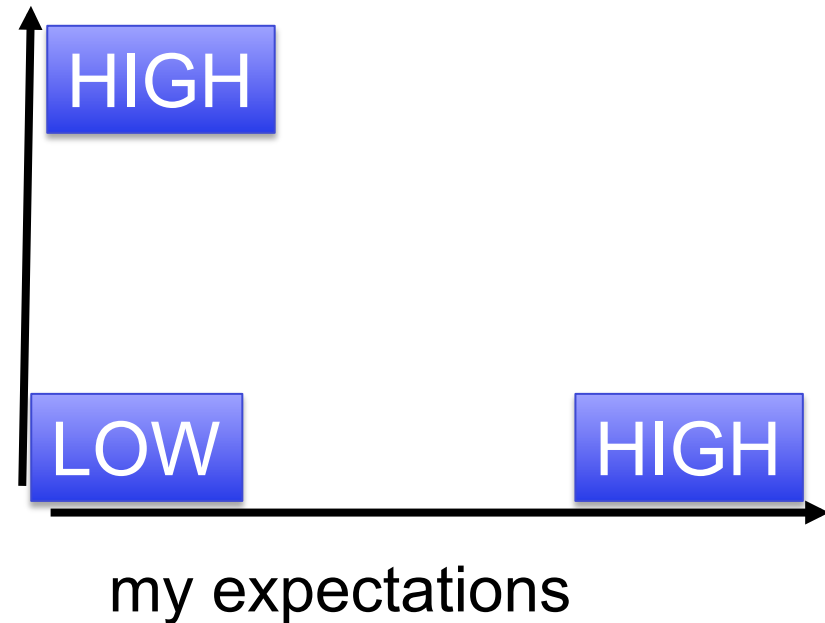
- Questionnaire up after exam results
- Another after labs in p3

Questions for you:

My most important question about the course:

my experience, knowledge

My most important question about computer security:



Questions?

- How can you be sure that you've eliminated every possibility of your program/network/system being hacked?
- How do I make a WLAN secure?
- Knowing how vulnerabilities are introduced and exploited so that programmes can avoid making the same mistake.
- Does it go through modern threats?

Questions II

- What is the patronus of Comp. Sci.?
- What will this be worth for if I start a small business?
- How is it practiced in reality?
- How to protect a system
- Can I succeed with the free literature?
- What's the most dangerous/serious security problem that computer systems face?

Questions III

- Web attacks used on existing systems, SQL injects and other basic techniques
- How do I become Voldemort?
- How secure are most companies that handle personal information e.g. Sony?
- What signifies a good security system?
- Is there a way to know if your program is 100% secure?

Questions IV

- Is it true that AV companies create viruses?
- How do I detect flaws in my own code?
- When does the Narwhale bacon?
- Will the first book cover everything on the exam?
- Iptables and web security
- Will any of the labs be useful for the exam?

Questions VI

- Why is everyone ignoring HW security?
- Can we stop quant computers from breaking in?
- When will you notice that I hacked you while you held this presentation?
- Will I be able to hack [redacted]?
- Is there a master password for CSC?
- Which are the most common attacks I should know about?

Relevance for You

- Which parts of what you learned about computer security in this course do you anticipate to use in the future?
- What can you use as a private person?
- What about your professional life?
- Any new-years resolutions for security?

Think and discuss!

As a User

- Personally, or in an organization
 - Authentication, passwords, roles
 - Social engineering
 - Policies
 - Firewalls, intrusion detection on your own machine
 - Online behavior
 - Crypto

As System Administrator

- Or consultant
 - Policies
 - Placement/configuration of firewalls, IDS, etc.
 - Processes
 - Audits, logging
 - Rights management, AC systems
 - User training

As Manager, Entrepreneur

- Resource allocation, how much to spend on what kind of security
- Processes/policies
- User training
- Audits, certification
- Client relations, secure data, availability

As Developer

- Programmer, SW architect, tester, quality assurance
 - Operating system specifics
 - Programs, web applications
 - Principles for design
 - Programming language specifics
 - Input checking, output checking, libraries, etc.
 - Memory management

As Researcher

- At a university or in industry
 - Attacks/defense (e.g. web attacks)
 - Usability v. security
 - Crypto (new algorithms, cryptanalysis, new applications)
 - Privacy Enhancing Technology
 - Computer Forensics

Topics Wishlist

- What topics would you like to know more about?
- Think, discuss, call out or e-mail to buc@kth.se

A close-up portrait of Severus Snape from the Harry Potter series. He has long, dark hair and is wearing a dark, high-collared robe. He has a serious, somewhat stern expression. The background is dark and out of focus, with some light reflecting off a surface to the right.

CSC honor code, plus:

**Defense Against the Dark Arts:
Do not attack a running system
without the consent of the owner
and the users!**

More Questions!

- How hard is it to hack a WPA-2 encrypted WiFi
- How do the AV programs actually block different types of attacks?
- What will be the biggest security issue in the future?
- How do I secure remote patching services from corruption?

Still More Questions!

- Why does protection feel too irrelevant to people and why to change attitudes
- Wow would my security knowledge compare to real-world security experts after finishing this course?
- Is the SSL certificate authority model fundamentally broken?
- Will legal issues be covered?

Oh, More Questions!

- What are the necessary settings to adjust for a Linux server connected to the Internet for a long period of time without an external firewall?
- Will we write an automat designed to launch sequential attacks on a subsystem to cripple the main system or will we primarily perform all attacks manually?
- Will it blend?