A Trusted Infrastructure for Symbolic Analysis of Event-Driven Web Applications (Artifact)

Gabriela Sampaio
Imperial College London, United Kingdom
g.sampaio17@imperial.ac.uk

José Fragoso Santos
INESC-ID/Instituto Superior Técnico, Universidade de Lisboa, Portugal
Imperial College London, United Kingdom
jose.fragoso@tecnico.ulisboa.pt

Petar Maksimović
Imperial College London, United Kingdom
p.maksimovic@imperial.ac.uk

Philippa Gardner
Imperial College London, United Kingdom
p.gardner@imperial.ac.uk

Abstract

This artifact contains the implementation of JaVerT.Click, a symbolic analysis tool for modern event-driven Web applications. The tool extends JaVerT 2.0, a state-of-the-art symbolic execution tool for JavaScript (JS), with JS reference implementations of the DOM Core Level 1, DOM UI Events, JavaScript Promises and the JavaScript `async`/`await` APIs, all underpinned by a simple Core Event Semantics which is sufficiently expressive to describe the event models underlying these APIs. Our reference implementations mostly follow the respective standards line-by-line and are all thoroughly tested against the official test suite. We also evaluate JaVerT.Click by performing symbolic analysis on two real-world libraries: `cash` and `p-map`, finding three previously unknown bugs.

2012 ACM Subject Classification Software and its engineering → Formal software verification; Software and its engineering → Software testing and debugging

Keywords and phrases Events, DOM, JavaScript, promises, symbolic execution, bug-finding

Digital Object Identifier 10.4230/DARTS.6.2.5

Funding Fragoso Santos, Gardner, and Maksimović were partially supported by the EPSRC Programme Grant "REMS: Rigorous Engineering for Mainstream Systems" (EP/K008528/1) and the EPSRC Fellowship "VetSpec: Verified Trustworthy Software Specification" (EP/R034567/1). Fragoso Santos was partially supported by national funds through Fundação para a Ciência e a Tecnologia (FCT), with reference UIDB/50021/2020 (INESC-ID multi-annual funding). Sampaio was supported by a CAPES Foundation Scholarship, process number 88881.129599/2016-01.

Related Article Gabriela Sampaio, José Fragoso Santos, Petar Maksimović, and Philippa Gardner, "A Trusted Infrastructure for Symbolic Analysis of Event-Driven Web Applications", in 34th European Conference on Object-Oriented Programming (ECOOP 2020), LIPIcs, Vol. 166, pp. 28:1–28:29, 2020. `https://doi.org/10.4230/LIPIcs.ECOOP.2020.28`

Related Conference 34th European Conference on Object-Oriented Programming (ECOOP 2020), November 15–17, 2020, Berlin, Germany (Virtual Conference)

1 Scope

This artifact contains a trusted infrastructure for the symbolic analysis of modern event-driven Web applications which, we believe for the first time, supports reasoning about code that uses multiple event-related APIs within a single, unified formalism. Using this infrastructure, we

develop JaVerT.Click as an extension of JaVerT 2.0 [1], a state-of-the-art symbolic analysis tool for JavaScript. JaVerT.Click comprises: **(1)** a Core Event Semantics, which captures the fundamental building blocks underpinning the event models of widely-used APIs; and **(2)** trusted JS reference implementations of DOM Core Level 1, DOM UI Events, JS promises, and the JS `async/await`, the APIs targeted in the related paper. We provide the test suites of the four JS reference implementations. We also provide the concrete and symbolic test suites of the `cash` library [3], a widely-used alternative for jQuery, which makes heavy use of DOM UI Events. Although we have recently performed symbolic analysis on the `p−map` library [2], for space restrictions, we delay the full account of our analysis to a future publication and do not include our analysis of `p−map` in this artifact.

This artifact supports the following claims of the paper: **(1)** our JavaScript reference implementations of the DOM Core Level 1, DOM UI Events and JS Promises APIs follow the respective standards line-by-line; **(2)** all four reference implementations were thoroughly tested and pass all applicable tests as described in the evaluation section of the paper; **(3)** JaVerT.Click is able to perform symbolic analysis of the `cash` library. We create a symbolic test suite for the `events` module with 100% line coverage, establishing bounded correctness properties and findings two previously unknown bugs.

2 Content

The artifact includes:

- a README file describing the project structure, with instructions for running JaVerT.Click and reproducing the experiment results;
- the source code of JaVerT.Click implemented in OCaml;
- a VM image (`javert−click.ova`) that replicates the execution environment for JaVerT.Click.

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/javert-click/javert-click`.

4 Tested platforms

JaVerT.Click was developed and tested in OSX 10.14 and 10.15. The artifact is packaged as a VM with Ubuntu 18.4 LTS installed. The recommended VM settings include 8GB RAM and 4 allocated CPUs.

5 License

The artifact is available under the BSD 3-Clause License.

6 MD5 sum of the artifact

The md5 sum of the artifact is c835f96d72b5cfaee386637e517db944.

7 Size of the artifact

The size of the artifact is 4.92 GiB.

References

1 J. Fragoso Santos, P. Maksimović, G. Sampaio, and P. Gardner. JaVerT 2.0: Compositional Symbolic Execution for JavaScript. *PACMPL*, 3(POPL):66, 2019.

2 S. Sorhus. p-map (GitHub). `https://github.com/sindresorhus/p-map`, visited 05/2020.

3 K. Wheeler, S. Shaw, and F. Spampinato. `cash` (GitHub). `https://github.com/kenwheeler/cash`, visited 05/2020.