# Computer Security DD2395 dasak21

https://canvas.kth.se/courses/27095

Fall 2021

Sonja Buchegger

buc@kth.se

Introduction

# Topic for Today: How To Dasak

ILOs: After this lecture, the students will know

- how the course works and where to get information
- what they are expected to do and when
- what perspective and mindset works well
- the basic concepts of security

After this lecture, the teacher will know

- the students’ prior knowledge
- what motivates them
- the most important questions about the course and security

# 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

# Mindset: Adversarial

Murphy’s law, only less naive.

”Whatever can go wrong, will go wrong.”

Usual interpretation: stuff happens.

In security: stuff happens on purpose (attacker)

“It’s not paranoia if they’re really after you”

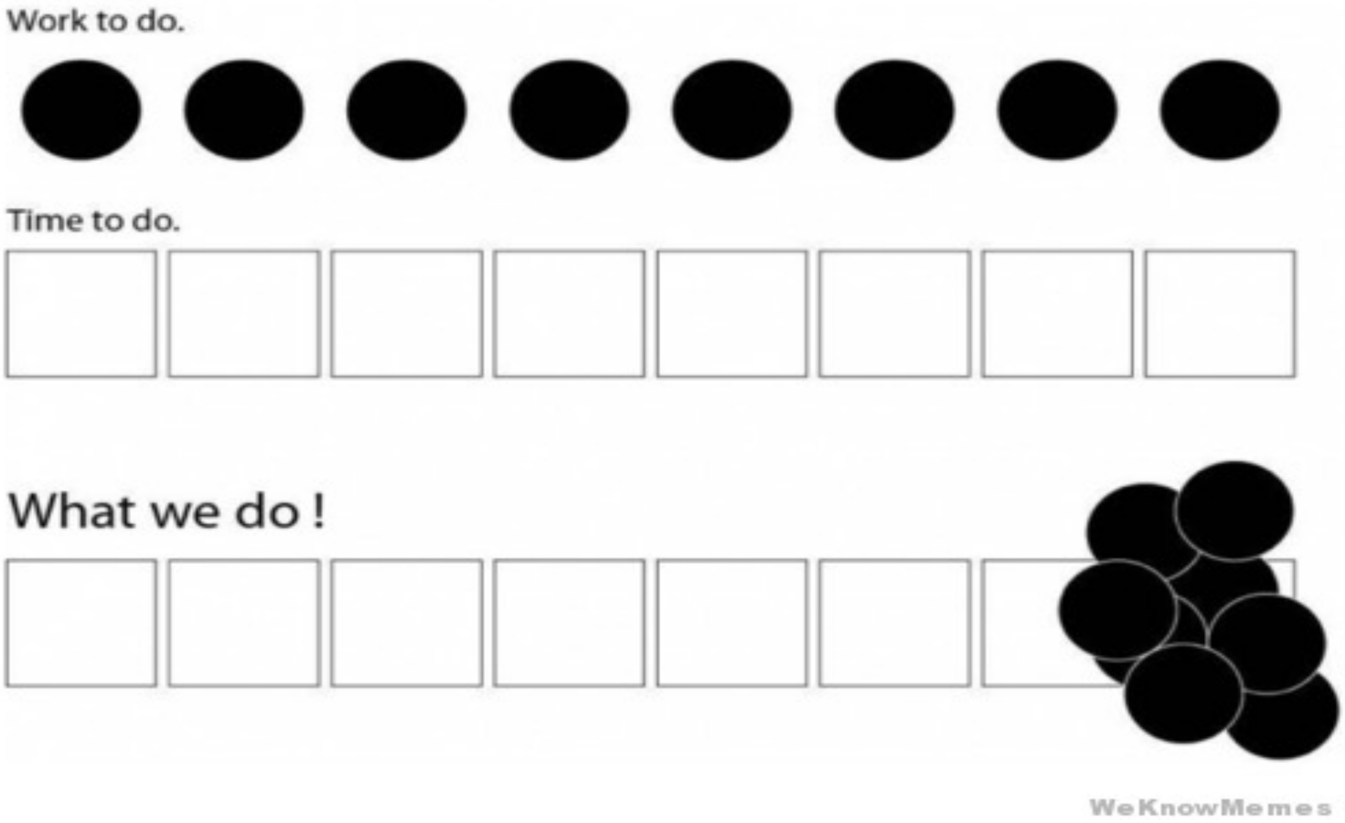
Defense against the dark arts course.

