Automation of Formal Verification (AUFOVER)

Red Hat
Kamil Dudka
November 11th 2021

Abstract

Red Hat uses static analyzers to automatically find bugs in the source code of Red Hat Enterprise Linux. Thanks to the Automation of Formal Verification (AUFOVER) project, Red Hat was able to extend the automation for the formal verification tools Symbiotic and Divine, which are developed by research groups of Masaryk University in Brno.

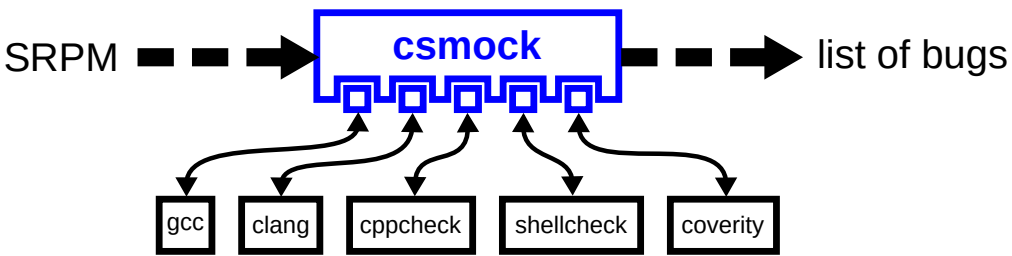
Automation of Formal Verification (AUFOVER)

- Project supported by Technology Agency of the Czech Republic: https://starfos.tacr.cz/en/project/TH04010192
- Driven by Honeywell as the main participant.
- Red Hat was integrating tools developed at Masaryk University:
  - Divine – explicit-state model checking
  - Symbiotic – instrumentation, slicing and symbolic execution
- Now available in Fedora:

  https://lists.fedoraproject.org/archives/list/devel@lists.fedoraproject.org/thread/RQBBWQOCMYVVEAIGMTX4MNHBIRALRNA3/

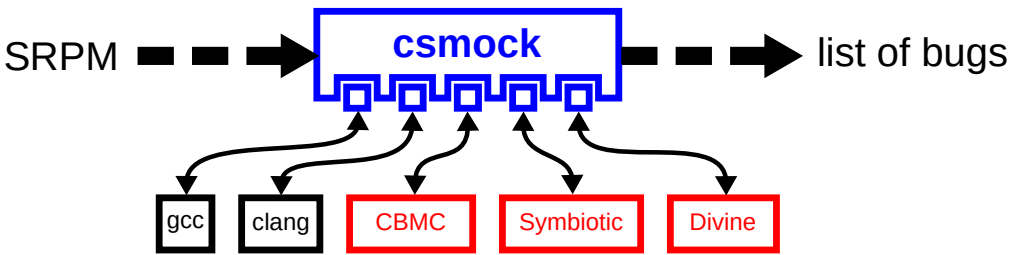
Static Analysis of RPM Packages

- Command-line tool to run static analyzers on RPM packages.
- One interface, one output format, plug-in API for static analyzers.
- Could we integrate formal verification tools?



Formal Verification of RPM Packages

```
$ sudo yum install csmock-plugin-symbiotic
$ csmock -r fedora-34-x86_64 -t symbiotic ${pkg}.src.rpm
```



Results

- Dynamic linker wrapper (csexec) presented at DevConf 2021:
  https://kdudka.fedorapeople.org/kdudka-devconf-21.pdf
- aufover-benchmark (covered by CI) is now publicly available:
  https://github.com/aufover/aufover-benchmark
- Two students decided to work on Symbiotic in their diploma thesis:
  - Lukáš Zaoral – Tune Symbiotic on real-world programs
  - Vincent Mihalkovič – Extend the support of parallel programs in Symbiotic