Computer Security

Tom Chothia

Introduction Lecture 1

Today’s Lecture

- An introduction.
- Lecture schedule.
- Module details.

Computer Security

- Techniques:
  - How do I make this particular system secure?
  - How does this attack work?
- Policy:
  - What does this business need to do to be secure?
  - What are the biggest security threats to this project?
  - How much should we spend on security?

Goals: The CIA Properties

- **Confidentiality**: attacker can’t read your data
- **Integrity**: The data I receive is genuine.
- **Availability**: I can get my data when I need it.

Goals

- It's safe to enter my credit card number into this website.
  - **Confidentiality**: outside attackers can't see my CC no.
  - **Integrity**: The website really is the shop I think it is.
- It's safe to submit my homework using BOSS:
  - **Integrity**: my homework is received correctly.
  - **Availability**: I will be able to submit my work before the deadline.

Other Goals

- Privacy: No one can monitor what I'm doing.
  - Do I trust Google?
  - Could use proxies, delete cookies.
- Reliability: The website won't loose my data.
  - Proper back ups
- My data isn't left on a train
  - Business has a good USB stick policy.

Attackers

- Lone Hackers, script kiddies.
  - Probably run known attacks using scripts.
- Professional Criminal gangs:
  - Take control of 100,000's of computers via bugs in web-browsers
  - Spam, phishing attacks.
  - DoS attacks
- Governments:
  - Unbelievable computing power
  - Wiretaps
  - Lawyers
- ISPs, Service providers
  - Don't break laws.
  - Do "spy" on you.
  - May sell/loose your data
- Insiders.

Assumption About the Attack

- We normally assume that the attacker is as strong as possible, but cannot break our crypto.

  "The attacker owns the network"

- Most attackers are much weaker than this.

- Bad crypto can be broken.

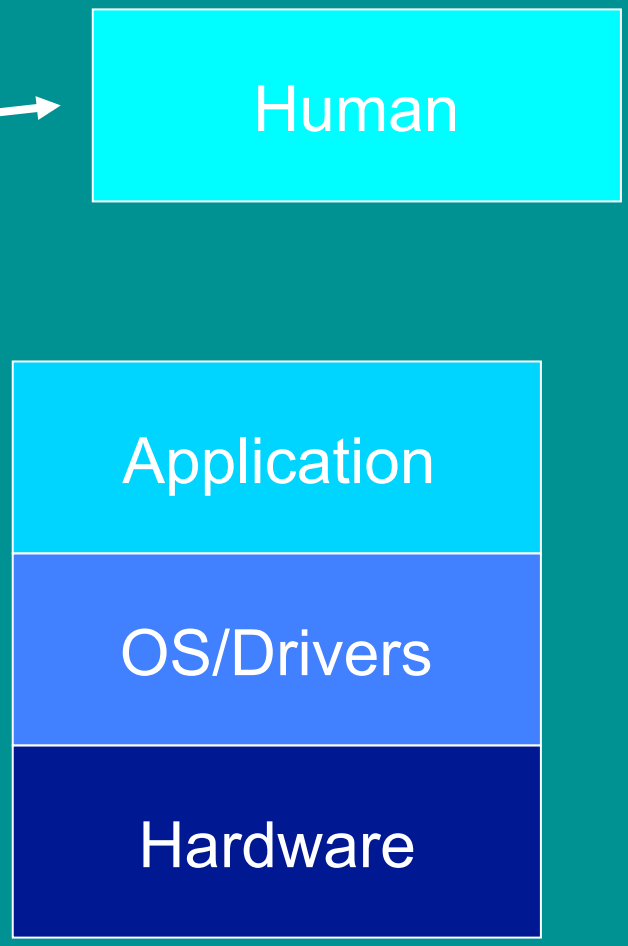
Levels of Attack

Phone user and pretend to be IT support

Attack an unpatched web browser

Exploit a buffer overflow in a driver

Open case and read disk



Tutorials

- Lectures will move quickly.
- Each week (from week 2) you will have a small group meeting with a tutor to discuss the lecture content.
- You can also e-mail your tutor with specific questions.
- Tutors will be assigned next week.

Lab Sessions

- From week 2, on Wednesday from 10-12 there will be a lab session.
- From 10 until the lab is empty, tutors will be available in the lab to answer any questions you may have about:
  - the practical content
  - the exercises
  - tools described in lectures.

Resources

- Lecture slides,
- Website:
  - Lecture slides ***(with audio)***
  - Links to supplementary material,
- My office hours:

  Tuesday 15:00 -16:00 Room 111

Web Page

http://www.cs.bham.ac.uk/~tpc/CompSec/

- All changes to the lecture timetable
- Lecture slides.
- Exercises.
- Further reading.

