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

Tutors/Assistants

Lorenzo Binosi

- Email: lorenzo.binosi@polimi.it

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

- **Alessandro Bertani**
  - Email: alessandro.bertani@polimi.it
- **Gabriele digregorio**
  - Email: gabriele.digregorio@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

- **Lorenzo Binosi**
  - Email: lorenzo.binosi@polimi.it
- **Daniele Mammone**
  - Email: daniele.mammone@polimi.it

What we do as Research Scientists

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

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 33 points)

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

(Bonus) Homeworks Challenges (up to 3 points)

- **Duration:** Last for two weeks (usually in May)
  - HW1 (1 week)
    - memory errors (buffer overflow vulnerabilities)
    - memory errors (format string vulnerabilities)
  - HW2 (1 week)
    - web vulnerabilities (client + server)
    - web vulnerabilities (server)

Quick advices on the Challenges

- **Score computation** New!
  - Based on the number of solves per challenge

- The challenges are **not mandatory**
  - **Bonus** points + The written exam alone reaches 33 points

- **Challenges prerequisites:**
  - They may contain advanced concepts that require
    - Individual effort and study

- **We won't allow any cheating attempts**
  - If we are able to single out cheaters:
    - We will void their grades
  - otherwise
    - We will void the challenges to anyone...ask your colleagues what happened last year...

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

  https://toh.necst.it

  https://twitter.com/towerofhanoi

- we hack at the NECSTLab
- we have a Discord channel
- just ask if you're curious!

What is this CTF thing, anyway?

Information security-oriented “game”

Try to break into (toy) applications “for fun”

… get flags: **`flag{this_is_a_flag}`**

Which skills?

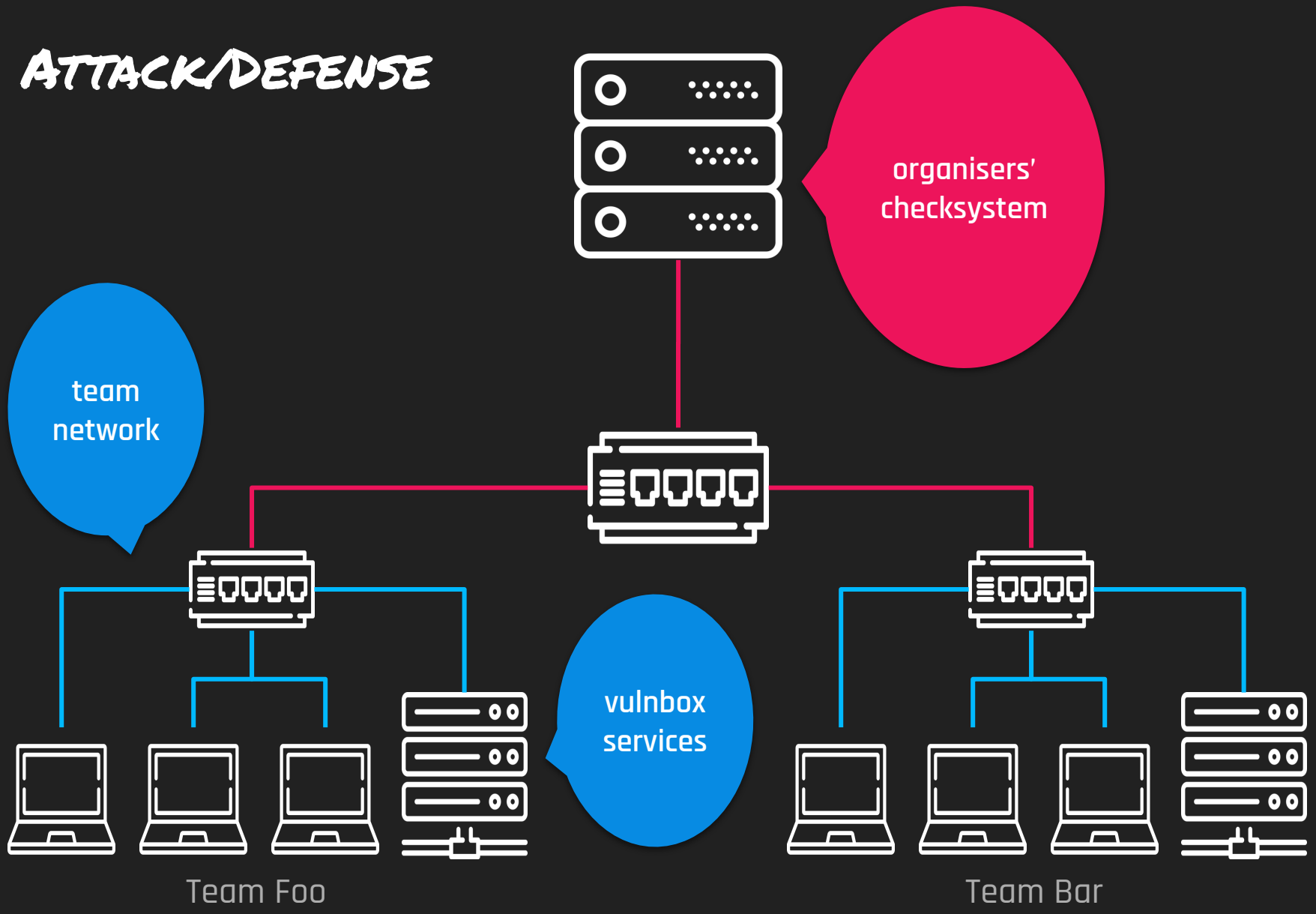
cryptography
reverse engineering
binary exploitation
web application security
stego / forensics
mobile security
... and others

