CYBERSECURITY
FROM DESIGN TO OPERATIONS
Why

✔ A thriving job market
  • predicted growth:
    172 billion USD (2023) -> 424 billion USD (2030)
  • 300,000 skilled workers needed in Europe
  • 3.4 million unfilled position globally

✔ An appealing career
  • ranked 5th in the U.S. News and World Report’s list of the 100 best jobs (up from 8th in 2022)
  • continuous, stimulating challenges
  • huge variety of employment opportunities, both in terms of roles and of application fields
Who

Academic faculty
• Bologna University
• King's College London

Committed industrial partners
• financial support
• experienced trainers
• engaging internship positions
MASTER’S PROGRAM IN CYBER SECURITY
FROM DESIGN TO OPERATIONS

When

- lectures
  - 12 hours each weekend
  - Friday afternoon
  - Saturday all day

- internship
  - to be decided with host

- project work
  - self-organized

November – December, lectures only

Winter Break
January – April, lectures + internship

Spring Break
May – June, lectures + internship

July, internship only

Summer Break
September, report and presentation writing
Early October, final exam
MASTER’S PROGRAM IN
CYBER SECURITY
FROM DESIGN TO OPERATIONS

Where

✔ IN PRESENCE BY DEFAULT
School of Engineering
Viale del Risorgimento 2
40136 Bologna

✔ OPTIONALLY ONLINE
ONLY FOR STUDENTS RESIDING MORE THAN 1 HOUR AWAY
How

11 BASE MODULES (LECTURES+LABS)
- Every topic will be illustrated in theory and demonstrated in practice

2 HOT TOPIC WORKSHOPS
- Application security testing
- Cloud security

BYOD
- Students need to bring their own laptop, suitable for the execution of virtual machines provided by instructors

KEEPING TABS ON PROGRESS
- Attendance of at least 80% of lecture hours is mandatory
- At the end of each module, an exam will measure its effectiveness
- Skipping or failing a few intermediate exams is not critical, but
- Admission to the final exam is judged on the overall positive performance
Fundamentals of Security and Cryptography

- Prof. Rebecca Montanari (UniBO)
  Prof. Marco Prandinii (UniBO)
- 24 hours

Outcomes:

- Knowledge of the main different aspects of security as a process, and of the technical language used to describe threats, vulnerabilities, and countermeasures.
- Security requirements: confidentiality, integrity, authenticity, and how to achieve them in presence of different adversaries.
- Analysis of the main cryptographic building blocks to design security countermeasures. Tips on correct implementation of cryptographic mechanisms.
Network security and administration

- Prof. Franco Callegati (UniBO)
- Prof. Walter Cerroni (UniBO)
- 40 hours

Outcomes:
- Basic ability to program network devices to implement segmented layer-2 and layer-3 internetworks.
- Knowledge of security issues in telecommunication and of protocols (e.g. IPSec, TLS) for their mitigation.
Computer security and administration

- Linux
  Prof. Gabriele D’Angelo (UniBO)
  Prof. Angelo Di Iorio (UniBO)
  Prof. Marco Prandini (UniBO)
- Windows/AD
  Dr. Mattia Masella (Cyberloop)
  Dr. Davide Ciandrini(Cyberloop)
- 40 hours

Outcomes:

- Knowledge of the basic steps of system configuration, from boot to service management. Basic ability to manage software installation, update and configuration in a production environment.
- Knowledge of the different categories of vulnerabilities in a system and of the corresponding attack vectors. Basic ability to use tools for proactive security assessment and centralized monitoring.
Security engineering I - secure coding

- Avv. Andrea Baldrati (Privacy Network)
- Dr. Matteo Navacci (Privacy Network)
- Dr. Matteo Meucci (IMQ Minded Security)

- 16 hours

Outcomes:
- Security-by-design and Privacy-by-design, and practical applications of the GDPR in secure systems development
- Knowledge of design patterns and best practices for the whole process of secure software development.
Seminar - Cloud Security

- Prof. Marco Prandini (UniBO)
- 8 hours

Contents:
- Threats, vulnerabilities and attacks specific of the cloud computing environment
- Cloud-oriented application development methodologies (image preparation, deployment, management)
Workshop - Static Application Security Testing

- Dr. Andrea Pagani (Crif)
- 8 hours (5 theory + 3 practical teamwork)

Contents:

