0. Administrivia

Computer Security Courses @ POLIMI

Prof. Carminati, Maggi, Zanero

Welcome

In this course, we will follow an **holistic approach** to **systems security**.

We will study what happens on **hosts**, **networks**, with an eye to the impact of **policies** and procedures...and the **PEBKAC**!

http://zstag.deviantart.com/art/PEBKAC-162278715

Instructors

Prof. Stefano Zanero - @raistolo

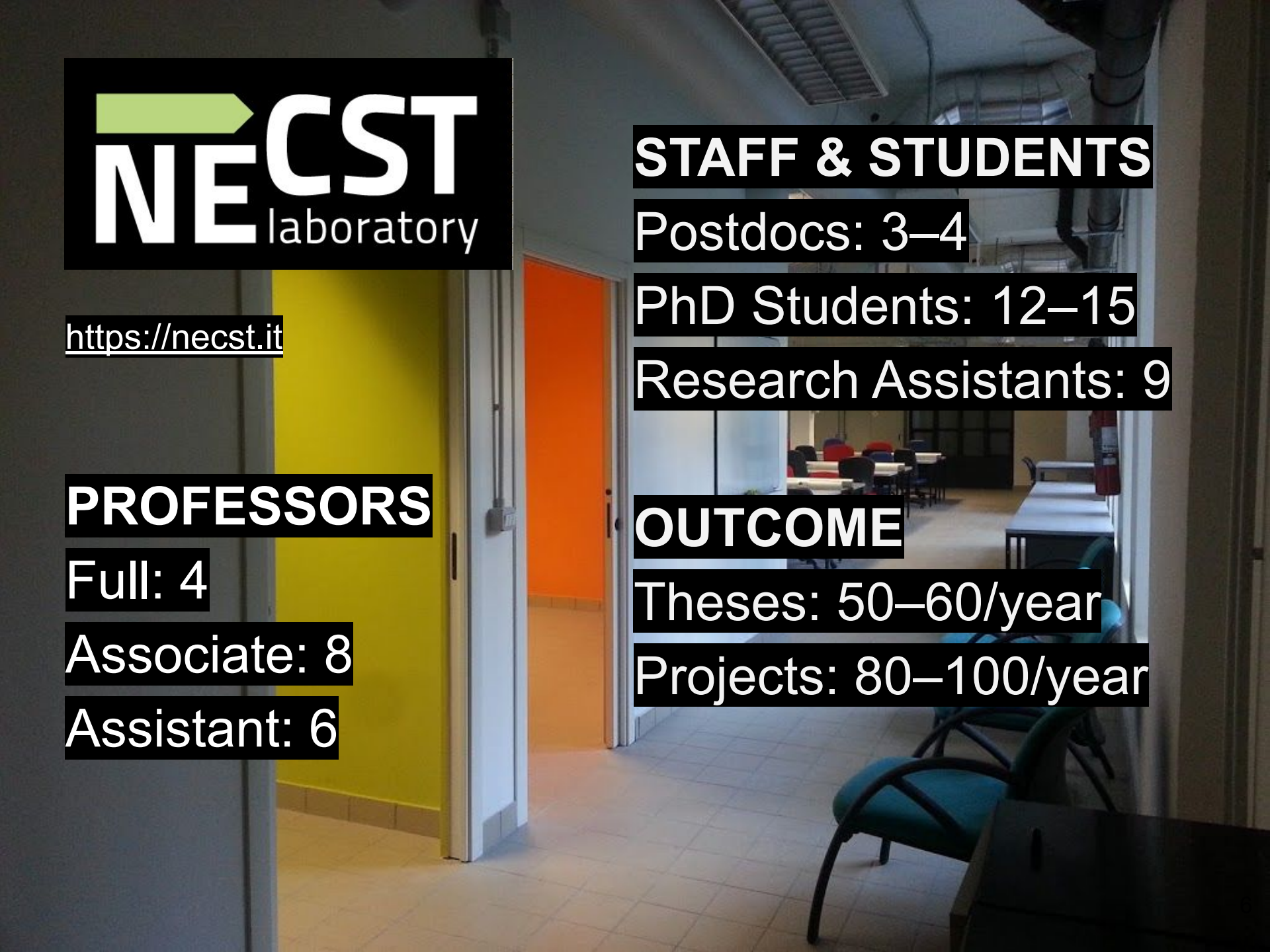
- Email: stefano.zanero@polimi.it
- Phone: 4017
- http://zanero.org

Prof. Michele Carminati

- Email: michele.carminati@polimi.it
- Phone: 3564

What we do as Research Scientists

- Novel attacks on bleeding-edge technology
- Malicious software (malware) analysis
- Computer forensics
- Mobile (mostly Android) security
- Web security
- Bank fraud analysis and detection
- Anomaly-based intrusion detection


NECST laboratory
https://necst.it
PROFESSORS
Full: 4
Associate: 8
Assistant: 6
STAFF & STUDENTS
Postdocs: 3–4
PhD Students: 12–15
Research Assistants: 9
OUTCOME
Theses: 50–60/year
Projects: 80–100/year

Course Topics

Summary

1. The concept of "secure" systems
2. Introduction to basic cryptography
3. Authentication
4. Authorization and access control policies
5. Application and web security
6. Network security
7. Malicious software

Exam Structure

Written test (up to 33 points)

- theory and practical exercises
- since 2013–14 we changed the structure, so previous exams are not representative

Homeworks (up to 2–3 points)

- HW1 (1 week)
  - web vulnerabilities (client + server)
  - web vulnerabilities (server)
- HW2 (1 week)
  - memory errors (buffer overflow vulnerabilities)
  - memory errors (format string vulnerabilities)

Prerequisites

Since some of you asked, here it is:

- we will use a little of C, bash, Python
- at some point, we will need a bit of IA32 assembly, but we have a prep class for this
- networking essentials (beyond "www.")
- willing to learn or able to use a Linux term.

Generally, you should be flexible to learn new things every day

- if you don't know, **just ask**!

Materials

Option 1: Slides + Attend class + [Optional material]

Option 2: Slides + Book + [Optional material]

~~**Option 3: Slides**~~ (best way to fail the exam)

Textbooks

- *D. Gollman*, "Computer Security", Wiley (3rd ed.)
- *R. Anderson*, "Security Engineering", Wiley (2nd ed.) FREE
- William Stallings, Lawrie Brown, Computer Security Principles and Practice

Slides (and announcements)

- https://beep.metid.polimi.it/web/3020302

[Optional Material]

Books

- *C. Anley, J. Heasman, F. Linder, G. Richarte*, "The Shellcoder's Handbook", Wiley, 2007
- *Howard, LeBlanc*, "Writing Secure Code", Microsoft

Papers

- The slides include links to in-depth material on select subjects (useful for theses).

Unofficial communication (and geekness)


Computer Security @ POLIMI

Hacking Group and CTFs

- about 14 years ago, we started playing CTFs
- now we have a local hacking group

- Tower of Hanoi (aka "Hanoiati")

  http://toh.necst.it

  https://twitter.com/towerofhanoi
- we meet weekly at the NECSTLab
- we have a Slack channel and a mailing list
- just ask me if you're curious!

Conclusions and Assignment

You just met your Professor :-)

The homework and exam structure changed since '13-14

Having a textbook is not mandatory, but is a good substitute for coming to class.

"Slides only" is a no-no.

TODO: Join the BeeP course and our Facebook group.