Filippo De Grandi

Italy, currently Ireland | fdegra@proton.me | github.com/Degra02 | linkedin.com/in/filippo-de-grandi-226198224 | fdegra.com

Systems and embedded security engineer. Currently on Qualcomm's TEE team working with ARM TrustZone, finishing an MSc in Cybersecurity at the University of Trento. Background in low-level C/Rust, embedded attack and defense (MITRE eCTF 2025 & 2026), and Linux infrastructure. Interested in memory-safe systems software and open source.

Work Experience

Secure Kernel Developer Intern June 2026 — Present
Qualcomm *Cork, Ireland*
- TEE team: develop and review secure-world components running under ARM TrustZone (TEE, secure monitor, aarch64)
- Develop Trusted Applications and the corresponding HLOS daemon bridging normal-world clients to secure-world services
- Threat-model and review the boundaries between the normal world (Linux) and the secure world

Intern 2024 — 2024
Fondazione Bruno Kessler - FBK *Trento, Italy*
- Worked on the thesis project regarding CVEs and CWEs, studying the current state of the art on BAS tools

Student Tutor - Advanced Programming 2023 — Present
University of Trento *Trento, Italy*
- Tutor on the Rust programming language, creating exercises and teaching students.

Education

University of Trento 2024 — Present
Master in Computer Science, Cybersecurity track *Trento, Italy*
- Relevant Coursework: Security Testing, Network Security, Ethical Hacking, Applied Cryptography, Advanced Programming of Cryptographic Methods
- Current GPA: 29.5/30

University of Trento 2021 — 2024
Bachelor of Science in Computer, Electrical and Telecommunication Engineering *Trento, Italy*
- Thesis: BAS Tools: Implementation of an attack pattern to mimic a threat actor — 110/110 with honors
- Relevant Coursework: Advanced Programming, Algorithms and Data Structures, Software Engineering

Projects & Associations

eCTF Challenge Participant, MITRE Corporation 2025 — 2026
- Member of the UniTN team in a two-phase embedded security competition: design a secure system to spec, then attack other teams' validated designs
- **2026**: contributed to a Hardware Security Module for a chip foundry: encrypted file storage with permission-group access control and HSM-to-HSM transfers (7th place)
- **2025**: contributed to a satellite TV decoder enforcing per-channel subscriptions over a unidirectional broadcast stream (13th place)
- Attack phase: analyzed and exploited other teams' designs via software and hardware attacks (C, Python, GDB, ChipWhisperer)

CyberChallenge Finalist, Cybersecurity National Lab - CINI 2024 — 2024
- Reached the final stage with the UniTN team, competing across web security, cryptography, reverse engineering and binary exploitation (Python, Ghidra, GDB, Burp Suite)

Self-hosted Linux Environment, Personal Infrastructure / Homelab 2022 — Present
- Run a Proxmox cluster self-hosting personal services: hardened Linux hosts, VPN, automated backups and monitoring (Linux, Proxmox, Docker, Git)
- Manage secrets and reverse proxying; configuration kept reproducible and version-controlled

Awards

- **Public AI Challenge Winner** — HIT & Trentino Sviluppo, 2025: ML model predicting pollen concentration from weather data
- **Hackathon Winner** — NOI Techpark, 2025: contributed to C3Nav, an open-source indoor navigation system

Skills

- **Security**: ARM TrustZone / TEE, embedded attack and defense, binary exploitation, reverse engineering, side-channel and fault injection, threat modeling, MITRE ATT&CK / CVE / CWE
- **Systems**: Linux internals, containers, networking
- **Languages**: Rust, C, C++, Python, Bash, assembly (ARM/x86)
- **Tools**: GDB, Ghidra, ChipWhisperer, QEMU, Docker, Proxmox, Git, CI/CD
- **Spoken**: English (C1 Cambridge, C2 Bulats), Italian (native)