Gabriele Digregorio

io.no.ctf@gmail.com io-no @Io_no__
io-no.com io-no

Languages: Italian (native), English (professional proficiency)

Education

2023 – 2026 **Ph.D. Information Technology (Cybersecurity)**, Politecnico di Milano.
Thesis: A Systems Perspective on Machine Learning Security: from Malware-Detection Pipelines to Model Artifacts.
Distinction: With honors.

2020 – 2023 **M.Sc. Computer Science and Engineering**, Politecnico di Milano.
Thesis: Tarallo: An End-to-End Framework for Malware Behavior Obfuscation.
Grade: 110/110 with honors.

2017 – 2020 **B.Sc. Computer and Automation Engineering**, Politecnico di Bari.
Thesis: Analysis of the performance of NB-IoT technology adapted for satellite communications.
Grade: 110/110 with honors.

Experience and Research

Nov 2025 - now **Security Research Intern** - Systems Security Automation, IBM Research, Zurich. Research on AI-driven automation of kernel security analysis, with a focus on integrating AI into pipelines for exploit generation.

Conference Talks

May 2026 **Speaker** at the 47th IEEE Symposium on Security and Privacy. IEEE S&P 2026. Hilton San Francisco Union Square, San Francisco, CA, U.S.A. "On the (In)Security of Loading Machine Learning Models".

Jun 2024 **Speaker** at the IEEE 99th Vehicular Technology Conference. VTC2024-Spring. Marina Bay Sands Hotel, Singapore, Singapore. "Evaluating the Impact of Privacy-Preserving Federated Learning on CAN Intrusion Detection".

Experience and Research (continued)

Jul 2024 — **Speaker** at the 21st Conference on Detection of Intrusions and Malware & Vulnerability Assessment. DIMVA '24. EPFL, Lausanne, Switzerland. "Tarallo: Evading Behavioral Malware Detectors in the Problem Space"

Awards

May 2026 — **Distinguished Artifact** for "On the (In)Security of Loading Machine Learning Models" at IEEE S&P 2026. Hilton San Francisco Union Square, San Francisco, CA, U.S.A.

Oct 2024 — **Best Poster Award** for "libdebug, Build Your Own Debugger for a Better (Hello) World" at ACM SIGSAC CCS 2024, Salt Lake City, U.S.A.

Community's Choice Poster Award for "libdebug, Build Your Own Debugger for a Better (Hello) World" at ACM SIGSAC CCS 2024, Salt Lake City, U.S.A.

Invited Talks

Nov 2025 — "Ctrl+SPACE CTF: Behind the "scenes" of the 1st European in-Orbit Hacking Challenge." ESA Security For Space Systems (3S) 2025, ESA ESTEC (European Space Research and Technology Centre), Noordwijk, The Netherlands (with Daniele Lain, Davide Avanzi, Yohann Roiron)

Projects

Starting from 2023, I am a **maintainer of libdebug**, an open-source Python library with C/C++ bindings for debugging binary executables, designed with efficiency and programmability in mind. libdebug is implemented as a debugger from scratch, built directly on low-level system calls rather than as a wrapper around existing debugging tools.

- GitHub: `https://github.com/libdebug/libdebug`
- PyPi: `https://pypi.org/project/libdebug/`

Bug Hunting Activities

I have responsibly disclosed security issues in multiple platforms and products, including **Keras**, **Google Messages** (on Wear OS), **Android**, **Skops** (by Hugging Face), and **Redis**. Some of these findings were significant enough to earn **bug bounties** and receive public **CVE** advisories. A selection of reports I've written and can ethically share publicly is available on my GitHub: io-no/CVE-Reports.

Associations & Activities

CTF Player

I actively participate in Capture The Flag (CTF) competitions with the **mhackeroni** and **Tower of Hanoi** teams. During CTFs, I usually work on binary/rev categories and support misc/ML.

2022 – now

mhackeroni, union of several Italian CTF teams.
Web-site: `mhackeroni.it`.
Core contributor to the team's international competitive results during my membership, including winning **Hack-A-Sat 4** (organized by the Air Force Research Laboratory, the world's first CTF in space) and reaching the finals of **DEF CON 34**, **DEF CON 33**, **DEF CON 32**, and **DEF CON 31**.
Since **DEF CON 34**, contributed to the development and coordination of **LLM-based tooling** adopted by mhackeroni for high-level CTF competitions.
Involved in team management and organization, supporting coordination, planning, and internal operations.

