Computer Security and Privacy (COM-301)

Preliminaries - Fall 2024

Instructor: Prof. Edouard Bugnion
edouard.bugnion@epfl.ch

Course by Prof. Carmela Troncoso
SPRING Lab
noreply-maternityleave@epfl.ch

About Prof Troncoso

SPRING
SECURITY AND PRIVACY ENGINEERING LABORATORY

Building secure and privacy-preserving systems

Private communications, machine learning, applied cryptography, privacy evaluations

PhD - KU Leuven

MsC Telecomm Engineering - University of Vigo

Secure and Privacy Technical Lead - Gradiant

Associate Professor at EPFL

Senior Researcher at IMDEA Software Institute

About
Prof Bugnion

Stanford University

18y

California

Switzerland

EPFL

12y

vmware

NUOVA SYSTEMS / CISCO

Data Center Systems Laboratory

Special notice – 2024 only

This is a mature class, with a clear set of policies prepared over the years by Prof Troncoso (not this year's instructor)

Please do not ask for any changes in policy; they will not be granted.

The team

Prof Bugnion

Class in English

Klim Kireev
he/him
(TA)

Mathilde Raynal
she/her
(TA)

Boya Wang
Any pronoun
(TA)

Saiid El Hajj Chehade
he/him
(TA)

Malo Perez
he/him
(TA)

Christian Knabenhans
he/him
(TA)

Marwan Azuz
he/him
(AE)

Hugo Majerczyk
he/him
(AE)

Florian Kolly
he/him
(AE)

Pierre-Hadrien Levieil
he/him
(AE)

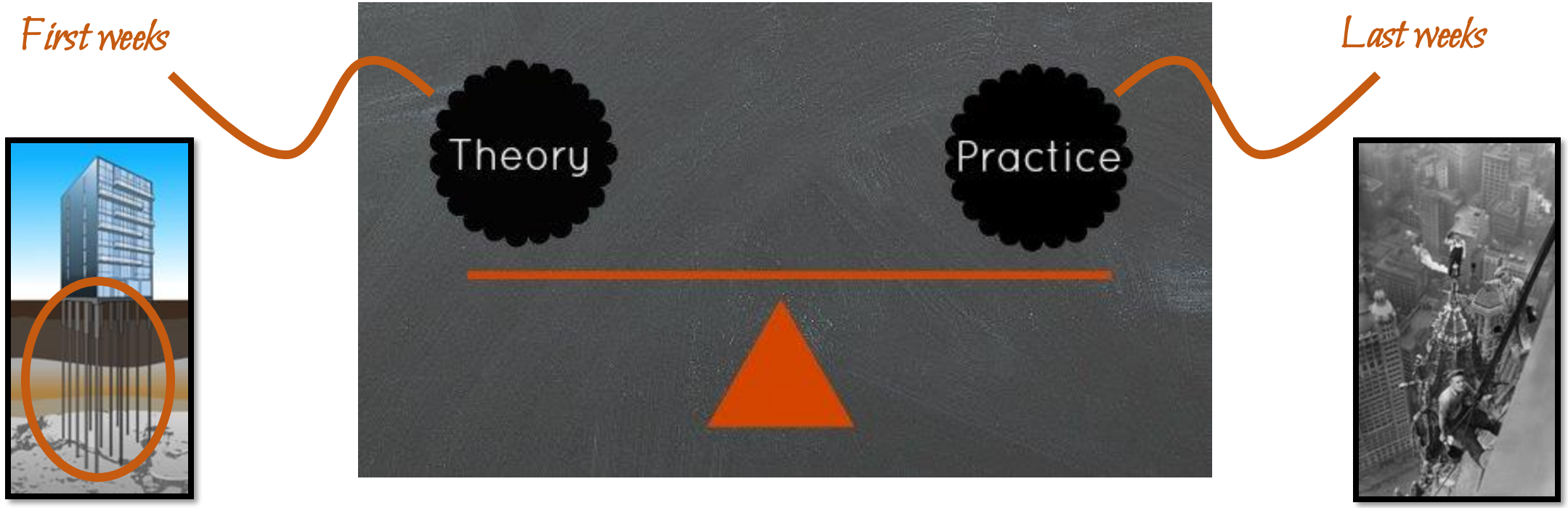
This course does **not** aim to

Train hackers

- You will learn concepts very relevant to hacking
- And do some hacking during your homework
- But to really hack, sign up for the CTF Team (see end of presentation)

Course Aims

1) Understand **basic concepts and principles of security** design and engineering that will **outlast current technology**



Course Aims

2) Learn to **model threats** and **think critically** about security problems

"adversarial thinking"

Keep the change program – Bank of America

If you purchase something for X dollars and Y cents (so 0<Y<0.99) they charge you X+1 and put (X+1-Y) in your savings account. If you buy coffee for $2.75, they charge 3 and put 0.25 in your savings.

