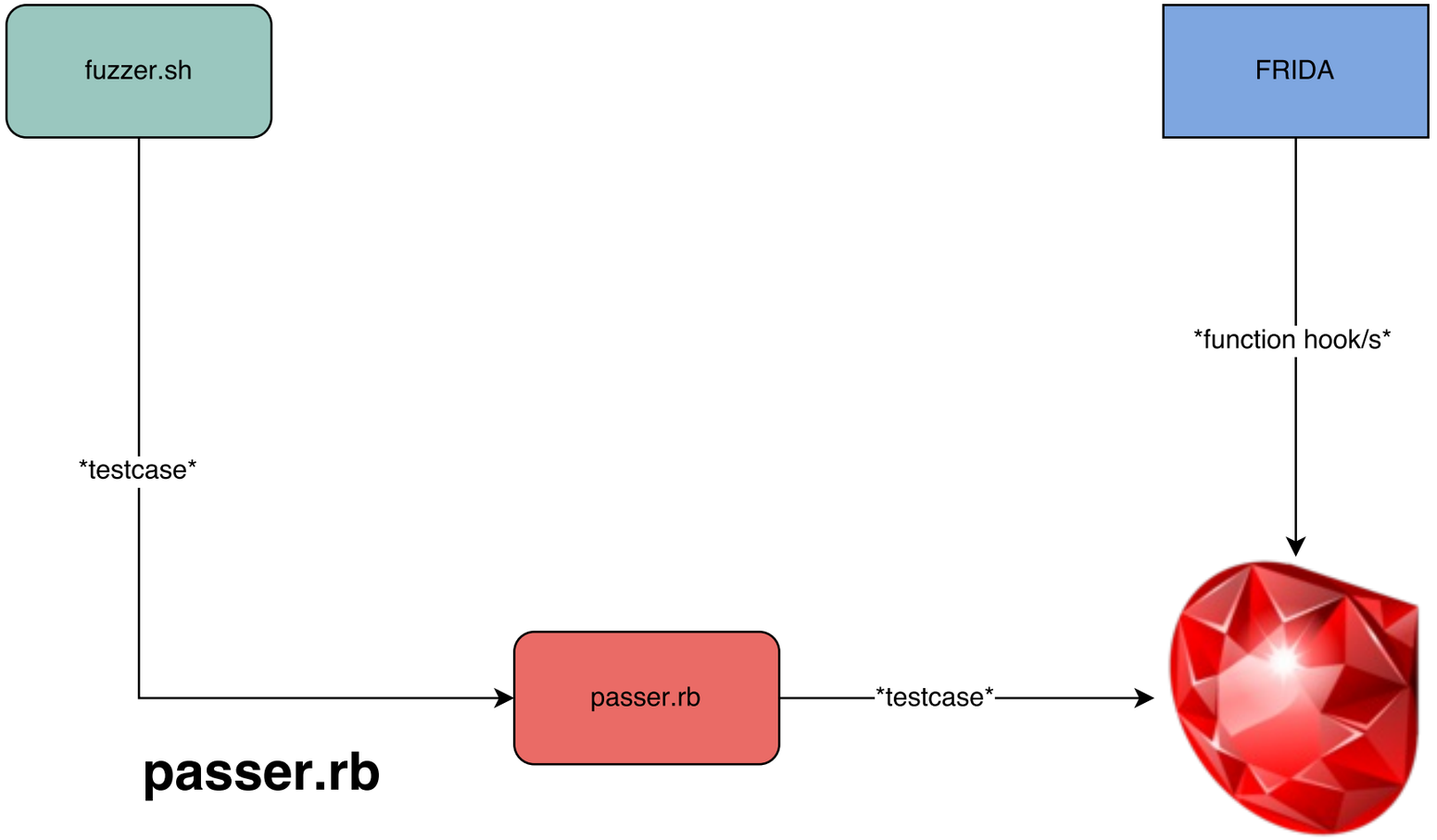
fuzzer.sh

- Wraps radamsa and generates testcases to be fed to passer.rb
- Watches exceptions thrown by passer.rb
- Anything that passes (does not throw exception) / throws something we deem to be 'interesting' , gets stored for future mutation.



FRIDA

- Hooks the target function we identified in the Ruby sourcecode.
- Using FRIDA in conjunction with our *testcase* allows us to see what coverage we get and how deep we go into the ruby flow.

passer.rb

- takes *testcase* via stdin
- throws *testcase* @ the target function we are aiming to snap.
- throws exception or passes based on result of the throw.

RUBY

- Compiled with ASAN from LLVM
- Takes our testcase and hopefully snaps :)
- Hackerone provides us with many coins.