Good teams generally have strong skills and experience in all these areas

Jeopardy

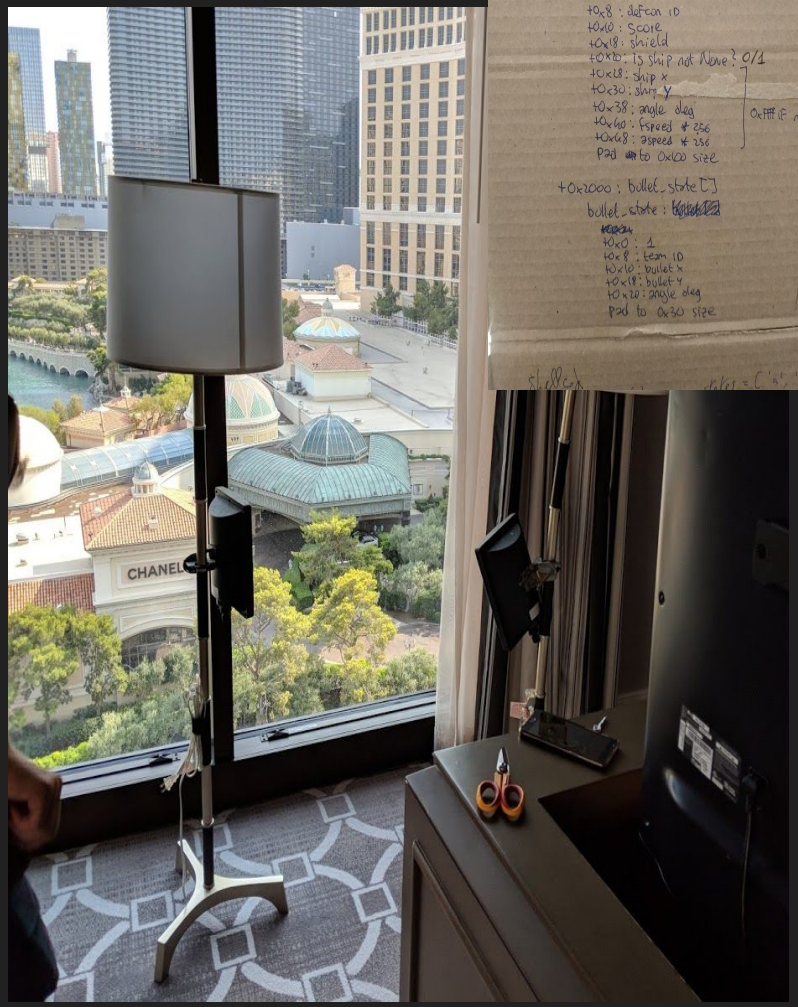

Teams
Scoreboard
Challenges
CAPTURE the FLAG
Beginners Quest
README
Logout [mHACHeroni]
CRYPTO
BETTER ZIP 231pt 38 solves
DM COLLISION 176pt 63 solves
DOGESTORE 267pt 27 solves
MITM 243pt 34 solves
PERFECT SECRECY 158pt 74 solves
MISC
BOOKSHELF 363pt 10 solves
FEEL IT 208pt 47 solves
PHRACK 420pt 5 solves
TAPE 355pt 11 solves
WIRED CSV 220pt 42 solves
PWN
DRIVE 500pt 0 solves
EXECVE SANDBOX 283pt 23 solves
APT42 - PART 2 420pt 5 solves
SANDBOX COMPAT 420pt 5 solves
SFTP 181pt 60 solves
RE
SHALL WE PLAY A GAME? 113pt 111 solves
BACK TO THE BASICS 293pt
WEB
BBS 453pt 3 solves
CAT CHAT 210pt

