ISA 563: Fundamentals of Systems Programming

Debugging
(with GDB)

Mar. 19, 2012

Note

Debugging tools help *the programmer* to debug the code. They do not debug the code themsleves.

Static Checking

- Static checking is done by analyzing the program source code common security vulnerabilities and programming mistakes.

- Common tools for C:

    - lint family of tools

Debugging (GCC/GDB)

- Compiling with debugging support:

  - gcc **-g** -o prog prog.c

- For multiple files:

  - Each file must be compiled with -g option

  - The flag must also be set when linking

Running GDB

- Starting a program under gdb:

    - $ gdb prog

- Running the program with arguments

    - (gdb) run arg1 arg2 ...

Stepping through Code

- First, stop your program somehow (Ctrl-C, breakpoints, etc)

- Then use next or step:

  - next: go to next line

    - if a function is reached, go over it

  - step: step through execution

    - if a function is reached, go into it

Operations on Variables

- Examining:
  - (gdb) print xyz
- Modifying:
  - (gdb) set xyz = abc

    or

  - (gdb) set var xyz = abc
    - This avoid ambiguity

Operations on Functions

- Calling a function:
    - (gdb) call function()

- Returning from function:
    - (gdb) finish
        - Complete execution of current function and return to caller

Stacks

- (gdb) backtrace
- (gdb) frame n
- (gdb) frame info

Breakpoints

- Setting a breakpoint at a line:
    - (gdb) break 9
    - (gdb) break main.c:9
- Setting a breakpoint at a function:
    - (gdb) break func1
- Getting information:
    - (gdb) info breakpoints

Breakpoints (cont'd)

- Temporary breakpoints:

  - tbreak – only stops the program once

- Removing a breakpoint:

  - disable <breakpoint-number>

    - breakpoint number as returned by info breakpoints

- Skipping a breakpoint

  - ignore <breakpoint-number> <number-of-times>

Watchpoints

- Setting a watchpoint:
    - (gdb) watch x
        - Report all changes made to variable x
- Setting a read watchpoint:
    - (gdb) rwatch x
        - Report all read access to variable x
- Setting a read/write watchpoint:
    - (gdb) awatch x

Watchpoints (cont'd)

- Getting information:
  - info breakpoints
    - lists both breakpoints and watchpoints
- Disabling watchpoints:
  - disable <watchpoint-number>
    - Enter <watchpoint-number> as printed by "info breakpoints"