Mauro Conti, PhD

University of Padua - MSc in Cybersecurity

Advanced Topics in Computer and Network Security

Academic Year: 2023/2024

Lecturer: *Mauro Conti*

Teaching Assistant: *Francesco Marchiori* and *Alessandro Lotto*

**Note: In this page you will find updated information about the course.
(students are invited to visit often this page).**

Language: The course and the exam will be held in English.

Credits: 6 CFU.

Schedule: I semester (course schedule is published **HERE**).

Mailing List: Students enrolled for this course are invited to join **THIS** Moodle.

Course Content:

The course is organized in three parts:

- Introduction to Advanced Topics in CyberSecurity.
- Student Presentations.
- Final Project.

In the **first part** of the course, we introduce advanced research topics in CyberSecurity, possibly also through invited speakers, including:

- IoT and Cyber-Physical System (Industrial security and Vehicular security).
- Machine Learning for security (authentication systems, privacy-preserving, threat identification).
- Adversarial Machine Learning (i.e., the security of machine learning applications).
- Blockchain theory and application.
- Encryption.
- Social Network Security

The **second part** consists in presentations held by the students, based on a selection of a Cybersecurity topic (that either has had a strong impact on security today or explore novel ideas that may be important in the future). The list of topics can be found HERE. For each topic, students are requested to read the suggested primary paper. The speakers for that topic (about 3 students) have a finite time (20 minutes) to **present the assigned topic** (primary and at least one of the secondary papers). The presentation will be followed by about 10 minutes of interactive discussion in the class.

Each student will also need to choose **3** of those lectures (in different topics) in which they will participate in the interactive discussion by asking some **thought-provoking questions** on the primary paper **in class** and also **upload them on a form** (at least 24 hours ahead of the topic presentations). These questions should critically evaluate the papers (e.g., questioning the assumptions, criticize the methodology, compare with other solutions, propose alternative solutions).

The **third and final part** consists of a project session. Each group previously composed during the second part must write a about 10-page long essay about the topic presented in class. The direction and the structure of the essay must be agreed with the lecturer. The essay might include some implementation prototype or experiments/simulations to evaluate/support the claim in the paper. If the student cannot attend the lectures, an alternative work (e.g. a longer essay) must be agreed with the lecturer. The final essay will be presented during an oral exam, where the students are asked to give a 15-minute presentation to the lecturer and the teaching assistants about the essay (presenting with slides is highly recommended).

Grading Criteria:

Students will be graded according to:

- (25%) the presentation during the second part of the course
  - (15%) Layout and Graphics
  - (30%) Content
  - (20%) Organization
  - (20%) Presentation
  - (15%) Q&A.
- (25%) the participation in the discussions during the second part of the course
- (25%) the content and quality of the essay
  - (30%) Style
  - (20%) Originality
  - (50%) Organization (clarity in your argumentation, coherence between assumptions and conclusions, logical organization, evidence to support claims)
- (25%) the oral presentation of the essay, during which the student can also be asked questions on the first part of the course