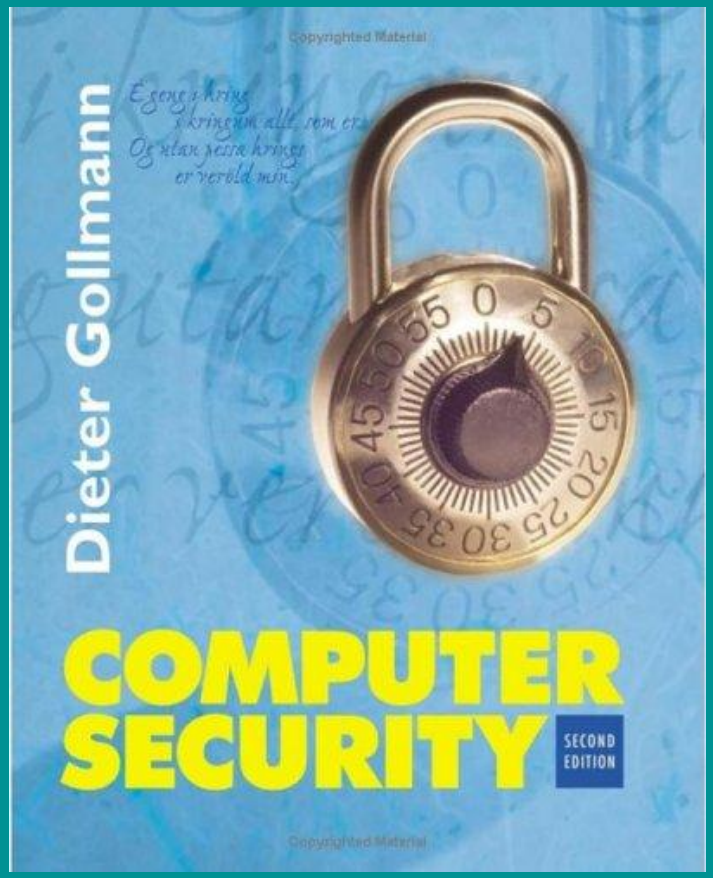
Social Networks

- A Facebook group for questions and discussion:
  - BhamComSec2011
- A twitter feed @UoBCompSec

Books

You don't need to buy a textbook for this module.

Gollman, is good for the first few lectures on techniques.

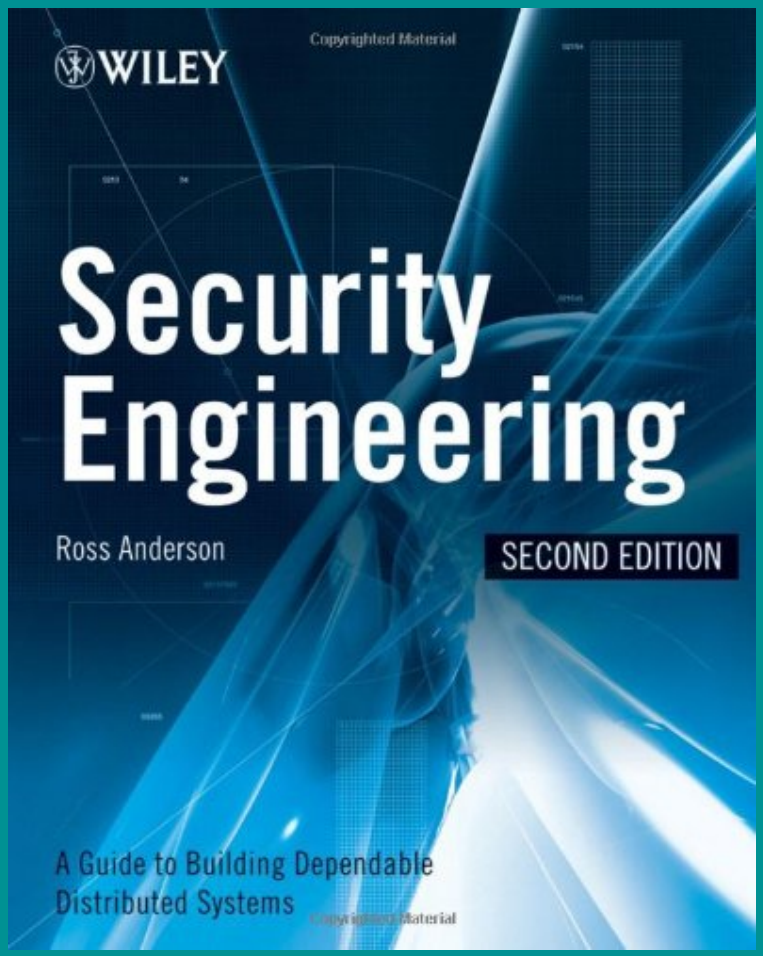


Books

Anderson, is also good.

First edition is fine and can be downloaded for free.