Attack/Defense



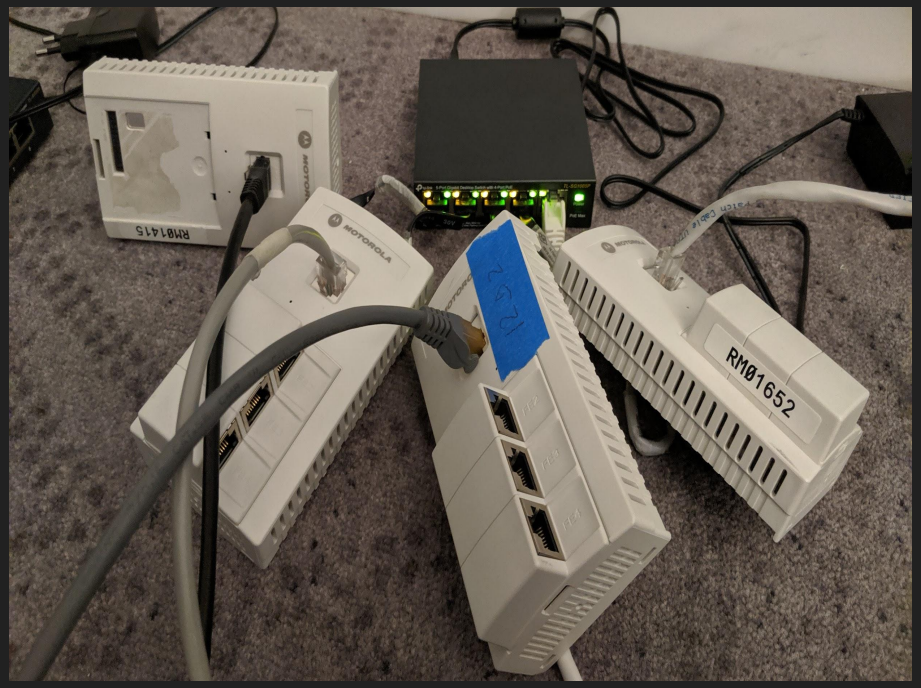
Slide credit: Marco Squarcina, TU Wien

Internet connection!



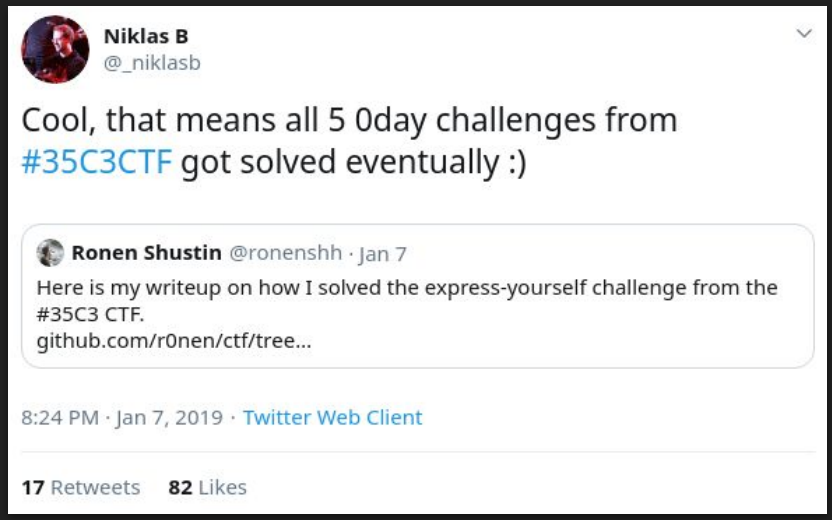
Internet connection!

