RUTGERS

THE STATE UNIVERSITY
OF NEW JERSEY

Computer Architecture (CS-211)
Recitation 5

Song Wen

Topics

- GDB
- PA3 (Bomb Lab)

* Some materials are collected and compiled from previous year's CS 211 lectures and TAs

GDB: GNU Debugger

- Find bugs in a program
  - Print out variables' values
  - Check the logic of the program
  - Debug using gdb

- GDB: can trace the program execution
  - Step through the program one line at a time
  - Monitor / modify internal variables

- How to use GDB to debug
  - Need to compile your source code with -g
    - gcc -g simple.c -o simple
  - Use gdb after compiling: gdb [your exe]

A GDB tutorial: https://www.youtube.com/watch?v=sCtY--xRUyI

Some GDB commands

- Start debugging the program in gdb
  - `(gdb) run` or `r`
- End debugging
  - `(gdb) quit` or `q`
- Set a breakpoint
  - `(gdb) break [func name]` or `b [func name]`
  - `(gdb) break [line number]` or `b [line number]`
- Execute next line of code
  - `(gdb) next` or `n`
- Print the value of a variable
  - `(gdb) print [var name]` or `p [var name]`
- List code around current line
  - `(gdb) list` or `l`

Some GDB commands

- Display a variable's value each time gdb stops
  - `(gdb) display [var name]`
- Continue execution until next breakpoint
  - `(gdb) continue` or `c`
- Set a temp value to a variable
  - `(gdb) print [var name]=[value]` or `p [var name]=[value]`
- Show all breakpoints
  - `(gdb) info breakpoint` or `info b`
- Clear a breakpoint
  - `(gdb) clear [func name]`
  - `(gdb) clear [line number]`
  - `(gdb) delete breakpoint [# of breakpoint]`
- Clear all breakpoints
  - `(gdb) delete`

Using GDB without source code

- Not compiled with -g
  - You cannot see the source code in gdb
  - E.g: PA3-bomblab
- Disassemble the binary (binary to assembly code)
  - `objdump -d simple`
- Use GDB to debug assembly code
  - Start GDB: gdb [exec]
    - gdb simple

GDB commands to debug assembly code

- `run` and `quit` are the same
- Set a breakpoint
  - `(gdb) break [func name]` or `b [func name]`
  - `(gdb) break *[address]` or `b *[address]`
- Execute next instruction of assembly code
  - `(gdb) nexti` or `ni`
- Clear a breakpoint
  - `(gdb) clear [func name]`
  - `(gdb) clear *[address]`
  - `(gdb) delete breakpoint [# of breakpoint]`
- Clear all breakpoints
  - `(gdb) delete`

GDB commands to debug assembly code

- Print value of a register in a given format
  - `(gdb) print/[format] [expression]`
    - Useful formats (default is decimal)
      - d: decimal
      - x: hex
      - t: binary
      - i: instruction
      - c: character
    - Expression can be program variables or registers,
    - A register is represented as $eax instead of %eax
    - E.g. p/x $eax (print the value in register eax in hex)
  - `(gdb) info r [register name]`
    - `info r eax` or `i r eax`
    - will print all registers' contents without register name

GDB commands to debug assembly code

- Print value of a specified memory address
  - `(gdb) x/[count][format] [address]`
  - `format` is the same as for `print`
  - Address can be symbolic (e.g. main) or numeric (e.g. 0x804848a) or register name (e.g. $eax)

- Step into and out of a function
  - Step in: `(gdb) step i` or `si`
  - Step out: `(gdb) step`

PA3 - Bomblab

- Find the solutions by debugging using GDB
  - `gdb bomb` (run in gdb)
  - Set break point for each phase (e.g. `(gdb) b phase_1`)
    - When running, it will step into the function of each phase
    - Guess the input according to the instructions in each phase function
- Generate the assembly code from binary
  - Disassemble the code ($ objdump -d bomb)
- Other useful informaiton
  - Print bomb's symbol table ($ objdump -t bomb)
  - Display printable strings ($ strings -t x bomb)

