Denis MAZZUCATO

Security Expert & Formal Methods

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

Core Competencies

Security	Expertise in developing static analysis tools based on formal verification for security vulnerabilities
Languages	Fluent in Python, Scala, Haskell; knowledge of OCaml, C, C++, Java, JavaScript, Lean, Agda
Tooling	Experience with Git, GitHub workflows, LaTeX, CI/CD, and AWS cloud computing platforms
Research	Awards winning research in static analysis by abstract interpretation of quantitative program properties

Professional Experience

october 2024 – march 2025
Postdoctoral Researcher – Security, Carnegie Mellon University, Pittsburgh

- Research in correctness and security of Assembly code, focusing on the *s2n-bignum* library of AWS, part of their cryptographic TLS/SSL implementation.
- Vulnerability detection of post-quantum cryptographic algorithms by the Hertzbleed attack.
- Engaged in cutting-edge research in formal methods, collaborating with renowned experts and NASA on security-critical projects.

2022, 6 months
Applied Scientist Intern – Automated Reasoning Team, Amazon Prime Video, London

- Developed a static analysis tool for backwards reasoning on TypeScript code within promise chains, leveraging TaJS and Datalog to enable local reasoning around code assertions.
- Collaborated in a customer-driven, team-oriented environment to ensure that analytical methods were aligned with production needs and security best practices.

december 2024 – october 2020
Ph.D. Researcher – Quantitative Program Analysis, École Normale Supérieure & INRIA, Paris

- Conducted award-winning research in quantitative static timing analysis to measure and mitigate timing side-channel vulnerabilities in cryptographic applications.
- Designed and implemented the TimeSec tool in Python, applying abstract interpretation and leveraging APRON's domains to quantify the impact of input data on execution timing.
- Authored key publications and presented findings at academic conferences, earning the Radhia Cousot Award for innovation in security research.

2018, 6 months
Quality Assurance Developer, *THRON*, Padua (IT)

- Developed automated testing frameworks for the THRON document management system, ensuring the quality and reliability before reaching the production environment.
- Developed a serverless architecture for a probing system to monitor the real-time performance of the platform, the system was deployed to AWS Lambda functions.

Additional Experience & Projects

2025, current
Ongoing Collaborative Research, *Carnegie Mellow University, NASA, Stanford University, AWS*
Relational Hoare logic for verifying security properties in critical cryptographic libraries.

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

2020, 6 months
Exchange Program, *Vrije Universiteit*, Amsterdam (NL)
Deepened knowledge in theorem provers and formal methods under the supervision of Jasmin Blanchette.

Awards & Recognitions

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

Education

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

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