2021 - now

Tower of Hanoi, CTF team from Politecnico di Milano.
Web-site: `towerofhanoi.it`.
Involved in team management and organization, supporting coordination, planning, and internal operations. Team treasurer since 2024.

CTF Organizer, Trainer & Contributor

2026

Challenge Developer, **Team Europe** Qualifiers 2026 / **WICC** Team Europe Selection.
Event Details: Selection processes for **Team Europe 2026**, representing Europe at the **International Cyber Security Challenge (ICSC)**, and for the European team competing at the **Women+ International Cyber Security Challenge (WICC)**.
My Role: Invited as a volunteer challenge author for these selection processes. Developed `BrokenSlop`, a reverse-engineering challenge on a transformer-like language model built around a reversible Feistel network and a CPython 3.13 experimental JIT bug.

2025

Ctrl+Space CTF (in-orbit competition), organized by mhackeroni with the **European Space Agency (ESA)** and **D-Orbit**.
Event Details: Online qualifiers + on-site finals at the ESA Security for Space Systems (3S) Conference, with challenges running in orbit on D-Orbit's ION Satellite Carrier.
My Role: Proposal drafting, development, challenge supervision, project management, and challenge testing. I also coordinated communication between D-Orbit (industry), ESA (government), and mhackeroni (team).

Associations & Activities (continued)

ToH CTF, organized by Tower of Hanoi.
Event Details: A 24-hour online CTF opened to global participation.
My Role: Authored challenges based on `0-day` vulnerabilities I discovered in Keras (after responsible disclosure and with Google's permission). I also handled project management, challenge supervision, and testing.

2024 - now **CyberChallenge**, CTF Training Program by Cybersecurity National Lab.
Web-site: `https://cyberchallenge.it`
My Role: Instructor at Politecnico di Milano's Section.

Jul 2025 **International Ethical Hacking Bootcamp**, hosted by TU Wien.
Event Details: An international technical bootcamp with 150 participants, including national CTF teams from across Europe.
My Role: Delivered one of the technical training sessions.

Apr 2025 **Team Europe Training Session**.
Details: Team Europe is composed of top talents selected from national teams across the continent to represent Europe at the International Cyber Security Challenge (ICSC).
My Role: Held a dedicated technical training session for the team.

Sep 2024 **Team Italy Training Program**.
Details: Team Italy is composed of young talents formed through Cybersecurity National Lab training programs.
My Role: Technical trainer specializing in reverse engineering, dynamic analysis, and software side-channel attacks.

Research Publications

Peer-Reviewed Conference Proceedings (Selected)

1. **G. Digregorio**, M. Di Gennaro, S. Zanero, S. Longari, and M. Carminati, " On the (In)Security of Loading Machine Learning Models," in *2026 IEEE Symposium on Security and Privacy (SP)*, Los Alamitos, CA, USA: IEEE Computer Society, May 2026, pp. 214–231. DOI: 10.1109/SP63933.2026.00123.

2. **G. Digregorio**, R. A. Bertolini, F. Panebianco, and M. Polino, "Poster: libdebug, Build Your Own Debugger for a Better (Hello) World," in *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '24, Salt Lake City, UT, USA: Association for Computing Machinery, 2024, pp. 4976–4978, ISBN: 9798400706363. DOI: 10.1145/3658644.3691391.

3 **G. Digregorio**, E. Cainazzo, S. Longari, M. Carminati, and S. Zanero, "Evaluating the Impact of Privacy-Preserving Federated Learning on CAN Intrusion Detection," in *2024 IEEE 99th Vehicular Technology Conference (VTC2024-Spring)*, IEEE, 2024, pp. 1–7. DOI: 10.1109/VTC2024-Spring62846.2024.10683636.

4 **G. Digregorio**, S. Maccarrone, M. D'Onghia, *et al.*, "Tarallo: Evading Behavioral Malware Detectors in the Problem Space," in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, Springer, 2024, pp. 128–149. DOI: 10.1007/978-3-031-64171-8_7.

Preprints

1 **G. Digregorio**, M. D. Gennaro, F. Pastore, S. Zanero, S. Longari, and M. Carminati, "Lifecycle-aware dynamic analysis for secure ml model execution," 2026. arXiv: 2606.19023 [cs.CR]. URL: https://arxiv.org/abs/2606.19023.