Updated in July 2025

Alexis CHALLANDE

Paris, France • (+33) 6 20 00 17 34 • alexis@challande.eu
linkedin.com/in/alexis-challande/ • github.com/DarkaMaul/ • darkamaul.github.io

PROFESSIONAL SUMMARY

After completing a PhD in Computer Science at École Polytechnique (France) focused on vulnerability detection using semantic patch signatures in closed source binaries, I've joined Trail of Bits to focus on security engineering for ecosystems. I have been part of the larger initiative to add packages attestations to the Python Package Index, layering bases for securely interacting with the package manager. I am also interested in using static analysis methods (e.g. CodeQL) to find security problems in the software supply chain and remediate them.

PROFESSIONAL EXPERIENCE

***Trail of Bits**, Remote • Security Engineer* — *09/2023 - Present*

- Analysed security vulnerabilities for a large open-source project and performed patch analysis, exploit generation, and variant analysis.
- Authored a RFC3161 client used in the sigstore ecosystem to power package attestations in the Python Package Index.
- Found multiple instances of Denial of Service due to recursions in various large projects and published the results at DistrictCon 0.
- Developed an infrastructure engine to create scenarios for assessing AI agents offensive capabilities.

***Quarkslab**, Paris • Security Engineer* — *10/2018 - 12/2022*

- Conducted a PhD on the research of 1-day vulnerabilities in Android phones
- Reverse engineer Android applications to perform security audits
- Developed a complex IDA Pro plugin to generate exports for arbitrary binaries
- Created tools around the Android Open Source Repository for security research

***ANSSI (French Cybersecurity Agency)**, Paris • Intern* — *03/2018 - 08/2018*

- Developed and implemented an IDA plugin to detect usage of cryptography in binary code using symbolic execution.

EDUCATION

***PhD of Computer Science** • Ecole Polytechnique, Palaiseau* — *2022*

***MSc Computer Science**, Digital Security track • Eurecom, Biot* — *2018*

SKILLS

Programming Languages	Python, C, C++, Rust (beginner)
Operating System	Unix, Android
Reverse Engineering	IDA, Ghidra

Development Tools	git, CMake, Docker, GitHub
Cloud	Azure, Terraform, CDKTF

PUBLICATIONS

Low-Effort Denial of Service with Recursion • *DistrictCon, Washington DC* *2025*

Quokka: A Fast and Accurate Binary Exporter • *GreHack, Grenoble* *2022*

Towards Patch Detection using Binary Only Semantic Signatures • *HAL* *2022*

Building a commit-level dataset of real-world vulnerabilities • *CODASPY, Baltimore* *2022*

Exploitation du graphe de dépendance d'AOSP à des fins de sécurité • *SSTIC, Rennes* *2021*

DISCLOSURES

CVE-2025-4565 • *Google* *2025*

CVE-2024-52981 • *Elastic* *2024*

CVE-2024-52980 • *Elastic* *2024*

CVE-2024-58103 • *Wire* *2024*

RUSTSEC-2024-0437 • *rust-protobuf* *2024*

CVE-2024-47072 • *XStream* *2024*

CVE-2024-7254 • *Google* *2024*