SESL: A Memory Safety Checker based on Separation Logic
(Competition Contribution)

Xie Li[1,2], Yutian Zhu[1,2], Zongxin Liu[1,2], Zhilin Wu[1], and Lijun Zhang[1,3]

[1] Institute of Software, China Academy of Sciences
[2] University of China Academy of Sciences
[3] IISG

Abstract. SESL is a memory safety analyzer for C programs. It uses SMACK as the front end. Its back end relies on a symbolic execution engine which encodes path constraints as array separation logic (ASL) formulas. The ASL formulas are then solved by a separation logic solver called CompSpen. The salient feature of SESL is that it utilizes array separation logic to support byte-precise formal reasoning of memory safety issues.

Keywords: Memory safety · Symbolic execution · Separation logic.

1 Overview

SESL is a static memory safety analyzer for `C` programs. The basic methodology are inherited from the symbolic execution[] and we use array separation logic(ASL) to symbolically represent the a set of states. Compared to the original separation logic(SL)[], ASL compacts a sequence of uninitialized memory into a single predicate, which improve the efficiency of analysis and checking. Based on the existing frontend tool SMACK[], we implemented a low level semantic of intermediate representation which supports byte-level manipulation of heap data. The algorithm of falsification utilizes the result of symbolic execution for later feasibility checking and error analysis using our ASL solver CompSpen[]. The main contribution of this tool is the implementation of our symbolic execution engine at backends.

2 Architecture

Front end

Back end

3 Strengths and Weaknesses

4 Tool Setup and Configuration

5 Software Project

6 Example Section

6.1 A Subsection Sample

Please note that the first paragraph of a section or subsection is not indented. The first paragraph that follows a table, figure, equation etc. does not need an indent, either.

Subsequent paragraphs, however, are indented.

Sample Heading (Third Level) Only two levels of headings should be numbered. Lower level headings remain unnumbered; they are formatted as run-in headings.

Sample Heading (Fourth Level) The contribution should contain no more than four levels of headings. Table 1 gives a summary of all heading levels.

Table 1. Table captions should be placed above the tables.

Heading level	Example	Font size and style
Title (centered)	**Lecture Notes**	14 point, bold
1st-level heading	**1 Introduction**	12 point, bold
2nd-level heading	**2.1 Printing Area**	10 point, bold
3rd-level heading	**Run-in Heading in Bold.** Text follows	10 point, bold
4th-level heading	*Lowest Level Heading.* Text follows	10 point, italic

Displayed equations are centered and set on a separate line.

$$x + y = z \tag{1}$$

Please try to avoid rasterized images for line-art diagrams and schemas. Whenever possible, use vector graphics instead (see Fig. 1).

Theorem 1. *This is a sample theorem. The run-in heading is set in bold, while the following text appears in italics. Definitions, lemmas, propositions, and corollaries are styled the same way.*

Proof. Proofs, examples, and remarks have the initial word in italics, while the following text appears in normal font.

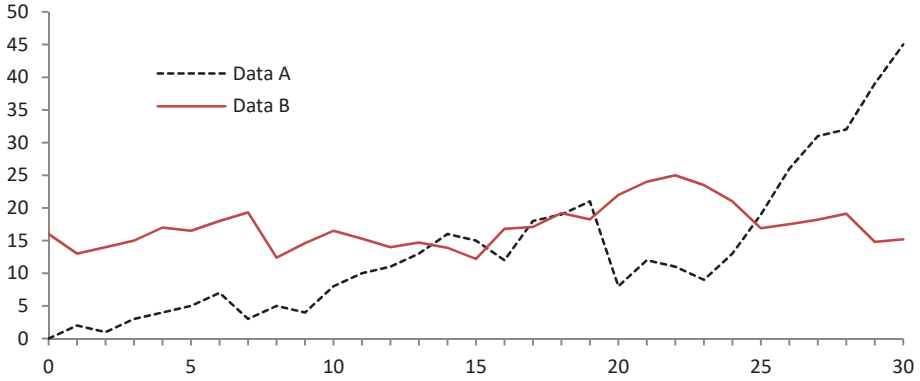

Fig. 1. A figure caption is always placed below the illustration. Please note that short captions are centered, while long ones are justified by the macro package automatically.

For citations of references, we prefer the use of square brackets and consecutive numbers. Citations using labels or the author/year convention are also acceptable. The following bibliography provides a sample reference list with entries for journal articles [1], an LNCS chapter [2], a book [3], proceedings without editors [4], and a homepage [5]. Multiple citations are grouped [1–3], [1, 3–5].

References

1. Author, F.: Article title. Journal **2**(5), 99–110 (2016)
2. Author, F., Author, S.: Title of a proceedings paper. In: Editor, F., Editor, S. (eds.) CONFERENCE 2016, LNCS, vol. 9999, pp. 1–13. Springer, Heidelberg (2016). https://doi.org/10.10007/1234567890
3. Author, F., Author, S., Author, T.: Book title. 2nd edn. Publisher, Location (1999)
4. Author, A.-B.: Contribution title. In: 9th International Proceedings on Proceedings, pp. 1–2. Publisher, Location (2010)
5. LNCS Homepage, http://www.springer.com/lncs. Last accessed 4 Oct 2017