Denis MAZZUCATO

Formal Methods and Security

denismazzucato@outlook.com
denismazzucato.github.io
denis-mazzucato

Education

10/2024–3/2025 **Postdoc**, *Carmege Mellon University*, Pittsburgh, PA (USA)
Six months Postdoc position at CMU (& visiting NASA) with Corina Pasareanu

10/2020–12/2024 **Ph.D.**, *École Normale Supérieure | PSL & INRIA*, Paris (FR), supervised by Caterina Urban
Static Analysis by Abstract Interpretation of Quantitative Program Properties

10/2015–9/2020 **Master and Bachelor**, *University of Padua*, Padua (IT), magna cum laude 110/110
Computer Science, Dipartimento di Matematica, Università degli Studi di Padova

Experience

2023 **Summer School on Formal Methods**, Marktoberdorf (DE)
2 WEEKS Scientific foundations and technologies for improving the quality and security of software

2022 **Applied Scientist Intern**, *Amazon Prime Video*, Automated Reasoning Team, London (UK)
6 MONTHS Research internship project supervised by Bor-Yuh Evan Chang and Franco Raimondi

2020 **Exchange Program**, *Vrije Universiteit*, Amsterdam (NL)
6 MONTHS Exchange student program, under the supervision of Jasmin Blanchette

Awards

October 2024 **Radhia Cousot Award**, *Young Researcher*, SAS 2024, Pasadena (USA), 3 000€ prize from the ENS foundation for the publication: "Quantitative Static Timing Analysis"

Spring 2024 **Automated Reasoning Amazon Research Award**, *Funding Award*, Amazon, 70 000€ prize
"Proving the Absence of Timing Side Channels in Cryptographic Applications" with Corina Pasareanu

Selected Projects

PHD THESIS **Static Analysis by Abstract Interpretation of Quantitative Program Properties**, `inria.hal.science/tel-04886659`, PhD Thesis, Denis Mazzucato, December 2024
My PhD Thesis focuses on static analysis by **abstract interpretation**, a general theory for approximating program semantics, of **quantitative program properties**. Use cases range from **neural network fairness** quantification to **timing side-channel** robustness.

PUBLISHED SAS 2024 **Quantitative Static Timing Analysis**, `doi.org/10.1007/978-3-031-74776-2_11`, Denis Mazzucato, Marco Campion, and Caterina Urban; Winner of the *Radhia Cousot Award*.
Sound static analysis by abstract interpretation to quantify the dependencies between input data and the execution time of a program. As the first author of this project, I contributed at every stage:
- I **conceived the idea** of combining syntactical non-interference with abstract interpretation to quantify the impact of input data on the number of iterations.
- I **implemented** the analysis in the `TimeSec` tool, written in *Python* with *APRON*'s abstract domains.
- I **identified** a suitable cryptographic library for our needs and **set up the benchmarks**, creating an artifact to ensure full reproducibility of the paper's results.
- I **wrote** the paper and designed an accessible presentation to effectively communicate my findings to the formal methods community, leading to my recognition with the *Radhia Cousot Award*.

RESEARCH INTERNSHIP **Backwards TypeScript Code Analysis within Promise Chains**, *Amazon, Automated Reasoning Team*, Supervised by Bor-Yuh Evan Chang and Franco Raimondi, Summer 2022, London (UK)
I developed a static analysis to enable backwards reasoning on TypeScript code within promise chains. The tool is based on the TaJS abstract interpreter written in Scala, with a pre-analysis in Datalog. During this research internship, I learned how to work in a team, developed coding best practices, and how to employ a customer-driven mindset.

ONGOING WORK **Relational Hoare Logic for Realistically Modelled Machine Code**, *from the ARA award*, In collaboration with Carnegie Mellow University, NASA, Stanford University, and Amazon AWS.
Verification of relational properties, such as timing side-channel freedom or program equivalence, in the performance- and security-critical context of the *Assembly s2n-bignum* library of AWS, part of their cryptographic TLS/SSL implementation; fully formalized in the *HOL Light* theorem prover (*OCaml*).