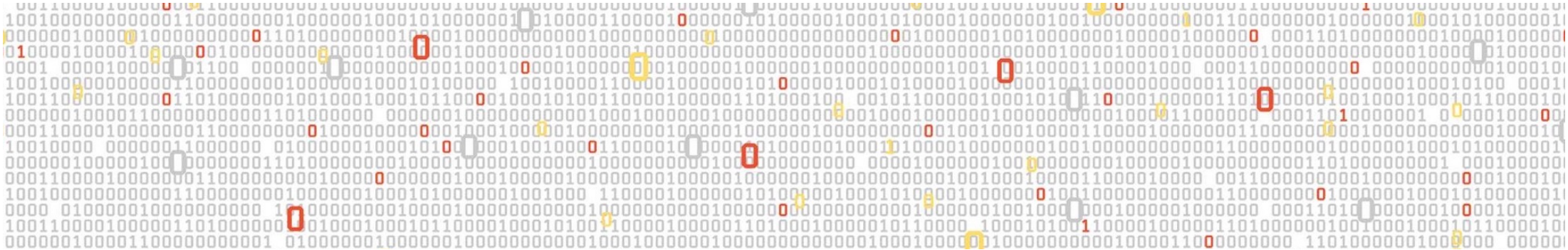
Foundations of Cybersecurity

Luca Caviglione
Institute for Applied Mathematics and Information Technologies
National Research Council of Italy
luca.caviglione@cnr.it



University of Pavia – Department of Electrical, Computer and Biomedical Engineering

About

- I am:
  - a Research Scientist at the **National Research Council of Italy**
  - started as a networking guy, now in cybersecurity
  - held courses for Ph.D. and M.Sc. students on security and computer networks
  - my main research areas are **information hiding** and **software security**.
- Contacts:
  - I work and live in Genova
  - mail: **luca.caviglione@ge.imati.cnr.it** or luca.caviglione@unipv.it
  - M$Teams: luca.caviglione@cnr.it
  - office near you: CNR – IMATI, Pavia, Via Adolfo Ferrata 5/a.

Goals

- The **course** has the following **goals**:
  - provide a comprehensive introduction to **basic cybersecurity** concepts
  - outline the most common **attack surfaces**
  - give a background for **autonomously** gathering information
  - show some **toy examples**
  - **have fun!**
- This course is **not** about:
  - hacking (read *Phrack Magazine, https://phrack.org*)
  - hardware security and cryptography
  - things likely to fall outside your early career as an engineer.

Grading

- There are **two paths** to the **final exam**.
- The **First Path (strongly suggested)** is organized in two steps.
- **Oral** presentation:
  - a small seminar of 15-20 minutes related to a topic that you found interesting
  - groups of students (it depends on the number of attendees)
  - prepare supporting material and slides you believe are useful
  - score: up to **24/30**.
- **Written** test:
  - **three** open questions on (very) core concepts
  - score: **3 per question**.
- **Final grade**:
  - if total score > 31, then "30 with honors"
  - else the plain sum.

Grading

- The **Second Path** is organized in a single step.
- **Written** test:
  - **eleven** open questions on (very) core concepts
  - score: **3 per question**.
- **Final grade**:
  - if total score > 31, then “30 with honors”
  - else the plain sum.

Other Information

- Checkpoint:
  - I propose a **mid-term checkpoint**
  - simulation of the written final test
  - the outcome **does not contribute in any manner** to the final exam.
- I am a very open-minded, but **please do not**:
  - copy
  - steal work
  - copy/paste concepts and data without proper attribution
- A note about AI:
  - ChatGPT & Co. are welcome if used to **support** routinary tasks
  - not allowed if they **prevent** you from **learning**!

Course Outline

- The course is organized in:
  - **7** modules covering major aspects of cybersecurity
  - **1** final wrap-up module
  - **1** seminar with a small set of demos.

1. Introduction and Basics:
  - motivations on the importance of cybersecurity
  - the Cyber Kill Chain
  - attack surface and attack surface reduction
  - hints at the human element.

2. Security Analysis and Modeling:
  - common weaknesses enumeration
  - common vulnerability enumeration
  - common vulnerability scoring system
  - testing strategies.

Course Outline

3. Software Supply Chain Security:

- main attack entry points
- dependency attacks
- (typo | slop | combo) squatting
- starjacking and dependency confusion
- build system attacks and reproducible builds.

4. Malware:

- major threats and architectures
- malware analysis, packers and anti-forensics
- YARA rules
- binary and source code obfuscation and minification.

5. Network Security:

- possible network attack types
- sniffing, spoofing and DoS/DDoS
- firewalls, policy enforcing and hardening
- network address translation, honeypots, and segmentation.

Course Outline

6. Information Hiding (Optional):

- information hiding and steganography
- network covert channels
- local covert channels and colluding applications
- sanitization (including side-channel attacks).

7. Watermarking and Artificial Intelligence (Optional):

- watermarking of data, software and AI models
- backdoors
- triggers.

8. Conclusions:

- discussion of presentations (tentative placement)
- final recommendations and lessons learned.

Course Material

- There is **no** a **unique** book that can be read cover to cover.
- Suggested sources:
  - slides
  - examples and open repositories
  - official or selected websites
  - introductive research papers.
- The needed **material** will be published in the GitHub of the course:
  - https://github.com/lucacav/foc
  - clone the repository and stay synced (*gh repo clone lucacav/foc*).
- Disclaimer:
  - this is the **first edition** of “Foundations of Cybersecurity”
  - we can adjust the outline together.