Systems Dev. Tutorial IV:

Debugging: Tips and Tools

15-441 Recitation
Wednesday, Sept 27th, 2006

Overview

- What is debugging?
- Strategies to live (or at least code) by.
- Tools of the trade
  - gdb
  - smart logging
  - electric fence
  - ethereal/tcpdump

What is debugging?

You tell me! Everybody writes codes with bugs.

What debugging have you needed to do already on the IRC project?

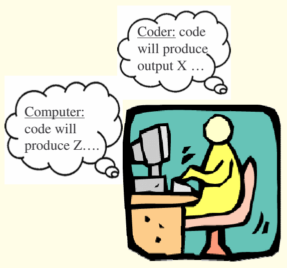
Things to think about:
- What caused the bug?
- How did you end up finding it?
- How could you have avoided the bug in the first-place?

Debugging Philosophy

Guiding Steps:

1) Think about why you believe the program should produce the output you expected.

2) Make assertions until you understand how your view differs from the computer's.


Coder: code will produce output X …
Computer: code will produce Z….

Requirements for Debugging

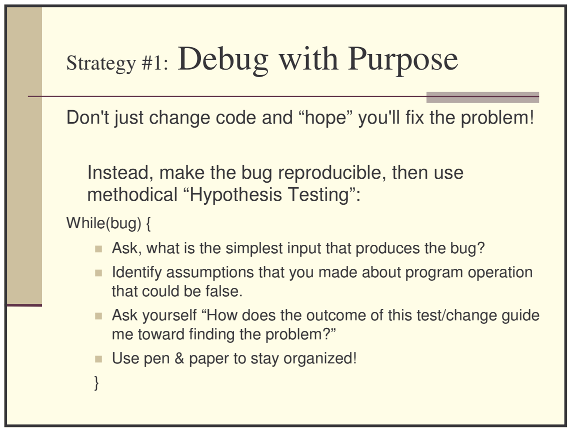
- WHAT program behavior to look for?
  - Sometimes this is nearly free.... (e.g., compiler error, or segfault)
  - Sometimes it is the hardest part.... (e.g., logic bugs, race conditions)
- How to easily expose information to test hypothesis?
  - gdb, logging, strace, ethereal....

Strategies to Live By...

Debugging is part art, part science.

You'll improve with experience….

… but we can try to give you a jump-start!



Strategy #1: Debug with Purpose

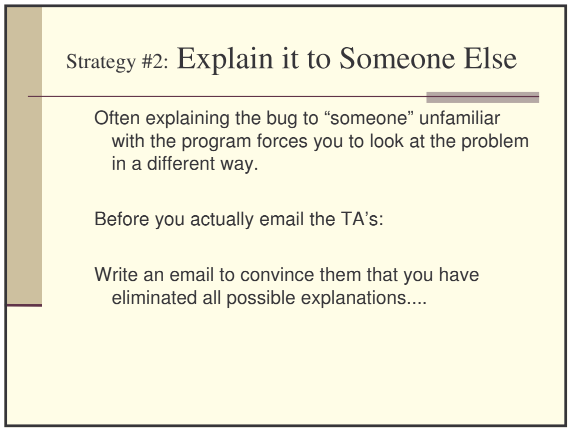
Don't just change code and “hope” you'll fix the problem!

Instead, make the bug reproducible, then use methodical “Hypothesis Testing”:

While(bug) {

- Ask, what is the simplest input that produces the bug?
- Identify assumptions that you made about program operation that could be false.
- Ask yourself “How does the outcome of this test/change guide me toward finding the problem?”
- Use pen & paper to stay organized!

}

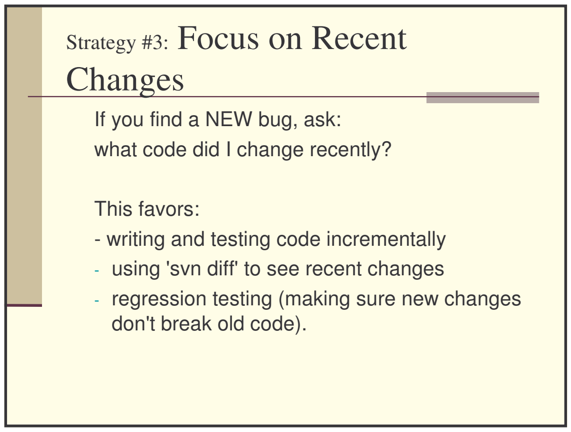


Strategy #2: Explain it to Someone Else

Often explaining the bug to “someone” unfamiliar with the program forces you to look at the problem in a different way.

