ISA 563: Fundamentals of Systems Programming

Valgrind

Mar. 26, 2012

What is Valgrind?

- Valgrind is a:
  - memory debugger
  - profiler
  - a tool that you can use to make other tools
- Author(s):
  - Julian Seward et al
- License:
  - GPL v2

Valgrind Features

- Works directly with executable:
  - No need to recompile, or modify the program in other manner
  - Although not required, helpful to re-compile with “-g” switch
- Provides useful tools:
  - memcheck – detects memory errors
  - cachegrind – cache profiler
  - callgrind – call-graph generator
  - ...

How Valgrind Handles Binaries?

- Runs programs using a “synthetic” CPU
- Simulates every single instruction
  - Brings big overhead – 10~100 times slower than native executables
- Detects errors in system libraries

Limitations

- Significant slow down in execution speed
- Larger memory consumption
  - Administrative book keeping
  - Larger translated code
- No robust signal simulation

Detecting Memory Errors

- Use of un-initialized values
  - Un-initialized values will be reported only if they change the behavior of the program

Demo: uninit.c

Memory Leaks

- Valgrind keeps track of all free(), malloc(), realloc() to report any memory leaks that the program may have.

Demo: stack4.c

Invalid Memory Read/Write

Demo: overstep.c

cachegrind and callgrind

- Gives cache hit/miss ratio
- Provides calling graphs
- Useful with visualization tools such as kcachegrind.
- Supports shared library calls.