GIANLUCA CAPOZZI, PH.D.

Cybersecurity and AI Researcher | Adversarial ML | Binary Analysis

PROFILE

Cybersecurity and AI researcher with a Ph.D. in Artificial Intelligence from Sapienza University of Rome.
Specializing in adversarial machine learning, binary similarity systems, and secure ML model design.
Strong background in Python, PyTorch, and modern ML frameworks.

RESEARCH EXPERIENCE

Post-doctoral Research Fellow in Cybersecurity and AI

Department of Computer, Control and Management Engineering, Sapienza University of Rome

June 2025 – ongoing | Rome, IT

Supervisor: Prof. Giuseppe Antonio Di Luna

- Research on advanced adversarial attacks against neural network-based systems for binary analysis, focusing on novel perturbation techniques to evaluate model vulnerabilities.
- Developing and evaluating defensive methodologies for robust AI models within binary analysis.

Research Collaboration (Collaborazione Occasionale)

CINI - Consorzio Interuniversitario Nazionale per l'Informatica

November 2024 | Rome, IT

Project: Studio di fattibilità per l'implementazione di un metodo per l'analisi del codice binario attraverso tecniche basate su machine learning
Supervisor: Prof. Leonardo Querzoni

- Evaluated function-level binary code representations: linear disassembly and execution traces for sequence-based models (RNN/Transformer), and control-flow graphs with engineered features for Graph Neural Networks.

Visiting Researcher

University College London, Department of Computer Science

January 2024 – July 2024 | London, UK

Supervisor: Prof. Lorenzo Cavallaro

- Investigated state-of-the-art neural network-based methods for source and binary code analysis.
- Conducted large-scale evaluation of adversarial robustness for deep learning-based Binary Function Similarity Systems, identifying critical vulnerabilities.
- Resulted in a first-author publication at the IEEE Euro S&P 2025 Conference [1].

Research Fellow in Cybersecurity and AI

Department of Computer, Control and Management Engineering, Sapienza University of Rome

September 2021 – October 2021 | Rome, IT

Project: Studio, pianificazione, analisi e valutazione di soluzioni per la generazione di codice binario resistente all'analisi di similarità
Supervisor: Prof. Leonardo Querzoni

- Studied neural network-based methods for binary function similarity systems.
- Studied the feasibility of adversarial attacks against binary function similarity systems.

Research Collaboration (Contratto di cessione di diritto d'autore)

CINI - Consorzio Interuniversitario Nazionale per l'Informatica

May 2021 - August 2021 | Rome, IT

Project: Studio sui meccanismi e gli strumenti per la compilazione e decompilazione del codice sorgente in ambito embedded systems
Supervisor: Prof. Leonardo Querzoni

- Investigated compilation toolchains for generating and loading executables on embedded devices.
- Investigated reverse engineering tools for static and dynamic binary code analysis.

Research Collaboration (Collaborazione Occasionale)

CINI - Consorzio Interuniversitario Nazionale per l'Informatica

March 2021 – April 2021 | Rome, IT

Project: Studio dei meccanismi di packing per firmware di dispositivi di rete
Supervisor: Prof. Leonardo Querzoni

- Analyzed disassembly techniques and tools: Radare2, IDA Pro, Ghidra, angr, BAP.
- Studied compiler toolchains (GNU, AVR, LLVM) and executable formats.
- Investigated the disassembly of firmware binaries in embedded systems environments.

EDUCATION

National Ph.D. Program in Artificial Intelligence

Department of Computer, Control and Management Engineering, Sapienza University of Rome

November 2021 – May 2025 | Rome, IT

Advisor: Prof. Giuseppe Antonio Di Luna
Thesis title: *"Attacking Binary Function Similarity Systems" [2]*
Publications:

- [1] **First author**. Presented the first large-scale adversarial analysis of Binary Function Similarity systems, based on a black-box methodology; accepted at *IEEE Euro S&P 2025*.
- [3] **First author**. Proposed an integrated system for comparing binaries within a firmware against a knowledge base.
- [4] **First author**. Proposed black-box and white-box attack methods against Binary Function Similarity systems, with a novel heuristic based on embedding spaces to guide the perturbation generation.

