


Michele Mastroberti

in MicheleMastroberti •  Mic52M

Education

Master of Science in Cybersecurity

University of Milan

Milan, Italy

2023 – Present

Thesis: "Assurance Evaluation of AI Models"

The thesis aims to define and implement assurance checks for artificial intelligence models. These checks will focus on various aspects that impact the final model and its application, such as the training dataset, the training process, and the resulting model. The evaluations will assess several non-functional properties, including robustness to specific attacks and fairness.

Bachelor of Science in Systems and Network Security

University of Milan

Milan, Italy

2020 – 2023

High School Diploma

Galileo Galilei Scientific High School

Terni, Italy

2015 – 2020

Work Experience

Research Assistant for SesarLab

University of Milan

February 2024 – February 2025

Core Competencies and Research Interests: Specialized in the application and assurance of machine learning within distributed systems, with a particular focus on MLOps practices and the assurance of cloud-based systems. Expertise encompasses the development, deployment, and rigorous evaluation of machine learning models in distributed environments, ensuring reliability, scalability, and security in cloud infrastructures.

Water Polo Instructor

September 2020 – September 2021

Lifeguard

Summer 2018, 2019, 2020

Projects

Bachelor's Thesis: "Design and Implementation of a System for Analysis and Blocking of Malicious Encrypted Traffic":

The project concerned designing and implementing advanced network security probes, ensuring that the networks are monitored and secured against advanced threats in the form of encrypted traffic. With advanced monitoring and detection techniques, the system smoothly identifies and mitigates security threats through encrypted communications while keeping the network secure. The project penetrated the state-of-the-art cybersecurity methodologies and carried out an in-depth exploration of advanced techniques in network analysis and threat mitigation. The system, therefore, proposed, utilized a careful evaluation of diverse lightweight and modern technologies, including network fingerprinting, towards attaining accurate detections on network connections. With a comprehensive approach, the project was using advanced tools and methodologies to lay a strong base for developing a dynamic solution that can handle encrypted communication—seamlessly

integrating theoretical knowledge with hands-on innovation and skillfully navigating the intricate challenges posed by encrypted network traffic.

🔊 Mic/bachelor-thesis

B. Future Challenge 2024:

The B. Future Challenge, organized by BOOM Knowledge Hub, is a competition for students that fosters innovative solutions to environmental and social challenges. The initiative emphasizes sustainability and the creation of a positive societal impact, encouraging participants to design forward-thinking and impactful projects related to AI.

On-going: AWS Certified Machine Learning Specialty 2025 - Hands On:

Currently attending a hands-on course to prepare for the AWS Certified Machine Learning Specialty certification. The course provides in-depth knowledge of building, training, and deploying machine learning models on the AWS platform, with a focus on leveraging cloud-based tools and services such as SageMaker and AWS AI frameworks.

On-going: HuggingFace ML Games Course:

Following the HuggingFace course on machine learning applications in video game development. The course focuses on leveraging large language models (LLMs) to enhance non-player character (NPC) behavior, enabling dynamic and intelligent interactions. The primary goal is to explore the integration of AI in gaming environments and develop innovative solutions for real-time NPC behavior management.

Languages

Italian: Mother tongue

English: Cambridge B2 Level

Chinese: beginner level

Skills

Security and Security Assurance: Network Monitoring and Analysis, Data Center Monitoring, Network Analysis, Malware Analysis, Distributed Systems Security, Cloud Security, Intrusion Detection and Prevention Systems (IDPS), Incident Response, Security for Cloud-Native Environments, Edge Cloud Security, Model Validation for Machine Learning, AI Governance and Risk Management, Explainable AI (XAI)

Programming Languages: Python, Bash scripting.

Operating Systems: Linux, Windows.

Tools: Docker, Kubernetes, Prometheus, AWS Security Hub, Wireshark, Nmap, Metasploit, TcpDump, Zeek, Docker Security Scanning, Snort, Suricata, Bro IDS, Trend Micro IoT Security, SciKitLearn, Numpy, Pandas, TensorFlow, AutoKeras, AIFairness360, Adversarial Robustness Toolbox.

I hereby authorize the processing of my personal data pursuant to Art. 13 of Legislative Decree no. 196/03 and Art. 13 of GDPR (EU Regulation 2016/679).

A handwritten signature in black ink, appearing to be 'Mich', is written over a horizontal line.