- Hotel LAN
- LTE Sim Cards
- Radio Bridge to another hotel
  - ...er, which one?
  - Bellagio was in sight



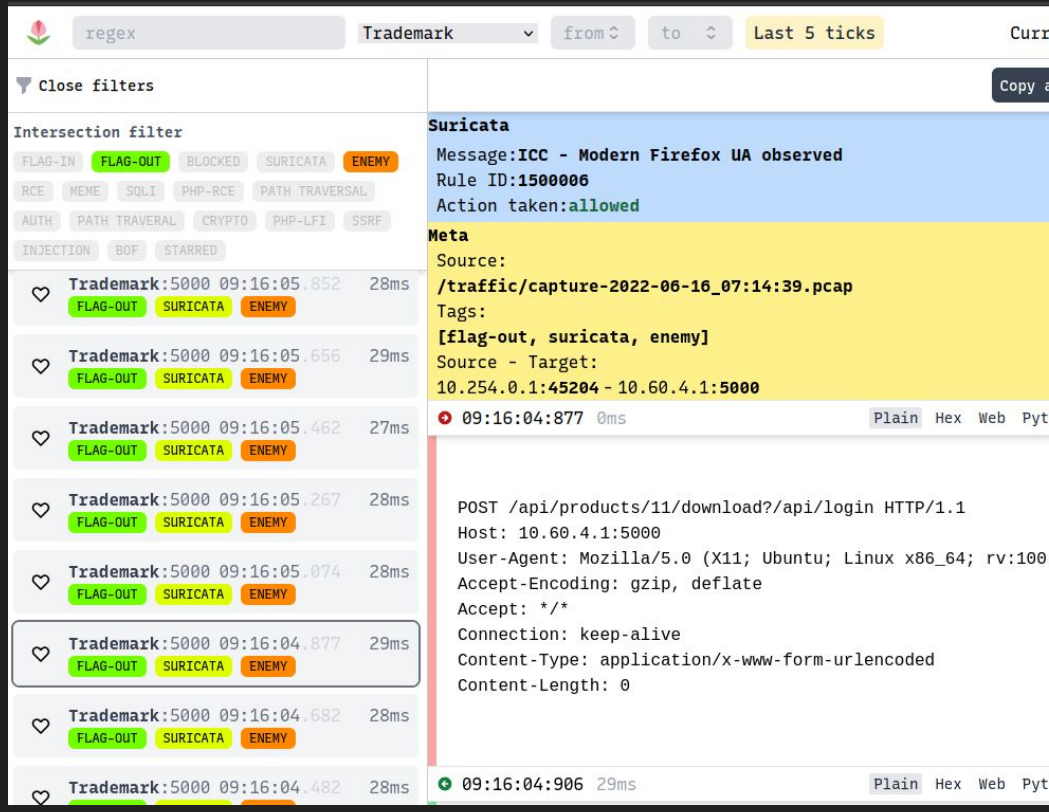
It is not a GAME

- CTFs are played by Professionals
  - Used as recruitment tool
- Very little fair play
  - Physical attacks
  - Attacking the infrastructure
- 0-days:
  - Kernel exploits: https://t.co/6OnnGK363y
  - XSS Auditor Fail
  - ExpressionEngine
- It is NOT Real Application
- Good Challenges
  - Let you explore Ideas
  - Guide you through something new