The first three months, they do not charge the +1, just add the cents to the savings.

What can go wrong? How would you take advantage of the system?

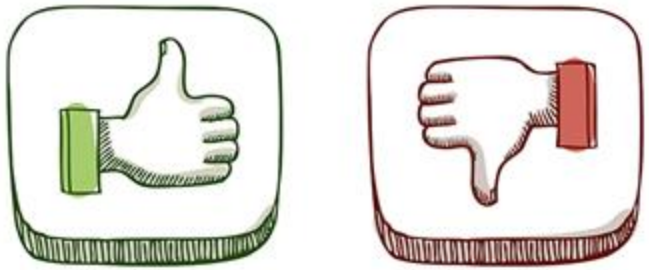
"Good engineering involves thinking about how things can be made to work; ***the security mindset involves thinking about how things can be made to fail****. It involves thinking like an attacker, an adversary or a criminal." – Bruce Schneier*

https://www.schneier.com/blog/archives/2008/03/the_security_mi_1.html

Course Aims

3) Get familiar with a number of security mechanisms, learn their purpose and limitations building a **toolbox for security engineering**

Knowledge of tools and mechanisms



Evaluate pros and cons in different scenarios

Departure point for further search

Topics we will cover

Principles of Computer Security

Access Control

Applied Cryptography

Authentication

Attacks and Malware

Software Security

Web & Network Security

Privacy

Course Organization

Tuesday 15-16 CE4, with overflow in CM011:
Lectures.

Later in the week:
Recording of Prof Troncoso's lectures

Tuesday 16-17 CE4, with overflow in CM011:
Live exercises (whole class).

Thursday 8:00 – 9:00 (3 exercise rooms):
Q&A time about programming homeworks and theory exercises.

Thursday 9:00 – 10:00 (one of 3 exercise rooms):
Live exercises (in groups).

Programming homeworks
Theory exercises

Tuesday 15-17

Lectures will start at 15:15 on Tuesdays (CE4, overflow room CM011)
Slides provided in advance (without speaker notes)
No streaming or taping

Followed by an interactive exercise solving / discussion on the lecture topic (to be completed on Thursday if necessary).

Prof Troncoso's "covid" lectures of the base material will also be published:
https://mediaspace.epfl.ch/channel/COM-301+Computer+security/29347

NB1: Video has only the lecture, does not include the live exercise / discussion
NB2: if you attend the Tuesday lecture, you do not need to watch the video

Thursday 8-10

8h15 - 9h00: Q&A time about programming homeworks and theory exercises
9h15-10h: Live exercise solving

8h15: the teaching staff will be available to answer individual / small groups questions about the theory exercises and the programming homeworks

9h15: there will be a “live” session run by the TAs, which may build on the “live” discussion planned on Tuesday.

Thursday 8-10

Selecting your class

Step 1: choose your group of friends of size >=1

Step 2: calculate (SUM(SCIPERs in group)) %3

- **0 → BS160**
- **1 → BS170**
- **2 → CE2**

Please stick to your room so that we have balanced groups

Material released during the week(*)

Release of additional material for the week, including

Slides with speaker notes from the lecture

- Rationale: take your own notes on the PDF “Lecture” (without the speaker notes) available before

Links to lecture videos

- Rationale: this is only a backup to the Tuesday class

Answers to live exercises and theory exercises

- Rationale: obvious

(*) We all know of course that Moodle restrictions are not an actual access control mechanism

Assessment & Grading

- 5 **graded programming homeworks** to do at home
  - Must be done individually!

- **Mid-term on Thursday Nov 7, 2024 8:15**
  - closed notes, location TBA

- **Final exam** during the winter session in Jan/Feb 2025
  - closed notes

- Score: max (60% * final + 30% * midterm + 10% assignments,
  90% * final + 10% assignments)

- You are **never** assessed during the lectures / exercises / forum / student hours

  Participate openly and freely → Ask questions in class and outside (the earlier the better!)

