Queso > Salsa

concolic execution

Concolic Execution

- Run code under instrumentation
- Taint trace during instrumentation to reduce trace to those instructions which affect input
- Convert to an IL
- Concretize the trace
- Convert to SMT
- Solve for new inputs

Queso

- Static binary analysis framework.
- Been working on this off-and-on for a few months.
- Does all sorts of cool stuff.
- Stole BAP’s taint tracer (ain’t no one got time for that).
- Decided to switch paths and pursue concolic execution a month ago.

Demo

```
user@debian:~/code/queso/test/test7$ time lua test.lua 2>/dev/null | grep nextInput
nextInput       89 89 00 89 89 89 89 89 89 89 89 89 89 89 89 89 89 89 89 89 89 89 89 89 89 89 89 89 89
nextInput       89 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
nextInput       89 50 4e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
nextInput       89 50 4e 47 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

real    0m14.874s
user    0m0.256s
sys     0m0.280s
user@debian:~/code/queso/test/test7$ echo $'\x89\x50\x4e\x47'
PNG
user@debian:~/code/queso/test/test7$
```

A picture in case this doesn’t work live

The End

Did my time go over?