How to Defuse It!

```
8048b6f:    e8 c0 09 00 00          call   8049534 <read_line>
8048b74:    89 04 24                mov    %eax,(%esp)
8048b77:    e8 04 01 00 00          call   8048c80 <phase_1>
8048b7c:    e8 ad 0a 00 00          call   804962e <phase_defused>
8048b81:    c7 04 24 40 a4 04 08    movl   $0x804a440,(%esp)
8048b88:    e8 f3 fc ff ff          call   8048880 <puts@plt>
8048b8d:    e8 a2 09 00 00          call   8049534 <read_line>
8048b92:    89 04 24                mov    %eax,(%esp)
8048b95:    e8 2a 01 00 00          call   8048cc4 <phase_2>
8048b9a:    e8 8f 0a 00 00          call   804962e <phase_defused>
8048b9f:    c7 04 24 81 a3 04 08    movl   $0x804a381,(%esp)
8048ba6:    e8 d5 fc ff ff          call   8048880 <puts@plt>
8048bab:    e8 84 09 00 00          call   8049534 <read_line>
8048bb0:    89 04 24                mov    %eax,(%esp)
8048bb3:    e8 30 01 00 00          call   8048ce8 <phase_3>
8048bb8:    e8 71 0a 00 00          call   804962e <phase_defused>
8048bbd:    c7 04 24 9f a3 04 08    movl   $0x804a39f,(%esp)
8048bc4:    e8 b7 fc ff ff          call   8048880 <puts@plt>
8048bc9:    e8 66 09 00 00          call   8049534 <read_line>
8048bce:    89 04 24                mov    %eax,(%esp)
8048bd1:    e8 9c 01 00 00          call   8048d72 <phase_4>
8048bd6:    e8 53 0a 00 00          call   804962e <phase_defused>
8048bdb:    c7 04 24 6c a4 04 08    movl   $0x804a46c,(%esp)
8048be2:    e8 99 fc ff ff          call   8048880 <puts@plt>
8048be7:    e8 48 09 00 00          call   8049534 <read_line>
8048bec:    89 04 24                mov    %eax,(%esp)
8048bef:    e8 d6 01 00 00          call   8048dca <phase_5>
8048bf4:    e8 35 0a 00 00          call   804962e <phase_defused>
8048bf9:    c7 04 24 b0 a3 04 08    movl   $0x804a3b0,(%esp)
8048c00:    e8 7b fc ff ff          call   8048880 <puts@plt>
8048c05:    e8 2a 09 00 00          call   8049534 <read_line>
8048c0a:    89 04 24                mov    %eax,(%esp)
```

PA3 – Generate the assembly code

```
-bash-4.1$ ls
bomb  bomb.c  bomb.s  defuser.txt  README
-bash-4.1$ objdump -d bomb > bomb.s
-bash-4.1$
```

Address and name of function

```
8048aa2:   e8 af 06 00 00          call   8049156 <initialize_bomb>
8048aa7:   c7 04 24 64 a2 04 08    movl   $0x804a264,(%esp)
8048aae:   e8 5d fd ff ff          call   8048810 <puts@plt>
8048ab3:   c7 04 24 a0 a2 04 08    movl   $0x804a2a0,(%esp)
8048aba:   e8 51 fd ff ff          call   8048810 <puts@plt>
8048abf:   e8 50 09 00 00          call   8049414 <read_line>
8048ac4:   89 04 24                mov    %eax,(%esp)
8048ac7:   e8 04 01 00 00          call   8048bd0 <phase_1>
8048acc:   e8 77 0a 00 00          call   8049548 <phase_defused>
8048ad1:   c7 04 24 cc a2 04 08    movl   $0x804a2cc,(%esp)
8048ad8:   e8 33 fd ff ff          call   8048810 <puts@plt>
8048add:   e8 32 09 00 00          call   8049414 <read_line>
8048ae2:   89 04 24                mov    %eax,(%esp)
8048ae5:   e8 2a 01 00 00          call   8048c14 <phase_2>
8048aea:   e8 59 0a 00 00          call   8049548 <phase_defused>
8048aef:   c7 04 24 0d a2 04 08    movl   $0x804a20d,(%esp)
```

