Lezione 1

Monday, March 1, 2021 1:03 PM

Foundations of Cybersecurity

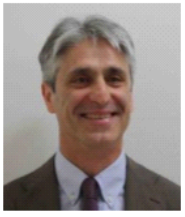
Gianluca Dini
Dept. of Ingegneria dell'Informazione
University of Pisa
gianluca.dini@unipi.it
Version: 2021-02-27

1

Lecturers

UNIVERSITÀ DI PISA

- Lecturer
  - Prof. Gianluca Dini
    - Dept. of Ingegneria dell'Informazione
    - Email: gianluca.dini@unipi.it
    - Office hours by appointment
- Teaching assistant
  - Ing. Michele La Manna
    - Dept. of Ingegneria dell'Informazione
    - Email: michele.lamanna@unifi.it



2

Prerequisites

- Computer architectures
- Operating systems
- Computer networks
- Algorithms and data structures
- Complexity and probability theory
- Modular arithmetic

3

Contents

- Applied cryptography
  - Learn how crypto-primitives work
  - Learn what "secure" means
  - Learn how to use them correctly and reason on security
  - Relationship between cryptography and data security
- Programming secure applications
  - Buffer overflow and secure coding in C/C++
  - Web security
- Handson and challenges
- Case studies
  - How to build insecure systems with secure components

4

Organization

- Foundations of Cybersecurity is a course of the Master in Computer Engineering (CE)
  - 9 CFU, 90 hours
- FoC is shared with the Master in Artificial Intelligence and Data Engineering (AIDE)
- FoC is partially mutuated by Applied Cryptography of the Master in Cybersecurity (CySec)
  - 9 CFU, 72 hours (Δ = -18)

5

Organization

- Survey on attendance segmentation

6

Organization

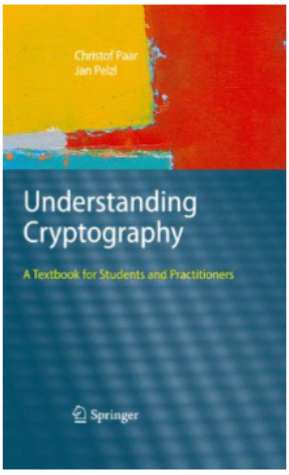
UNIVERSITÀ DI PISA

Time table	Class	Topics	Total #hours
Mon 13:30 – 16:30	ALL	• Applied crypto • Open SSL programming	72
Wed 10:30 – 13:30	ALL		
Thu 10:30 – 12:30	CE/AIDE	• C/C++ secure programming • Web security • Challenges	18

7

Textbooks

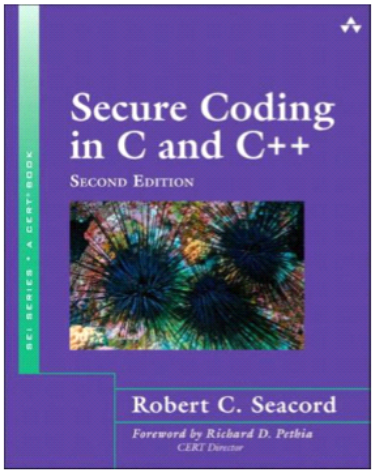
– C.Paar, J.Pelzl. Understanding Cryptography – Testbook for Students and Pratictioners. Springer



8

Textbooks

- Robert C. Seacord. Secure Coding in C and C++ - second edition. Addison-Wesley



9

Textbooks

UNIVERSITÀ DI PISA

- Handouts
- Reader
  - Papers
  - Standards
  - …
- Microsoft Team 880II 20/21 – Foundations of Cybersecurity
  - Generale/File

10

Final Exam

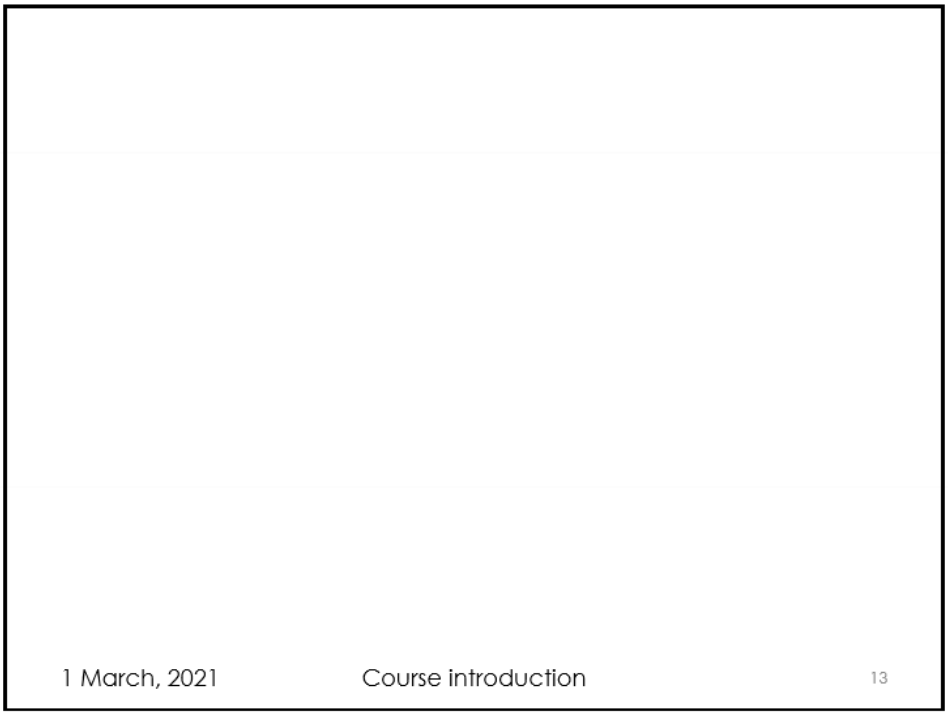
- Project
  - 1-2 people per group
  - *Conditio sine qua non*
- Written-part
  - Closed-book, closed-notes
- Oral-part

11

Communications

- Microsoft Team 880II 20/21 – Foundations of Cybersecurity
  - Generale/Post
- Microsoft Teams chat
- Email (filter safe)
  - Subject: [FoC] <the subject>

12



13