Cybersecurity foundations and research challenges

A short introduction for Ph.D students in Computer Science and Engineering @Unibo

About the course

Instructor

Marco Prandini
Dipartimento di Informatica – Scienza e Ingegneria (DISI)
Email: marco.prandini@unibo.it
Web: https://www.unibo.it/sitoweb/marco.prandini/

Schedule

- June 22, 2020 – 14:00-16:30
- June 29, 2020 – 14:00-16:30
- July 6, 2020 – 14:00-16:30
- July 13, 2020 – 14:00-16:30

Location

Online – Register to the Team using this link
https://teams.microsoft.com/l/team/19%3af723ac5766094819b4e52b4d2ff423a6%40thread.tacv2/conversations?groupId=2351548f-55a9-4417-9b01-2ee98d33fb14&tenantId=e99647dc-1b08-454a-bf8c-699181b389ab

Teaching material

The instructor will provide slides, and a list of bibliographical references and additional material. All the course material is in English.

Learning and assessment modalities

The course will be taught in either Italian or English at the preference of the attendees.

The final assessment consists of a technical report on a foundational or recent paper on one of the course topics.

Syllabus

Foundations

- Information security properties
- Cryptography 101: symmetric and asymmetric crypto, hash functions, steganography
- Access control models: DAC, MAC
- Secure network channels: TLS, OpenVPN, SOCKS, TOR, IPSec

Cybersecurity: an overview

- *The kill chain (hints)*
- Vulnerabilities
  - Network: LAN and routing issues, covert channels
  - System: hardware faults, configuration issues
  - Applications: coding errors, privilege management errors
  - Users: social engineering, awareness
- *The Cybersecurity Framework (hints)*

Hardening your research platform

- Mitigation of system vulnerabilities:
  - Network filters
  - Vulnerability assessments
- Mitigation of software weaknesses:
  - Secure coding guidelines
- Data protection:
  - Anonymization techniques
  - Applied cryptography
- *Monitoring and intrusion detection tools (hints)*

Current challenges and research directions

- Crypto challenges
  - Post quantum crypto
  - Computing on encrypted data
- Critical infrastructures
  - IoT security
  - SDN and security
  - Cyber-physical and industrial systems security
- Privacy and other social implications