Before you actually email the TA’s:

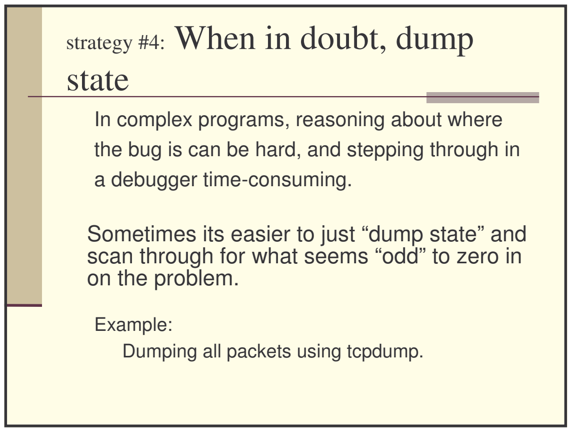
Write an email to convince them that you have eliminated all possible explanations....



Strategy #3: Focus on Recent Changes

If you find a NEW bug, ask:
what code did I change recently?

This favors:
- writing and testing code incrementally
- using 'svn diff' to see recent changes
- regression testing (making sure new changes don't break old code).

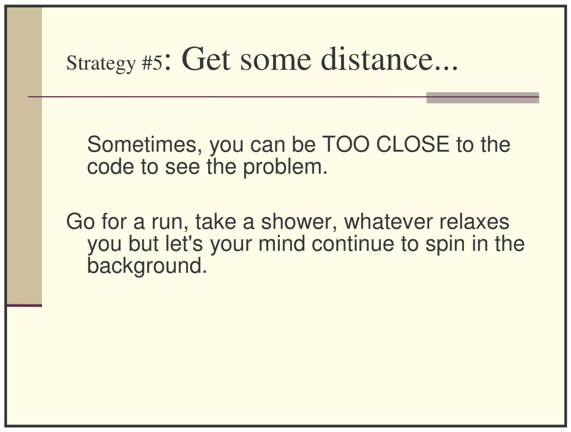


strategy #4: When in doubt, dump state

In complex programs, reasoning about where the bug is can be hard, and stepping through in a debugger time-consuming.

Sometimes its easier to just “dump state” and scan through for what seems “odd” to zero in on the problem.

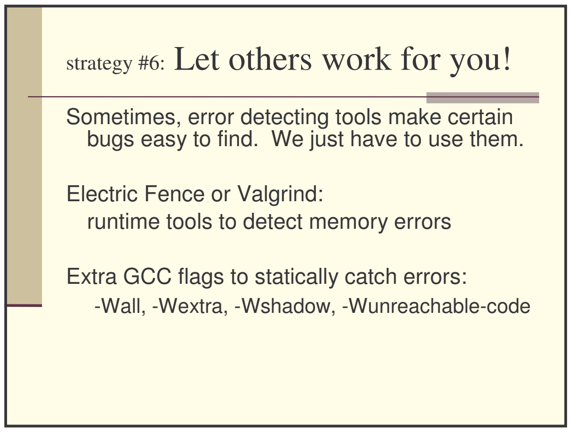
Example:
Dumping all packets using tcpdump.



Strategy #5: Get some distance...

Sometimes, you can be TOO CLOSE to the code to see the problem.

Go for a run, take a shower, whatever relaxes you but let's your mind continue to spin in the background.



strategy #6: Let others work for you!

Sometimes, error detecting tools make certain bugs easy to find. We just have to use them.

Electric Fence or Valgrind:
runtime tools to detect memory errors

Extra GCC flags to statically catch errors:
-Wall, -Wextra, -Wshadow, -Wunreachable-code

Strategy #7: Think Ahead

Bugs often represent your misunderstanding of a software interface.