# Mindset: Accurate

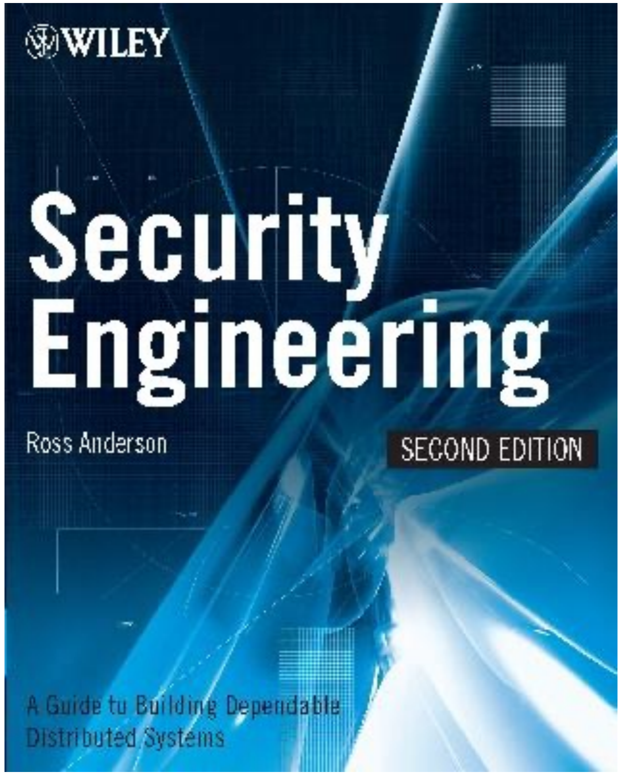
- Careful, meticulous, details matter.
- Approximately OK is not enough, leaves vulnerabilities.

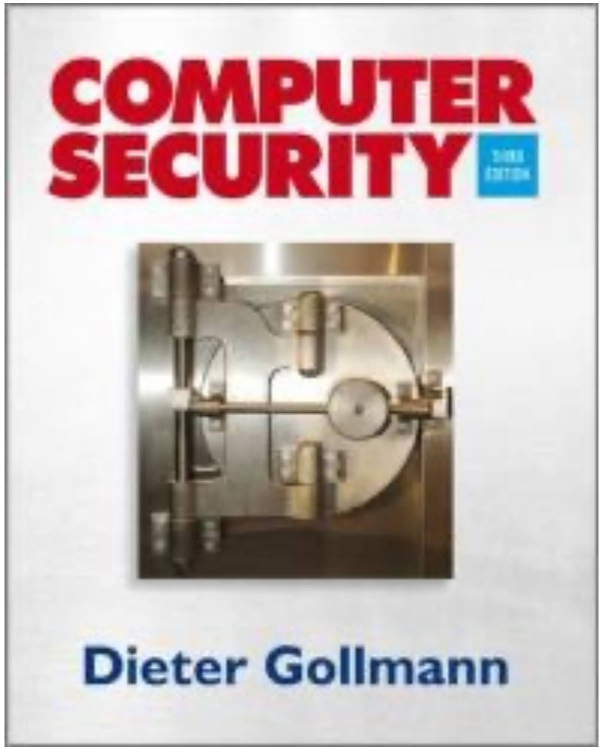
# Mindset: Anticipating

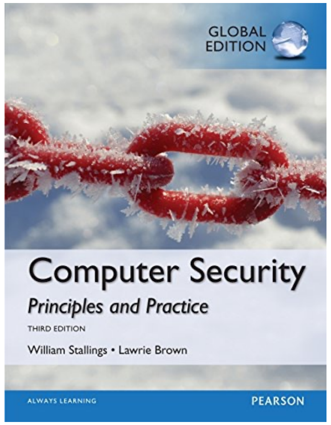
- Anticipate adversarial behavior, prevention
- Anticipate in terms of time, proactively



# Books


WILEY
Security Engineering
Ross Anderson
SECOND EDITION
A Guide to Building Dependable Distributed Systems


COMPUTER SECURITY
THIRD EDITION
Dieter Gollmann


GLOBAL EDITION
Computer Security
Principles and Practice
THIRD EDITION
William Stallings • Lawrie Brown
ALWAYS LEARNING
PEARSON

# Components:
# lectures, labs, seminar, exercises

# Lectures, flipped classroom

- Watch pre-recorded videos and read material in your own time before the scheduled class
- In class, we go through old exams, questions about the topic, and relevant current news. Not recorded.

