

ALI EL HUSSEINI

Singapore

github.com/elhusseiniali

elhusseiniali@u.nus.edu

EDUCATION

National University of Singapore

January 2023 – Present

- I am currently a PhD candidate in the Trustworthy and Secure Software group at NUS, advised by Prof. Abhik Roychoudhury. My research is focused on improving the security of large language models (and systems that use them, i.e. agents) by understanding and analyzing how these models operate.

École Normale Supérieure Paris-Saclay

September 2019 - December 2022

- I completed both the M1 and M2 of the Parisian Masters of Research in Computer Science.

American University of Beirut

September 2014 – June 2019

- I successfully obtained a **Bachelor of Science in Computer Science** and a **Bachelor of Arts in Philosophy**.

PUBLICATIONS

Repairing LLM Executions for Secure Automatic Programming

[Ali El Hussein](#), Yacine Izza, Blaise Genest, Abhik Roychoudhury

2026 International Conference on Software Engineering (ICSE)

In this paper, we proposed a novel approach to identify and repair internal representations that cause a large language model to produce vulnerable code. We built a tool that monitors the LLM at run-time and intervenes when appropriate to improve the security of the generated code.

Detecting Python Malware in the Software Supply Chain with Program Analysis

Ridwan Shariffdeen, Behnaz Hassanshahi, Martin Mirchev, [Ali El Hussein](#), Abhik Roychoudhury

2025 International Conference on Software Engineering:

Software Engineering in Practice (ICSE-SEIP)

In this paper, we proposed a program-analysis-based approach to detect supply chain attacks in the Python ecosystem. Our tool combines AST-level differential analysis, CodeQL-based behavioral detection, and transitive dependency tracking to identify malicious Python packages.

EXPERIENCE

Static Analysis of Jupyter Notebooks

March 2022 – August 2022

INRIA Paris

France

I worked on creating an abstract domain to represent different data transformations inside Jupyter notebooks, providing an implementation of the domain in LiSA. Some of the goals of the analysis were to study the safety of the notebooks, their sensitivity to changes in shapes of data, or even the soundness of the results. I was supervised by Dr. Caterina URBAN.

Reachability-based Formal Methods for Neural Network Safety.

Apr. 2021 – Sep. 2021

Commissariat à l'Énergie Atomique (CEA)

France

I worked on using abstract interpretation to verify different formal properties (e.g. robustness) for neural networks. Specifically, my work focused on improving the soundness of the numerical computations required by the analysis on GPUs. I was supervised by Dr. Zakaria CHIHANI and Augustin LEMESLE.

A library to handle simple regular expressions.

June 2020 – August 2020

Centre National de la Recherche Scientifique (CNRS)

France

I developed a modern Python library to handle Simple Regular Expressions (see this paper). The goal was to facilitate the analysis of lossy channel systems, allowing users to verify different formal properties. I was supervised by Dr. Philippe Schnoebelen, and the library can be found [here](#).

LANGUAGE PROFICIENCY

- Arabic: Native speaker.
- English: Fluent.
- French: B2.

REFERENCES

All references are available upon request by email.