Lorenzo Cazzaro, Ph.D. student

lorenzo.cazzaro@unive.it @LorenzoCazz
https://www.linkedin.com/in/lorenzo-cazzaro-622b37175/
+393486494934
via J.Castelli 43, Venice, Italy

Profile

Extremely curious and hard-worker second-year Ph.D. student in Computer Science at Ca' Foscari University of Venice. Independent and motivated student who started his training in research immediately after earning his Bachelor's Degree in Computer Science and participated proactively in research activities about the intersection of Artificial Intelligence, Cybersecurity and Formal Methods. Possessing good time management and teamwork skills.

Education

2021 – · · · ·
Ph.D in Computer Science, Ca' Foscari University of Venice
Research project title: *Principled Verification of Machine Learning Models*
Research interests: *Adversarial Machine Learning, Verification of Machine Learning Models, Applications of Artificial Intelligence in Cybersecurity*.

2019 – 2021
M.Sc. in Computer Science - Software Dependability and Cyber Security (summa cum laude), Ca' Foscari University of Venice
Thesis title: *AMEBA: An Adaptive Approach to the Black-Box Evasion of Machine Learning Models*.

2018
Cybersecurity training in Cyberchallenge.IT 2018, Ca' Foscari University of Venice
Cyberchallenge.IT is the first Italian training program in cybersecurity for talented young. 20 students are admitted per University. The training consists of theoretical lessons and challenges typical of CTF competitions.

2016 – 2019
B.Sc. in Computer Science - Data Science (summa cum laude), Ca' Foscari University of Venice
Thesis title: *Transferability of Adversarial Examples from Linear SVM to Decision Tree Ensembles*.

Employment History

2022-2023
- **Database Systems teaching assistant senior**, Ca' Foscari University of Venice.
- **Algorithms and Data Structures teaching assistant senior**, Ca' Foscari University of Venice.

2022
- **Discrete Math teaching assistant**, Ca' Foscari University of Venice.
- **Database Systems teaching assistant**, Ca' Foscari University of Venice.
- **Cryptography teacher for CyberChallenge.IT 2022**, Ca' Foscari University of Venice.

2021-2022
- **Algorithms and Data Structures teaching assistant senior**, Ca' Foscari University of Venice.

2021
- **Discrete Math teaching assistant**, Ca' Foscari University of Venice.
- **Cryptography and Software Security teacher for CyberChallenge.IT 2021**, Ca' Foscari University of Venice.

2020 - 2021
- **Linear Algebra teaching assistant**, Ca' Foscari University of Venice.

2019 - 2020
- **Research fellow in Adversarial Machine Learning**, Ca' Foscari University of Venice.

2019
- **Trainee - Web Development**, Ennova Research S.r.l. - Mestre/Venice

Research Publications

Journal Articles

1. Calzavara, S., **Cazzaro, L.**, Lucchese, C., Marcuzzi, F., & Orlando, S. (2022). Beyond Robustness: Resilience Verification of Tree-Based Classifiers. *Computers & Security*, *121*, 102843. doi:https://doi.org/10.1016/j.cose.2022.102843

Conference Paper

1. Calzavara, S., **Cazzaro, L.**, Lucchese, C., & Marcuzzi, F. (Forthcoming - Accepted at SaTML 2023). Explainable Global Fairness Verification of Tree-Based Classifiers.
2. Calzavara, S., **Cazzaro, L.**, & Lucchese, C. (2021). AMEBA: An Adaptive Approach to the Black-Box Evasion of Machine Learning Models. In J. Cao, M. H. Au, Z. Lin, & M. Yung (Eds.), *ASIA CCS '21: ACM asia conference on computer and communications security, virtual event, hong kong, june 7-11, 2021* (pp. 292–306). doi:10.1145/3433210.3453114

Conference Presentations

2023 — Speaker at **IEEE Conference on Secure and Trustworthy Machine Learning (IEEE SaTML 2023), Raleigh, North Carolina, USA** - Presentation of the paper *Explainable Global Fairness Verification of Tree-Based Classifiers*.

2022 — Speaker at **AI for Security and Security of AI workshop (AISSAI22) in Italian Conference on Cybersecurity (ITASEC22), Rome, Italy** - Presentation of the short version of the paper *Beyond Robustness: Resilience Verification of Tree-Based Classifiers*.

2021 — Speaker at **ACM Asia Conference on Computer and Communication Security (ASIACCS21), virtual event** - Presentation of the paper *AMEBA: An Adaptive Approach to the Black-Box Evasion of Machine Learning Models*.

Invited Talks

2021 — Invited speaker at **OWASP Italy Meetup in December 2021** - Talk on the topic *An introduction to the security of AI (extended version)*.

Invited speaker at **Security Summit Italy Streaming Edition in November 2021** - Talk on the topic *An introduction to the security of AI*.

Awards and Achievements

2021 — **First prize for the best master's thesis in Computer Science**, Ca' Foscari University of Venice.

2018 — **Merit Award: first prize for the best freshman of the Bachelor's Degree in Computer Science**, Ca' Foscari University of Venice.

Skills

Languages — CEFR B2 level in reading, writing, listening and speaking skills in English.

Coding — Strong coding skills in C, C++ and Python; medium coding skills in LaTeX, R, Javascript, SQL

Skills (continued)

Web Dev	Experience with Angular, Apache Web Server, ExpressJS, Flask, PostgreSQL.
Machine Learning framework	Strong skills in using python for data cleaning and feature selection. Good knowledge of the packages scikit-learn and Tensorflow.
Research	Strong background in evasion attacks against Machine Learning models and robustness of Machine Learning algorithms. Good analytical and critical thinking and teamwork skills.

Projects

Fairness analyzer for decision tree ensembles	A fairness analyzer for decision tree ensembles written in C++. Given a decision tree ensemble and a set of sensitive features, it returns a set of logical formulas predicating on the subsets of instances on which it is guaranteed that the Machine Learning (ML) model doesn't perform causal discrimination (a fairness property) on them.
Stability analyzer for decision tree ensembles	An analyzer for decision tree ensembles written in C++. Given a decision tree ensemble and an attack specification, it returns the regions of the feature space (hyper-rectangles) in which the ML model exhibits stability.
Human detector	A tool for detecting humans in images based on the Dalal & Triggs algorithm and convolutional neural networks.
ARBAC analyzer	An analyzer of ARBAC policies in python.
Blockchain Web application	A web application based on Flask that allows one to explore American flights data stored in a blockchain.
Sudoku solver	A sudoku solver in python.
Web application for restaurant management	A web application for managing restaurant orders. The front-end is based on Angular, while the back-end is based on ExpressJS.