- CyberSec Fields and TradeOffs
- What is Source Code Analysis? SAST, OSS & Dependency, DAST & IAST Considerations
- Top Application Security Risks; OWASP Top 10 2021 Detection
- Lab 1 – Demo of a SAST tool: Running Fortify scans
- Remediation: High level fixing strategies
- Industrialization of SCA: Distributing SAST on large scale
- Lab 2 – Corporate SAST: Scenarios for building SAST architectures
Security engineering II - web app security and testing

- Dr. Giuseppe Porcu (IMQ Minded Security)
- Ph.D. Andrea Melis (UniBO)
- 24 hours

Outcomes:
- Knowledge of the OWASP methodology for web applications.
- Tools to verify web app security according to the OWASP methodology.
- Specific challenges of web application security testing
- Intelligence gathering and threat modeling
- Vulnerability analysis
- Client side attacks, Server side attacks
- Tools and techniques
Security engineering III - mobile security and testing

- Dr. Luca Capacci (Cryptonet Labs)
  Dr. Alfonso Solimeo (Cryptonet Labs)
- 24 hours

Outcomes:
- Knowledge of the design patterns and security testing methodology for mobile applications.
- Tools to verify mobile app security according to the presented methodology.
- Specific challenges of mobile application security testing
- Intelligence gathering and threat modeling
- Vulnerability analysis
- Testing authentication, cryptography, code quality.
- Android, iOS and hybrid applications anatomy
- Tools and techniques
Security engineering IV - Industrial Control Systems

- Ph. D. Andrea Melis (UniBO)
- Dr. Edoardo Montrasi (Cryptonet Labs)
- 16 hours

Outcomes:
- Understanding of the structure of an ICS and of challenges posed by its peculiar differences with respect to IT systems.
- Knowledge of security issues and possible countermeasures.
- Specific challenges of industrial control systems.
- Intelligence gathering and threat modeling.
- Vulnerability analysis.
- Embedded systems and fieldbus protocols anatomy.
- Tools and techniques.
Security monitoring I - Malware analysis and detection
- Ph.D. Fabio Pierazzi (King's College London)
  Dr. Luigi Martire (Yoroi)
- 32 hours

Outcomes:
- Knowledge of the CERT operations to detect threat trends and ongoing attacks.
- Tools for static and dynamic analysis of code to identify malware.
Security monitoring II - Information correlation

- Dr. Federico Foschini + staff (Certego)
- Dr. Tommaso di Donato (Crif)
- Dr. Massimiliano Pinto (Crif)
- 24 hours

Outcomes:
- Knowledge of network-based intrusion detection systems and other kinds of probe-based systems to collect and correlate traces of malicious activity in progress.
- Critical (industrial, infrastructural, etc) system architectures and methods for their protection from attacks.
What 10/11

Incident response
- Dr. Luca Losio (4n6)
- 16 hours

Outcomes:
- Knowledge of the methods to identify ongoing incidents and restore normal operations after a security breach.
- Ability to draw an incident response plan and policy
Digital Forensics

- Prof. Alessandro Amoroso (UniBO)
- Dr. Luca Losio (4n6)
- 32 hours

Outcomes:

- Knowledge of the issues and challenges of forensics, from a technical and legal viewpoints, such as chain of custody.
- Ability to use the main forensics tools to analyze data and to write the final report.
MASTER'S PROGRAM IN
CYBER SECURITY
FROM DESIGN TO OPERATIONS

APPROXIMATE DATES - TBC

Key steps

✔ Apply by 30 September 2022
  • Look for the call (opening soon) on https://www.unibo.it/en/teaching/professional-master/2022-2023

✔ Pass selections on 10 October 2022
  • Basic operating systems, network and programming skills are needed
    • Verified during interview if you acquired them on the field
    • Automatically satisfied by holding an IT-related degree (but interview is mandatory nonetheless: strong motivation is essential!)

✔ Enrollment: 19 October - 3 November 2022
  • Law requirement: holding a bachelor degree by the time of enrollment

APPROXIMATE DATES - TBC
How much

- €4,900 to be paid in two installments of equal amount
  - at the enrolment
  - spring 2024

- Companies can directly pay for their employees upon communication of their intent
MASTER’S PROGRAM IN
CYBER SECURITY
FROM DESIGN TO OPERATIONS

Director: Prof. Marco Prandini
Dept. of Computer Science and Engineering

master.cybersecurity@unibo.it

https://master.unibo.it/cybersecurity/