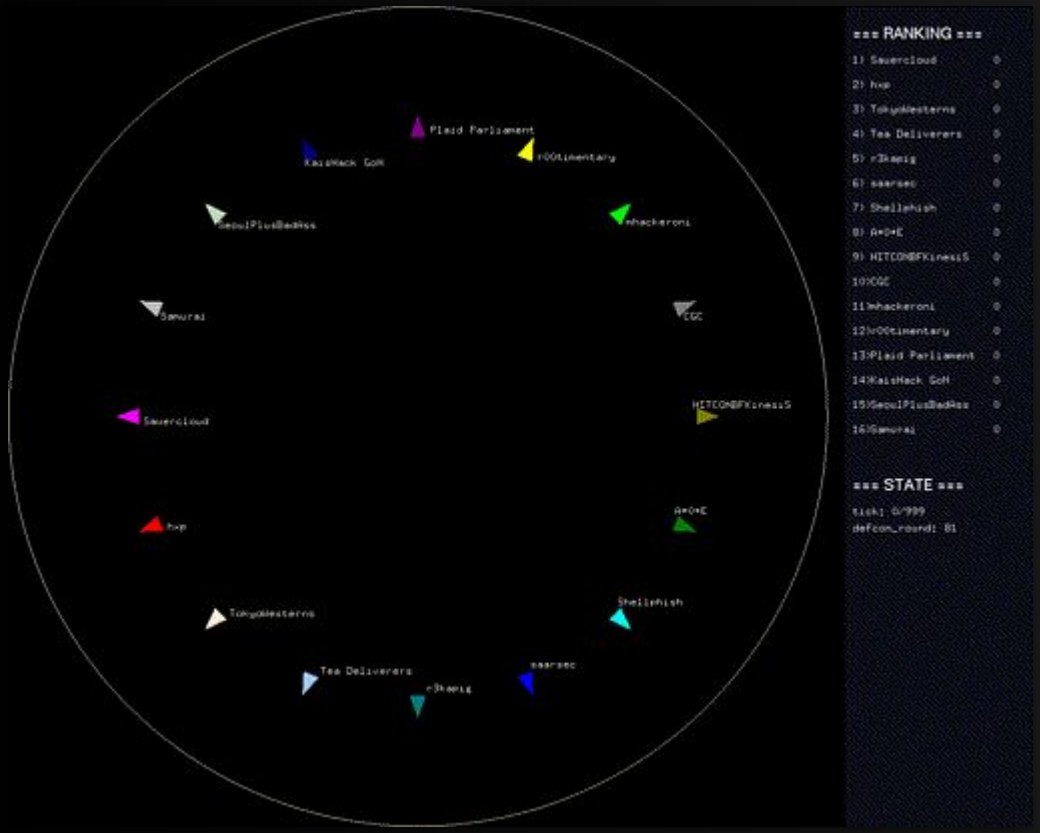


Tools: TULIP and The META GAME

- Traffic Analyzer
- Reply Capabilities
- Developed By Team Europe
- github.com/OpenAttackDefenseTools/tulip
- Attacks on Tulip at ECSC 2022



Other Games: King Of The Hill



Best Exploits WIN!

- Ranking, bytes limit

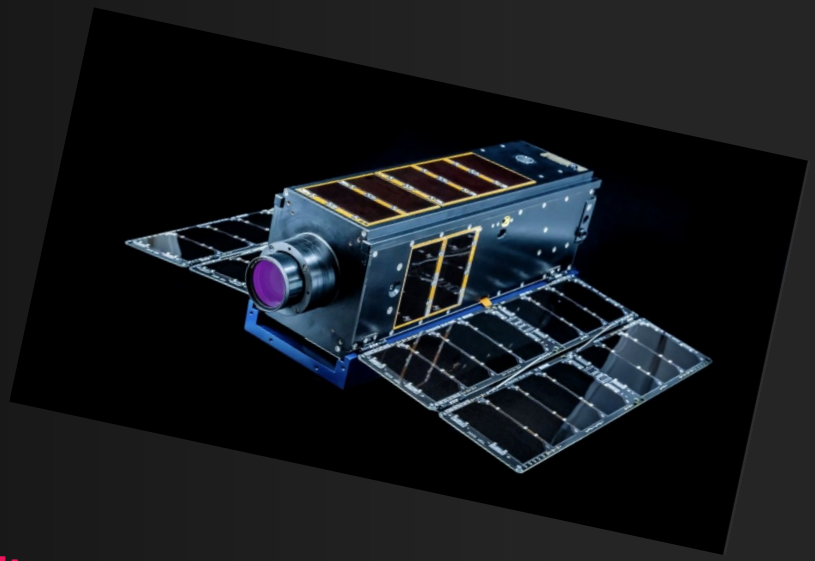
ROPShip

- In a nuthsell... **Visual A/D!**
- Automatically generate **ROP chains** from random data to determine the next action of the spaceship

  `up, down, right, left, shield, attack, nop`
- Many different strategies

Building an E-Sports ?

Hack-A-Sat



- **Space Themed CTF**
  - Orbiting Challenge
  - Landing
  - Communication
  - Apollo Code Reversing and Attack
  - etc.
- **2023 There was a Final on an orbiting Satellite**

mHackeroni Won!

mHackeroni Won!

mHackeroni Won!

https://twitter.com/i/status/1690882077078732801

How About Machines?

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.

If you find yourself interested in security by the end of this course, a natural continuation would be to explore...

056896 - OFFENSIVE AND DEFENSIVE CYBERSECURITY