# Lab Assignments (3 ECTS)

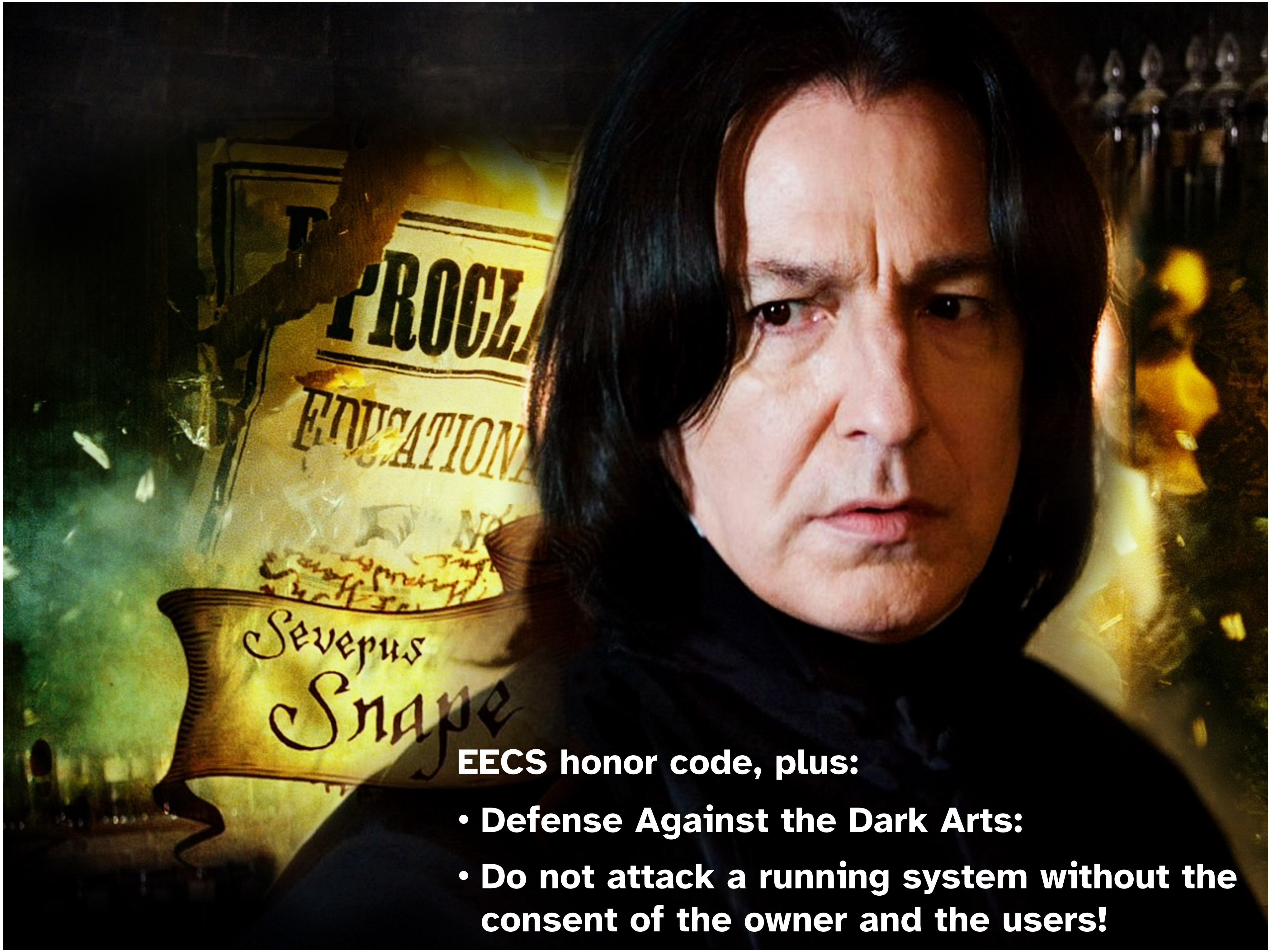
- See timeedit schema for lab sessions and posted info on how they work (tl;dr: you make zoom rooms, get in queue, TA joins you)
- 5 different ones: 4 lab assignments, 1 seminar
  - G: on GnuPG (individual)
  - F: on firewalls (group)
  - O: on buffer overflows (individual)
  - W: on web attacks (group)
  - S: presentation, report, assess (group, individual peer review)

# Finding Lab/Seminar Partners

- Discussion thread in Canvas
- Assigned by teachers if not in formed groups

# Seminar

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



EECS honor code, plus:

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

STAY PARANOID AND TRUST NO ONE

# Course Information on Canvas

Check notification settings

Check course on Canvas regularly for updates

During the lecture we went through the Course Memo. If you missed the lecture, read the Course Memo. If you were present at the lecture, read the Course Memo again.

# Course Responsible Students

- Select 2 course responsible students amongst yourselves (more info on Canvas)
- Purpose/Task: Discuss course evaluation questionnaire results, other feedback

Contact me if you are willing to do this

# What is where on Canvas

- We went through the course memo, module setup, and assignments

# Mentimeter: Status Quo

- add answers
- see answers by everyone

# Unusual Times, Unusual Methods

- It’s challenging to study from home. What can/will you do to make it easier?
- How can you create the conditions such that you get the most out of the course, i.e. check videos and material before class?
- What do you find motivating?

- Think about it yourself for a few minutes, jot down thoughts
- Join breakout room and discuss for 10 minutes
- Write down your answers, post them on menti.com 8879 2931
- add answers
- see answers by everyone

# Next Courses, Track on Security & Privacy

- Applied Cryptography with me, Douglas Wikström and others
- Foundations of Cryptography with Douglas Wikström
- Software Safety and Security with Cyrille Artho
- Privacy-Enhancing Technologies with me
- Networked Systems Security (project) with Panos Papadimitratos
- Systems Security Projects with Roberto Guanciale
- Parallel and Distributed Computing with Mads Dam
- Ethical Hacking with Pontus Johnsson
- Security of Large-Scale Systems with Robert Lagerström
- Hardware Security with Elena Dubrova