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 - Apr. 2022 (Expected)*

- **GPA 5.51/6**, focus on **Machine Learning** ∩ **Security** ∩ **Privacy**.
- Working on my Master's Thesis about the robustness of Vision Transformers at **Princeton University**, in **Prof. Mittal**'s lab.
- Worked 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.

Politecnico di Torino
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*

- Worked in the **Multi Asset Risk System** team, on the re-design and implementation of the configuration of a distributed logging library.

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**.

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"**, *Thirty-fifth Conference on Neural Information Processing Systems Datasets and Benchmarks Track*, 2021, URL: `https://openreview.net/forum?id=SSKZPJCt7B`.

Honors

2021 **Best Paper Honorable Mention Prize,** ICLR 2021 Workshop on Security and Safety in Machine Learning Systems, for a preliminary version of the RobustBench paper. *Virtual*

Projects

RobustBench: a standardized adversarial robustness benchmark
EPFL, 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**.

Counteracting DeepFakes
EPFL, 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**.

Membership Inference Attacks against "unlearned" GANs

armasuisse CYD Campus

- Adapt the MIA technique proposed by the *GAN-Leaks* work (by Chen at al.), in order to improve the performance when the adversary can **observe the model before and after retraining** given the removal of some datapoints.
- Provide intuition of why the **unlearning setting makes membership inference easier**.
- The technique achieved **promising results** when attacking DCGAN trained on the CelebA dataset
- Stack: **PyTorch**, **PyTorch Lightning**, **CometML**, on top of **Python**.

Distributed logging library configuration

Bloomberg LP

- Move the configuration of a **distributed logging library** from an internal technology to a **centralized SQL DB**.
- Used a **cache** and created a **C++ based service** to fetch the configuration and serve it to the client library.
- The configuration is checked **~1M times per minute**, and the usage of the cache gave a **~23x speed improvement** w.r.t. querying the DB.
- Stack: **C++03**, **C++17**, **Comdb2** (SQL).

Extra

JEToP (PoliTo's Junior Enterprise)

Turin, Italy

International Manager

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.