Compositional Bug Detection for Internally Unsafe Libraries: A Logical Approach to Type Unsoundness (Artifact)

Pedro Carrott
Imperial College London, UK

Sacha-Élie Ayoun
Imperial College London, UK

Azalea Raad
Imperial College London, UK

Abstract

This artifact is a companion to the paper "Compositional Bug Detection for Internally Unsafe Libraries: A Logical Approach to Type Unsoundness". It contains the Rocq formalisation of the RISL program logic, the RUXtBelt semantic model and the inadequacy theorem of RUXt. It also contains the OCaml prototype for RUXt, along with the case studies discussed in the paper.

2012 ACM Subject Classification Theory of computation → Program analysis; Theory of computation → Separation logic; Theory of computation → Programming logic; Theory of computation → Automated reasoning; Theory of computation → Program specifications; Software and its engineering → General programming languages

Keywords and phrases Rust, bug detection, static analysis, program logics, under-approximation

Digital Object Identifier 10.4230/DARTS.11.2.9

Acknowledgements This project was sponsored by the Defense Advanced Research Projects Agency, (DARPA), Information Innovation Office (I2O), Program BAA HR001124S0003, under Cooperative Agreement No. HR00112420359. Disclaimer: The content of the information does not necessarily reflect the position or the policy of the U.S. Government, and no official endorsement should be inferred. Raad is further supported by the UKRI Future Leaders Fellowship MR/V024299/1, by the EPSRC grant EP/X037029/1 and by VeTSS.

Related Article Pedro Carrott, Sacha-Élie Ayoun, and Azalea Raad, "Compositional Bug Detection for Internally Unsafe Libraries: A Logical Approach to Type Unsoundness", in 39th European Conference on Object-Oriented Programming (ECOOP 2025), LIPIcs, Vol. 333, pp. 5:1–5:28, 2025. `https://doi.org/10.4230/LIPIcs.ECOOP.2025.5`

Related Conference 39th European Conference on Object-Oriented Programming (ECOOP 2025), June 30–July 2, 2025, Bergen, Norway

Evaluation Policy The artifact has been evaluated as described in the ECOOP 2025 Call for Artifacts and the ACM Artifact Review and Badging Policy.

1 Scope

The paper makes the following claims:

- We have proven in Rocq that any UB reported by RUXt corresponds to a true safety violation.
- We have implemented in OCaml a working prototype of RUXt.

These claims are backed by the artifact, which contains the full Rocq mechanisation of the definitions and theorems presented in the paper, as well as the OCaml code for the RUXt prototype. The Rocq mechanisation consists of **(i)** the RUXtBelt semantic model; **(ii)** the RISL proof rules

DAGSTUHL ARTIFACTS SERIES
Dagstuhl Artifacts Series
Schloss Dagstuhl – Leibniz-Zentrum für Informatik,
Dagstuhl Publishing, Germany

and their soundness against RUXtBelt; and **(iii)** the formalisation of the RUXt algorithm and its inadequacy result. The prototype implementation is complemented by the `Even` and `List` case studies discussed in the paper.

2 Content

The artifact package includes:

- A README file with instructions on how to install and run the artifact.
- A Docker image containing the Rocq mechanisation and the OCaml prototype implementation.

3 Getting the artifact

The artifact endorsed by the Artifact Evaluation Committee is available free of charge on the Dagstuhl Research Online Publication Server (DROPS). In addition, the artifact is also available at: `https://doi.org/10.5281/zenodo.15268680`.

4 Tested platforms

We have tested the Docker container on a machine with the following configuration:

- **OS:** EndeavourOS
- **CPU:** 13th Gen Intel(R) Core(TM) i7-1360P @ 1.9GHz × 12
- **Memory:** 16GB
- **Disk:** 1TB
- **GPU:** Intel Iris Xe Graphics

5 License

The artifact is available under license Creative Commons Attribution 4.0 International.

6 MD5 sum of the artifact

8c254471c0089ac7139a4a6a94d1ace9

7 Size of the artifact

3.04 GiB