Once you've fixed a bug:
1) Smile and do a little victory dance....
2) Think about if the bug you fixed might manifest itself elsewhere in your code (a quick grep can help).
3) Think about how to avoid this bug in the future (maybe coding 36 straight hours before the deadline isn't the most efficient approach....)

Tools of the Trade

Different bugs require different tools:

1) Program crashes with segfault
   -> gdb

2) Hard to reproduce or highly complex bugs
   -> logging & analysis

3) Program hangs waiting for network traffic
   -> tcpdump / ethereal

GDB: Learn to Love it

Run a program, see where it crashes, or stop it in the middle of running to examine program state.

Two ways to run:
- gdb *binary* (to run binary inside of gdb)
- gdb *binary core-file* (to debug crashed program)

GDB Commands

Controlling Execution	Getting Info
■ run <cmd-line args>	■ backtrace
■ break <func>	■ print <expr>
■ step	■ info locals
■ next	■ list
■ control-c	■ up/down

GDB Tricks & Tips

- See handout for detailed explanations, and abbreviations
- Remember: always compile with -g, and no optimizations.
- If your not getting core files, type: 'unlimit coredumpsize'
- You can use GDB in emacs! (see slides at end)

Smart Logging

- Use a debug macro that you can easily turn off to suppress output just by changing one line. (example posted online)
- Often smart to create generic log functions like dumpIRCMessage() or dumpRoutingPacket()
- A tool like 'strace' or 'ktrace' may be able to log easily read information for free!

Electric Fence

Adds run-time checks to your program to find errors related to malloc.

e.g.: writing out of bounds, use after free...

just compile your programs using -lefence

Alternative: Valgrind finds more memory errors, but is VERY slow.

tcpdump & ethereal

Helps you understand what is happening “below” your networking code.

- Benefits
  - Often will automatically parse well known protocols for you! (like, say... IRC)
  - Accept filters to ignore unimportant packets
- Downsides
  - Need root access

That’s It!

Questions?

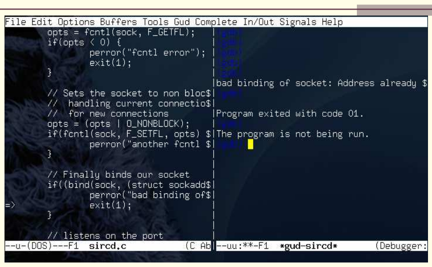
Feedback from Checkpoint 2?

Using GDB in Emacs

The commands/keystrokes to make it happen:

1. Compile with -g and *NO* -O2 or -O3
2. build with a "make"
3. emacs sircd.c (or any other source file)
4. CTRL+x and then '3' (open a right frame)
5. CTRL+x and then 'o' (switch cursor to right frame)
6. ESC+x and then "gdb" and hit enter
7. Type in the name of your binary *only*, like "sircd" and hit enter
8. Set any break points you want, then type "run params ...", for example "run 1 node1.conf" and hit enter
9. Use GDB with your code!! (next, step, print, display...)

GDB in Emacs



```
File Edit Options Buffers Tools Gud Complete In/Out Signals Help
        opts = fcntl(sock, F_GETFL);    |(gdb)
        if(opts < 0) {                  |(gdb)
                perror("fcntl error");  |(gdb)
                exit(1);                |(gdb)
        }                               |(gdb)
                                        |bad binding of socket: Address already $
        // Sets the socket to non bloc$|(gdb)
        //  handling current connectio$|
        //  for new connections         |Program exited with code 01.
        opts = (opts | O_NONBLOCK);     |(gdb)
        if(fcntl(sock, F_SETFL, opts) $|The program is not being run.
                perror("another fcntl $|(gdb)
        }                               |
                                        |
        // Finally binds our socket     |
        if((bind(sock, (struct sockadd$|
                perror("bad binding of$|
=>              exit(1);                |
        }                               |
                                        |
        // listens on the port          |
--u-(DOS)---F1  sircd.c           (C Ab|--uu:**-F1  *gud-sircd*        (Debugger:
```

Note the arrow in the left source file window shows the line being executed!