M.Sc. in Engineering in Computer Science

Department of Computer, Control and Management Engineering, Sapienza University of Rome

September 2018 – January 2021 | Rome, IT

Advisor: Prof. Leonardo Querzoni
Thesis title: *"A study on the robustness of the SAFE system for binary similarity against adversarial coding attacks"*
Mark: 110/110

B.Sc. in Computer and Control Engineering

Department of Computer, Control and Management Engineering, Sapienza University of Rome

September 2015 – December 2018 | Rome, IT

Advisor: Prof. Leonardo Querzoni
Thesis title: *"iMedical: un'applicazione progettata per migliorare l'interazione tra medico e paziente"*
Mark: 97/110

ADDITIONAL QUALIFICATIONS

Abilitazione alla professione di Ingegnere dell'Informazione Sezione A

Sapienza University of Rome

24 November 2021 | Rome, IT

FUNDED PROJECTS

- Scientific coordinator of the project “RL-based and LLM-based Attacks against Binary Code Models” within the “Avvio alla Ricerca” program, funded by Sapienza University of Rome.
- Scientific coordinator of the project “Attacking and Defending Code Models” within the “Avvio alla Ricerca” program, funded by Sapienza University of Rome.

RESEARCH PROJECTS PARTECIPATIONS

- Member of the Project “SAFE-ES” within the “Piano Nazionale della Ricerca Militare” program.
- Member of the Ateneo Project “Automatic and Scalable Analysis of Environment-sensitive Malware”, funded by Sapienza University of Rome.
- Member of the Ateneo Project “Execution-Aware Assembly Code Models for Securing Smart Devices”, funded by Sapienza University of Rome.
- Collaborator of the Project “SINAPSI”.
- Collaborator of the Project “MBDA OdA 74104/2017”.

SERVICE

Program and Organization Committees:

- Program Committee member for the 1st HotDiML Workshop, co-located within the 45th IEEE International Conference on Distributed Computing Systems (ICDCS), 2025.
- Organization Committee member for the 18th European Conference on Computer Systems (EuroSys), 2023.

Reviewing Activities:

- Reviewer for the 1st HotDiML Workshop, co-located within the 45th IEEE International Conference on Distributed Computing Systems (ICDCS), 2025.
- Reviewer for the 27th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS), 2025.
- Reviewer for the IEEE Transactions on Software Engineering journal (IEEE TSE), 2024.
- Reviewer for the 25th International Conference on Distributed Computing and Networking (ICDCN), 2024.

TEACHING

Teaching Assistant for the “Sistemi di Calcolo” course

Department of Computer, Control and Management Engineering, Sapienza University of Rome

A.Y. 2021/2022 - A.Y. 2022/2023 — Rome, IT

SEMINARS

Seminar for the IntelliSEC Research Group – “Attacking Binary Function Similarity Systems” (remote)

Karlsruhe Institute of Technology

28 August 2025 — Karlsruhe, DE

Seminar for the Machine Learning course - “Adversarial Attacks against Classification Systems”

Department of Computer, Control and Management Engineering, Sapienza University of Rome

14 December 2021 — Rome, IT

PUBLICATIONS

1. **G. Capozzi**, T. Tang, J. Wan, Z. Yang, D. C. D’Elia, G. A. Di Luna, L. Cavallaro, and L. Querzoni, “On the lack of robustness of binary function similarity systems,” in *Proceedings of the 10th IEEE European Symposium on Security and Privacy (EuroS&P ’25)*, 2025, pp. 980–1001. DOI: 10.1109/EuroSP63326.2025.00060.
2. **G. Capozzi**, “Attacking binary function similarity systems,” Available at https://hdl.handle.net/11573/1740580, PhD thesis, Sapienza University of Rome, May 2025.

3 **G. Capozzi**, G. Laurenzi, M. Mormando, C. Gianni, G. Marcilli, L. Querzoni, and G. Di Luna, “Binsafe: Extending functions embeddings to entire binaries,” in *Proceedings of the Joint National Conference on Cybersecurity (ITASEC & SERICS 2025)*, ser. CEUR Workshop Proceedings, urn:nbn:de:0074-3962-X, 2025.

4 **G. Capozzi**, D. C. D’Elia, G. A. Di Luna, and L. Querzoni, “Adversarial attacks against binary similarity systems,” *IEEE Access*, vol. 12, pp. 161 247–161 269, 2024. DOI: 10.1109/ACCESS.2024.3488204.