

Edoardo Debenedetti

MSc STUDENT IN CS @ EPFL

☎ (+39) 340 512 6541 | ✉ edoardo.m.debenedetti@gmail.com | 🏠 edoardo.science | 📺 dedeswim | 📄 edoardo-debenedetti

Education

EPFL - Federal Institute of Technology Lausanne

Lausanne, Switzerland

MSc IN COMPUTER SCIENCE

Sep. 2019 - Mar. 2022 (Expected)

- **GPA 5.51/6**, focus on **Machine Learning** ∩ **Security** ∩ **Privacy**.
- In October I will start working on my Master's Thesis about the robustness of Vision Transformers at Princeton University, in **Prof. Mittal's** lab.
- Working on **RobustBench**, a standardized benchmark for **Adversarial Robustness** at **Prof. Flammarion's** TML Lab.
- Worked on a **research** project about **deepfakes** counteraction via influence functions at **Prof. Troncoso's** SPRING Lab.

PoliTo - Turin Polytechnic University

Turin, Italy

BSc IN COMPUTER ENGINEERING

Sep. 2016 - Jul. 2019

- **GPA 28.4/30**, graduation mark 110/110, **top 9%**.
- **Exchange year** at 同济大学 (Tongji University), in Shanghai (China), supported by a **full scholarship** granted to the top 31% applicants.

Navy Military College "F. Morosini"

Venice, Italy

HIGH SCHOOL DIPLOMA

Sep. 2013 - Jul. 2016

- Selected to lead sophomores as **prefect** during my final year.
- **Military training** on Italian Navy's Ships and at Italian Navy's Marine Corps.

Experience

Bloomberg LP

London, UK

SOFTWARE ENGINEERING INTERN

Jul 2021 - Sep. 2021

- Working in the **Multi Asset Risk System** team, designing and implementing a configuration and permission management system.

armasuisse Cyber-Defence Campus

Lausanne, Switzerland

RESEARCH INTERN

Aug. 2020 - Feb. 2021

- Conducted research about **Machine Unlearning** and **Membership Inference Attacks** against Generative Models under the supervision of **Dr. Mathias Humbert**. Tools: **PyTorch**, **PyTorch Lightning**, **Comet ML**, and **Python**.

Reply

Turin, Italy

SOFTWARE ENGINEERING INTERN

Nov. 2018 - Feb. 2019

- Developed a **chatbot** that answers questions about GDPR law, using **TypeScript**, **Redis**, **MongoDB**, **IBM Watson Assistant**, and **Docker**.
- Worked on **RPA**, using **Python**. One of the bots I developed **decreased a task duration by 88%**, without requiring human intervention in it.

Publication

[Cro+21] Croce*, F., Andriushchenko*, M., Sehwag*, V., Debenedetti*, E., Flammarion, N., Chiang, M., Mittal, P., Hein, M., **"RobustBench: a standardized adversarial robustness benchmark"**, *Workshop on Security and Safety in Machine Learning Systems*, ICLR, 2021, **Best Paper Honorable Mention Prize**, URL: <https://arxiv.org/abs/2010.09670>.

Projects

RobustBench: a standardized adversarial robustness benchmark

Graded 6/6

- **Benchmark and leaderboard** to analyze the **robustness** of image classifiers, under different threat models.
- **Model Zoo** containing 60+ **PyTorch** models trained robustly for CIFAR-10 and CIFAR-100.
- **Analysis** on the current progress in adversarial robustness: I worked on the Lipschitzness of robust models, as well as an ensemble black-box transfer attack.
- Contributed to the Model Zoo and leaderboard expansion, API refactoring and to the analysis.

Counteracting DeepFakes

Graded 5.75/6

- Term **Research Project** run at Prof. Troncoso's SPRING Lab at EPFL.
- Attempt to run **poisoning** attacks via **Influence Functions** (by Koh et al.) to counteract DeepFakes training.
- The attack was tested on MNIST-trained **autoencoder** and shown **major distortions** in the decoder outputs after the poisoned training.
- Stack: **PyTorch**, **TensorFlow** and **Keras**, on top of **Python**.

NeurIPS 2019 Reproducibility Report

Graded 6/6

- Reproducibility report of a NeurIPS 2019 paper about **black-box adversarial attacks against ML models**, submitted to the NeurIPS 2019 Reproducibility Challenge.
- With our re-implementation we **reduced by 76% the median attack time** wrt the paper. Stack: **Python**, **PyTorch**, **TeX**.

JEToP (PoliTo's Junior Enterprise)

INTERNATIONAL MANAGER

Turin, Italy

Oct. 2018 - Jun. 2019

- **Executive board** member responsible for external relations of the Junior Enterprise. Signed **8 new partnerships**.

LeadTheFuture

MENTEE

Sept. 2019 - Current

- Selected to be part of the **leading mentorship organization for STEM students in Italy** - Acceptance rate < 20%.
- Held a **mentoring session** about MSc admissions at EPFL.