Google
"Ross Anderson".



Live Demos

- These lectures will include lots of live demos.
- All live demos are risky, some will go wrong, e.g.,
  - Dropped network connections
  - Crashed program.
- If you want to be shown how to do a demo yourself, see me or a tutor during a lab session.

Recommended Paper

- Each week I will recommend a paper to read that supports the material taught.
- The exam and exercises will be possible without reading these papers.
- But reading them will really help.
- This weeks paper: “Stalking the wily hacker” by Clifford Stoll

Required Knowledge

This is an advanced module:

- Exercises 1 and 3 require you to know Java.
- Exercise 2 requires knowledge of how websites work. (HTML, SQL, HTTP, …).

There will be a refresher lecture on each subject, but if you don’t already know this stuff you will need to do a lot of work to catch up.

Questionnaire

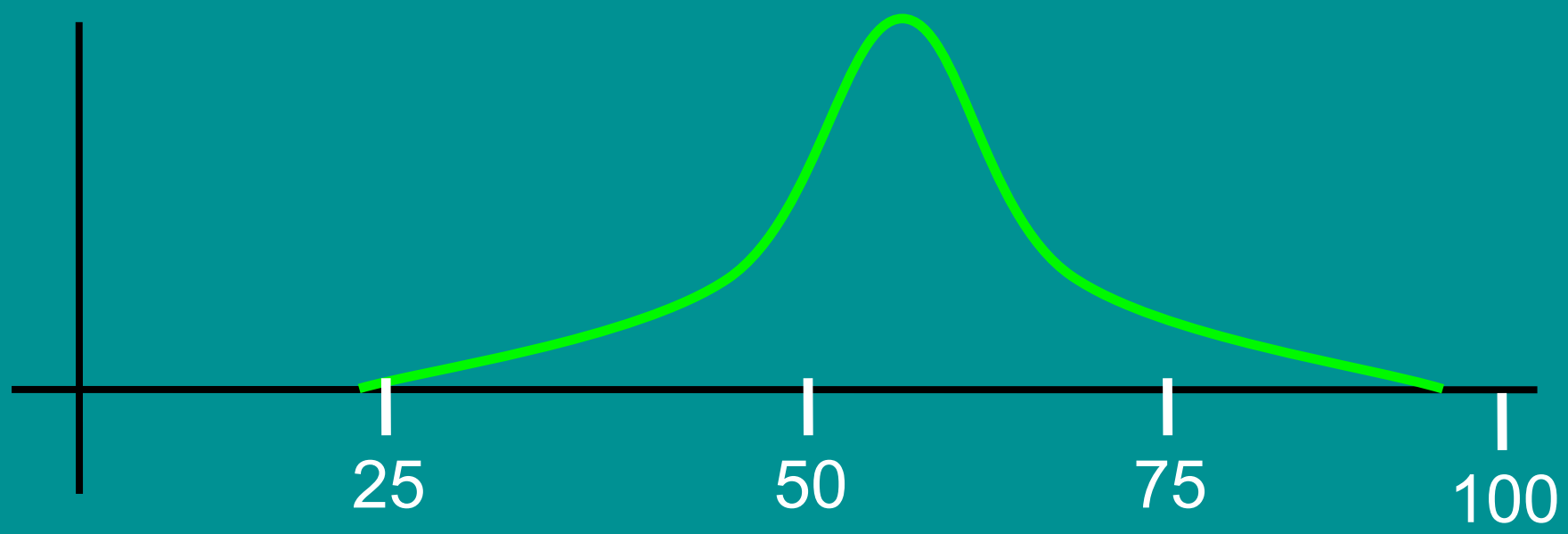
- If you want to take this module, you must fill out the questionnaire.
- Fill out the questionnaire and come and see me on Tuesday afternoon or Wednesday morning (Room 111).
  - There will be a sign up sheet on my door.

Work Required

- 4 marked exercises, ~2 weeks each, full time.
- This module has a ***major*** course work requirement (40% of 20 credits).
- This is a very intensive course, expect to work harder than you ever have before.
- ***You cannot leave exercises to the last week.***

Marks

- 40 pass, 60 Merit, 70 Distinction.
- Distribution of marks:



DO NOT TRY OUT ANYTHING ON COMPUTERS YOU DON'T OWN

- It is illegal to access computers without the owner's permission.
- Most access is logged, and it's easy to get caught.
- Trying something "just for fun" could get you kicked out of the University.

Plagiarism

- All exercises must be your own work.
- No group work is allowed.
- Any plagiarism or illegal computer use will result in immediate removal from the module.
- If you have any doubts about what is not allowed see me, during my office hour.

Next Week

- Symmetric Key Encryption Ciphers
  - Frequency Analysis
  - One time pads
  - AES, DES and 3-DES
- Block cipher modes
- Truecrypt