What's new in the LLVM Ecosystem, and how does that affect the kernel?

Marshall Clow
Qualcomm Technologies, Inc.
mclow@qti.qualcomm.com
Twitter: @mclow

What is LLVM?

- Used to stand for “Low Level Virtual Machine”
  - Now it’s just a name
- A set of libraries and tools for manipulating source and object code

Sanitizers

- Find a particular kind of bug
- Instrumentation in the compiler
- Custom runtime
- Goals: 0 false positives, exact reporting

Existing Sanitizers

- Address Sanitizer (ASAN)
- Undefined Behavior Sanitizer (UBSAN)
- Memory Sanitizer (MSAN)
- Thread Sanitizer (TSAN)

Address Sanitizer and the Kernel

- https://code.google.com/p/address-sanitizer/wiki/AddressSanitizerForKernel
- found use-after-free, out-of-bounds read/write, stack-overflow bugs.

clang-tidy

- An extensible tool to find/fix bugs
- Based on AST matching
- Currently ships with 110 checkers
- Can include static-analyzer tests
- http://clang.llvm.org/extra/clang-tidy.html
  - http://clang-analyzer.llvm.org/available_checks.html#unix_checkers

clang-tidy checkers

- swapped-arguments
  - void f(int, float); f(1.f, 2); // compiles, but is probably wrong.
- memset(foo, sizeof(foo), 0); // size == 0?
- long *p = malloc(sizeof(short)); // really?

other uses

- There’s a checker for cyclomatic complexity - find complicated functions
- Checkers can suggest fixes, and may (if the user wants) rewrite the source code (-fix option)
- The LLVM project wrote a checker that checked the names of the header guards, and then ran it against LLVM and updated 100s of header files.

Refactoring framework

- There's a full set of facilities for writing refactoring tools in LLVM
  - Many of these are used by clang-tidy, but can be used in other tools
- Great talk at CppCon this year by Hyrum Wright
  - https://www.youtube.com/watch?v=ZpvvmvlTOrk

clang-format

- source code formatting tool
  - style is data-driven
  - built in styles are: LLVM, Google, Chromium, Mozilla, WebKit
- used by refactoring framework to make refactoring changes match.
- Can be used as stand-alone tool as well