0. Administrivia

055633 - COMPUTER SECURITY

Proff. Barenghi, Carminati, 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

Alessandro Barenghi

- Email: alessandro.barenghi@polimi.it
- Office: 1st floor, building 20, DEIB
  - Office hours: just e-mail me and we'll find a timeslot
- Phone: 9039

Mario Polino

- Email: mario.polino@polimi.it
- Office: 1st floor, building 20, DEIB

Instructors

Michele Carminati

- Email: michele.carminati@polimi.it
- Office: 1st floor, building 20 or NECSTlab, DEIB
- Office hours: just e-mail me and we'll find a timeslot
- Phone: 4041

Tutors/Assistants

- **Lorenzo Binosi**
  - Email: lorenzo.binosi@polimi.it
- **Stefano Longari**
  - Email: stefano.longari@polimi.it

Instructors

Stefano Zanero

- Email: stefano.zanero@polimi.it
- Office hours: just e-mail me and we'll find a timeslot
- Phone: 4017
- http://zanero.org

Tutors/Assistants

- **Armando Bellante**
  - Email: armando.bellante@polimi.it
- **Mario D'Onghia**
  - Email: mario.donghia@polimi.it

What we do as Research Scientists

- Anomaly-based intrusion detection
- Cyber-physical security (automotive, robotics, medical)
- Fraud analysis and detection
- Hardware security and Secure HW design
- Malicious software (malware) analysis
- Novel attacks on bleeding-edge technology
- Side channel attacks and countermeasures
- Post quantum cryptography

Course Topics

Summary

1. Framing what a secure system is
2. Fundamentals of cryptography
3. Techniques for user authentication
4. Authorization and access control policies
5. Application and web security
6. Network security
7. Malware

Exam Structure

Written test (up to 31 points)

- Theory and practical exercises
- Since 2021–2022 we changed the structure, so previous exams are not representative
- Closed books & No remote exam

Homeworks (up to 2–3 points)

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

Prerequisites

- C Programming and its execution model
  - Essentially “Fondamenti di informatica” / CS101
- A little of bash and Python
- IA32 (aka i386) assembly
  - There’s a prep class to bring you up to speed
- Network protocol fundamentals
- Be able to work in a GNU/Linux environment with a CLI
- If you are missing something, **just ask**!

Materials

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

Option 2: Slides + Books + [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
- Mike Rosulek "The joy of cryptography" FREE

Slides (and announcements) on WeBeep

[Optional Material]

Books

- *C. Anley, J. Heasman, F. Linder, G. Richarte*, "The Shellcoder's Handbook", Wiley, 2007
- *Howard, LeBlanc*, "Writing Secure Code", Microsoft
- Advanced Linux Programming - Chapter 10

Papers

- The slides include links to in-depth material on select subjects

Hacking Group and CTFs

- about 20 years ago, we started playing CTFs
- now we have a local hacking group

- Tower of Hanoi (aka "Hanoiati")

  https://toh.necst.it

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

Conclusion

You just met your Professor :-)

Having a textbook is not mandatory, but is a good substitute for coming to class (or watching recordings).

"Slides only" is a no-no.