  Asking and answering help exercising your **adversarial thinking**

Programming Homeworks

- Practical exercises to reinforce the learnings of the course
  - Require programming (basic knowledge of Python)
  - Support during exercise sessions on Thursday (+forum and student hours)

- Submission deadline: Fridays at 23:59:59

Homework	Assigned on Monday	To be handed-in on Friday
Understanding access control	23 Sep	11 Oct
Using Encryption algorithms	14 Oct	01 Nov
Password (OPTIONAL, midterm week)	04 Nov	08 Nov
Web attacks	11 Nov	22 Nov
Sniffing traffic	25 Nov	06 Dec
Protecting traffic	09 Dec	20 Dec

Each homework 100 pts

Grade out of 500 pts

Homework -- getting a good start

- The homeworks use Linux as an environment
  - Not Windows/WSL, Not macos
  - Some homeworks require that you have “root” access on the machine.
  - This rules out using EPFL VDI as an infrastructure.

- You have two options to do the homeworks
  - Use your own Linux machine (with root access)
  - Install the COM-301 VM on your own laptop
- On Moodle, you will find:
  - A page with the homework and a link to https://com301.epfl.ch
  - A tutorial to install VirtualBox
  - A special tutorial if you have a macbook M{1,2,3} (ARM rather than x86)
  - A link to the virtual machine disk image

- You may (and should) collaborate to install your environment
- Get your environment ready **before** the first homework is assigned.

Code of Conduct

We expect **high integrity and professional** conduct **inside** of this course

Programming homework assignments and exams **must be solved individually**

Cheating and plagiarism are **not** allowed and **will be severely penalized**

Code of Conduct

We expect **high integrity and professional** conduct **outside** of this course

- We will learn about **attacks**. We expect you to respect:
  - Conventions regarding Computer Misuse and Data Protection
    - **Not acceptable** to mount attacks on live systems
    - **Not acceptable** to collect private data
  - Procedures for research with human subjects
  - **Responsible research** and disclosure procedures (White hat hacking)
  - Compliance and risk-based assessments

Code of Conduct

You can find the code of conduct on Moodle

Code of Academic Conduct and Integrity

v1.0, September 2019

EPFL COM-301, COM-402, COM-523

This code of conduct has two objectives:

- The first objective is to establish an environment of integrity and professionalism that assures that each student is receiving appropriate recognition for their work, and everyone gets a chance to access the learning material.
- The second is to present guidelines on the responsible and ethical behaviour that students should follow regarding the knowledge and skills acquired in the course. Both inside the courses and beyond.

It is the responsibility of every student to be aware of the code's contents, abide by its provisions and also be aware of the current laws and regulations governing IT systems and privacy.

Principles

Projects and Homeworks

COM-301 Moodle

Summary of the information given in this presentation

Complementary material

Previous years' exams - NO SOLUTIONS WILL BE PUBLISHED (talk to others about your solutions!)

Pointers to books

Regular posts on Mondays:

- Slides for this week's lecture (PDF)
- Handouts for graded assignments (when applicable)
- Exercises for Thursday's lab

COM-301 Ed Discussion- help

Ed Discussion is the place to get **HELP** (complementing the Thursdays Q&A sessions)

- Questions on the forum will **not** be considered for the grade, please don't suffer in silence
- Two forums
  - One for questions about the course lectures and materials
  - One for questions about the programming exercises
- Why on Ed?
  - Others can help with your question -- discussing with your peers is a great learning method
  - Others benefit from the discussion -- you are never the only one with a particular doubt

Mail: if you want, you can also ask questions via email (com301@groupes.epfl.ch)

Student hours: we have hours reserved in our calendars to have one-to-one (or small group) meetings. Email the person you want to meet with (including me, though it may be easier to meet with TAs)

Resources

Books (see “Reference Guide” in Moodle for a mapping from the course to the books)

- Dieter Gollmann “Computer Security”
- Ross Anderson “Security Engineering”
- Stallings and Brown: “Computer Security: Principles and Practice”

Read **papers**! Slides will have references. Ask for more!

Read the **news**! Lots of security stories to learn from

Any case you find interesting, we can discuss in the class

Do read the news, do think about the security implications, train your adversarial thinking

Join polygl0ts

http://ctf.epfl.ch

Learn about security

Competitive challenges

Team sport

Develop skills

Understand attacks

Write better code