Semantics for Noninterference with Interaction Trees (Artifact)

Lucas Silver
University of Pennsylvania, Philadelphia, PA, USA

Paul He
University of Pennsylvania, Philadelphia, PA, USA

Ethan Cecchetti
University of Maryland, College Park, MD, USA
University of Wisconsin – Madison, WI, USA

Andrew K. Hirsch
State University of New York at Buffalo, NY, USA

Steve Zdancewic
University of Pennsylvania, Philadelphia, PA, USA

Abstract

Noninterference is the strong information-security property that a program does not leak secrets through publicly-visible behavior. In the presence of effects such as nontermination, state, and exceptions, reasoning about noninterference quickly becomes subtle. We advocate using *interaction trees (ITrees)* to provide compositional mechanized proofs of noninterference for multi-language, effectful, nonterminating programs, while retaining executability of the semantics. We develop important foundations for security analysis with ITrees: two *indistinguishability* relations, leading to two standard notions of noninterference with adversaries of different strength, along with metatheory libraries for reasoning about each. We demonstrate the utility of our results using a simple imperative language with embedded assembly, along with a compiler into that assembly language.

2012 ACM Subject Classification Theory of computation → Denotational semantics; Security and privacy → Logic and verification; Security and privacy → Information flow control

Keywords and phrases verification, information-flow, denotational semantics, monads

Digital Object Identifier 10.4230/DARTS.9.2.6

Acknowledgements This work was funded in part by the NSF under the award 1521539 (Weirich, Zdancewic, Pierce).

Related Article Lucas Silver, Paul He, Ethan Cecchetti, Andrew K. Hirsch, and Steve Zdancewic, "Semantics for Noninterference with Interaction Trees", in 37th European Conference on Object-Oriented Programming (ECOOP 2023), LIPIcs, Vol. 263, pp. 29:1–29:29, 2023.
`https://doi.org/10.4230/LIPIcs.ECOOP.2023.29`

Related Conference 37th European Conference on Object-Oriented Programming (ECOOP 2023), July 17–21, 2023, Seattle, Washington, United States

Evaluation Policy The artifact has been evaluated as described in the ECOOP 2023 Call for Artifacts and the ACM Artifact Review and Badging Policy.

1 Scope

This artifact formalizes the definitions and theorems presented in the associated paper in the Coq proof assistant.

Dagstuhl Artifacts Series, Vol. 9, Issue 2, Artifact No. 6, pp. 6:1–6:2
DAGSTUHL ARTIFACTS SERIES
Dagstuhl Artifacts Series
Schloss Dagstuhl – Leibniz-Zentrum für Informatik,
Dagstuhl Publishing, Germany

2 Content

Definitions and verified theorem proofs are contained in the provided codebase. The file Artifact-README.md provides exhaustive mappings from names and identifiers in the paper to names in the code.

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://github.com/DeepSpec/InteractionTrees/tree/secure`. And a docker image of the code is available at: `https://zenodo.org/record/7473666`.

4 Tested platforms

This code repository should build on any system with the following dependencies:

- coq >= 15.2
- coq-paco >= 4.1.2
- coq-ext-lib >= 0.11.7

5 License

The artifact is available under license . . . .

6 MD5 sum of the artifact

b4f158914476b56f95cced770ccc355c

7 Size of the artifact

1.1 GiB