Formal Verification of RPM Packages

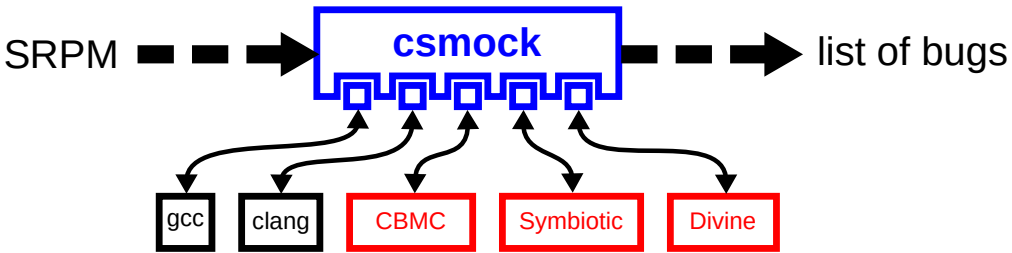
Kamil Dudka <kdudka@redhat.com>

September 15th 2021

Dynamic Linker Wrapper (csexec)

- dynamic analysis of unmodified source RPM packages
- presented at DevConf 2021:
  - slides: https://kdudka.fedorapeople.org/kdudka-devconf-21.pdf
  - video: https://www.youtube.com/watch?v=FjV84hbD1GY
  - demo: https://github.com/csutils/cswrap/wiki/csexec
- now used by csmock plug-ins for CBMC, Divine, and Symbiotic

Formal Verification of RPM Packages




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

Experiments and Progress

- Unable to complete formal verification for most RPM packages.
- Timeouts help to get partial results in a predictable amount of time.
- Making the output format easier to understand by developers:
  - name of binaries being executed
  - command-line arguments passed to the binaries
  - absolute paths to files containing the source code
- aufover-benchmark (covered by CI) is now publicly available:
  `https://github.com/aufover/aufover-benchmark`
- aufover namespace in Fedora COPR:
  `https://copr.fedorainfracloud.org/groups/g/aufover/coprs/`