# Experiments with Symbiotic and Divine at Red Hat

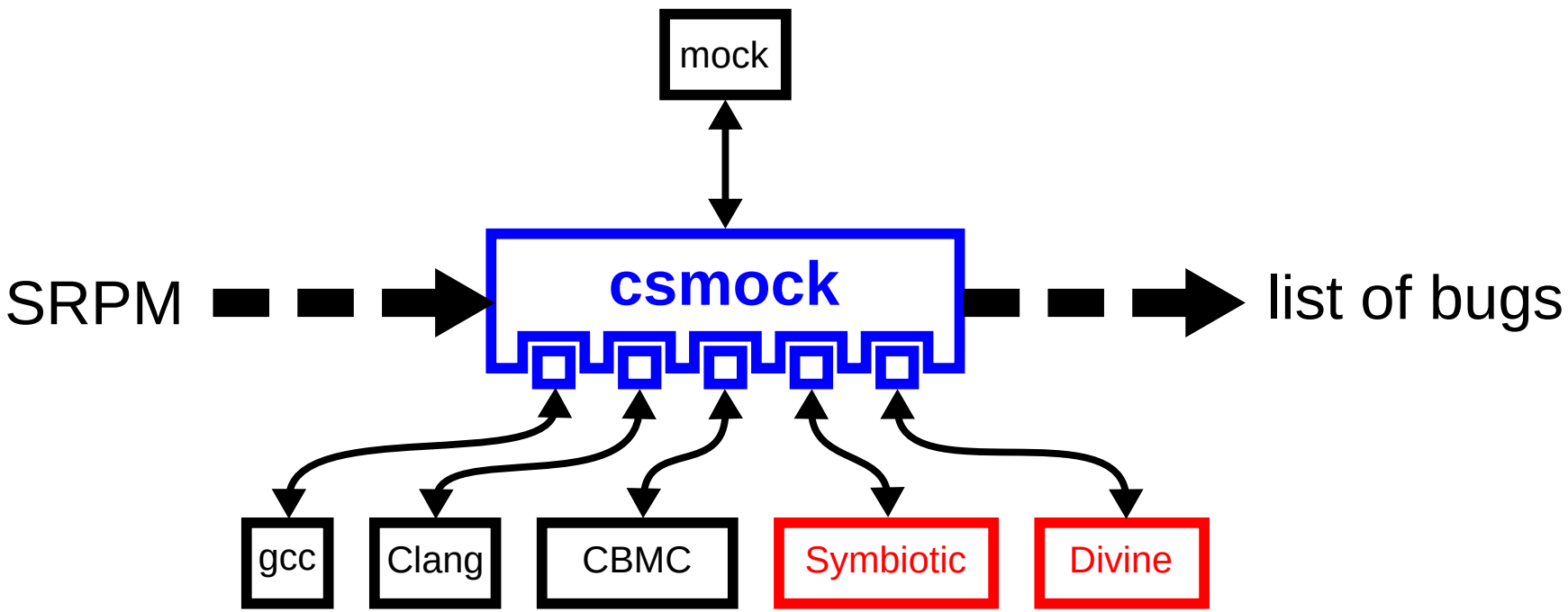
Kamil Dudka <kdudka@redhat.com>

November 26th 2019

Red Hat

# csmock

- command-line tool to run (not only) static analyzers
- one interface, one output format, plug-in API
- fully open-source, available in Fedora/CentOS



Red Hat

# Example: test-0002.c

```
 1  #include <stdlib.h>
 2
 3  extern int __VERIFIER_nondet_int(void);
 4
 5  int main() {
 6      void **undef;
 7      void **null_value = NULL;
 8
 9      if (__VERIFIER_nondet_int())
10          null_value = *undef;
11
12      void **err = *null_value;
13
14      return 0;
15  }
```

# Output format – Symbiotic

```
6.1.0-dev-llvm-unknown-symbiotic:6.1.0-de
INFO: Starting instrumentation
INFO: Instrumentation time: 0.005555868148803711
INFO: Optimizations time: 0.02058720588684082
INFO: Starting slicing
INFO: Total slicing time: 0.004923105239868164
INFO: Optimizations time: 0.019819974899291992
INFO: After-slicing optimizations and transformations time: 1.811981201171875e-05

 --- Error trace ---

Error: memory error: out of bound pointer
File: ./test-0002.c
Line: 12
assembly.ll line: 47
Stack:
#000000047 in main () at ./test-0002.c:12
Info:
address: 0:0
pointing to: none
```

Red Hat

# Output format – Divine

```
states per second: 250
state count: 2
mips: 0.9

error found: yes
error trace: |
  FAULT: null pointer dereference: [global* 0 0 ddn]
  [0] FATAL: memory error in userspace

active stack:
  - symbol: void __dios::FaultBase::handler<__dios::Context>(_VM_Fault, _VM_Frame*, void (*)())
    location: /opt/divine/include/dios/sys/fault.hpp:118
  - symbol: main
    location: test-0002.c:12
  - symbol: __dios_start
    location: /opt/divine/include/dios/libc/sys/start.cpp:89
```

# Output format – csmock

```
Error: CLANG_WARNING: [#def1]
./test-0002.c:10:22: warning: Dereference of undefined pointer value
./test-0002.c:9:9: note: Assuming the condition is true
./test-0002.c:9:5: note: Taking true branch
./test-0002.c:10:22: note: Dereference of undefined pointer value

Error: CLANG_WARNING: [#def2]
./test-0002.c:12:12: warning: Value stored to 'err' during its initialization is never read
./test-0002.c:12:12: note: Value stored to 'err' during its initialization is never read

Error: CLANG_WARNING: [#def3]
./test-0002.c:12:18: warning: Dereference of null pointer (loaded from variable 'null_value')
./test-0002.c:7:5: note: 'null_value' initialized to a null pointer value
./test-0002.c:9:9: note: Assuming the condition is false
./test-0002.c:9:5: note: Taking false branch
./test-0002.c:12:18: note: Dereference of null pointer (loaded from variable 'null_value')
```

# Output format – csmock/Divine [WIP]

```
Error: COMPILER_WARNING: [#def1]
./test-0002.c: scope_hint: In funtion ‘main’
./test-0002.c:12: error: DIVINE FAULT: null pointer dereference: [global* 0 0 ddn]
./test-0002.c:12: note: [0] FATAL: memory error in userspace
./test-0002.c:12: note: backtrace:
/opt/divine/include/dios/sys/fault.hpp:118: note: void
__dios::FaultBase::handler<__dios::Context>(_VM_Fault, _VM_Frame*, void (*)())
./test-0002.c:12: note: main
/opt/divine/include/dios/libc/sys/start.cpp:89: note: __dios_start
```

# Status update (1/2)

- Symbiotic and Divine are now available as RPM packages:
  https://copr.fedorainfracloud.org/coprs/acalabek/symbiotic/
  https://copr.fedorainfracloud.org/coprs/lzaoral/Divine/
- Symbiotic uses the system LLVM stack (works on Fedora 30).
- Divine still uses its own builds of almost everything.

# Status update (2/2)

- Started to experiment with CBMC for independent comparison.
- Developing output converters for Divine, Symbiotic and CBMC.
- Filed 6 tickets for Symbiotic and 29 tickets for Divine (some of them with patches).
- 10 Divine tickets without any reply yet.