Phase_1

PA3 – A glance at phase_1

```
08048bd0 <phase_1>:
 8048bd0:   83 ec 2c                sub    $0x2c,%esp
 8048bd3:   c7 44 24 1c 00 00 00    movl   $0x0,0x1c(%esp)
 8048bda:   00
 8048bdb:   8d 44 24 1c             lea    0x1c(%esp),%eax
 8048bdf:   89 44 24 08             mov    %eax,0x8(%esp)
 8048be3:   c7 44 24 04 b4 a5 04    movl   $0x804a5b4,0x4(%esp)
 8048bea:   08
 8048beb:   8b 44 24 30             mov    0x30(%esp),%eax
 8048bef:   89 04 24                mov    %eax,(%esp)
 8048bf2:   e8 89 fc ff ff          call   8048880 <__isoc99_sscanf@plt>
 8048bf7:   83 f8 01                cmp    $0x1,%eax
 8048bfa:   74 05                   je     8048c01 <phase_1+0x31>
 8048bfc:   e8 84 07 00 00          call   8049385 <explode_bomb>
 8048c01:   81 7c 24 1c 5c 02 00    cmpl   $0x25c,0x1c(%esp)
 8048c08:   00
 8048c09:   74 05                   je     8048c10 <phase_1+0x40>
 8048c0b:   e8 75 07 00 00          call   8049385 <explode_bomb>
 8048c10:   83 c4 2c                add    $0x2c,%esp
 8048c13:   c3                      ret
```

Be careful !!

- Execute the instruction line by line using `ni`
- Find out what it does before call the function *explode_bomb*
- Quit from gdb if it's going to execute *call xxx <explode_bomb>*

More GDB Commands

$ gcc –m32 hello.c –g –o hello
$ gdb hello
(gdb) run
(gdb) c - continue
(gdb) layout asm – gui for assembly code
(gdb) ni - next instruction
(gdb) si - step in (e.g. step into function)
(gdb) step - step out
(gdb) disas - disassemble instructions
(gdb) until *addr – jump to the given addr
(gdb) i r – print all reg values
(gdb) x/s addr – print value of the addr (similarly x/d)

More Commands DRAFT

see contents of the registers and memory
(gdb) info registers or i r

print out the contents of the ECX register in decimal, hexadecimal, and binary, respectively
print/d $ecx
print/x $ecx
print/t $ecx

The gdb command "info display" will list all the active displays. Use "undisplay" to remove an item on this list.
display $eax
display/i $eip

then the contents of the EAX register will be printed to the screen every time the program is halted.

http://csapp.cs.cmu.edu/2e/docs/gdbnotes-ia32.pdf
https://www.csee.umbc.edu/~cpatel2/links/310/nasm/gdb_help.shtml

PA 3 – Scoreboard

- Remember : You will lose **0.5** points for each explodes!

Bomb Lab Scoreboard

This page contains the latest information that we have received from your bomb. If your solution is marked **invalid**, this means your bomb reported a solution that didn't actually defuse your bomb.

Last updated: Tue Mar 7 12:18:30 2017 (updated every 30 secs)

#	Bomb number	Submission date	Phases defused	Explosions	Score	Status
1	bomb3	Tue Feb 28 19:02	9	0	100	valid
2	bomb19	Sat Mar 4 18:50	9	0	100	valid
3	bomb15	Mon Mar 6 19:28	9	8	96	valid
4	bomb32	Sun Mar 5 06:25	8	8	86	invalid phase 9
5	bomb17	Mon Mar 6 23:07	6	0	60	invalid phase 7
6	bomb20	Tue Mar 7 11:27	7	1	75	invalid phase 8
7	bomb24	Sat Mar 4 20:56	5	0	45	invalid phase 6
8	bomb26	Sun Mar 5 09:23	5	1	45	invalid phase 6
9	bomb6	Thu Mar 2 19:21	5	33	29	invalid phase 6
10	bomb16	Mon Mar 6 20:39	4	4	33	invalid phase 5
11	bomb51	Mon Mar 6 23:51	3	0	25	invalid phase 4
12	bomb31	Sun Mar 5 14:17	3	1	25	invalid phase 4
13	bomb48	Tue Mar 7 00:06	3	1	25	invalid phase 4
14	bomb5	Tue Mar 7 08:00	2	14	8	invalid phase 3
15	bomb28	Sat Mar 4 21:10	1	5	3	invalid phase 2
16	bomb37	Sun Mar 5 14:43	0	1	0	invalid phase 1
17	bomb47	Mon Mar 6 08:47	0	1	0	invalid phase 1
18	bomb41	Sun Mar 5 19:47	0	2	-1	invalid phase 1
19	bomb44	Sun Mar 5 22:57	0	2	-1	invalid phase 1
20	bomb18	Sat Mar 4 15:11	0	3	-1	invalid phase 1
21	bomb30	Mon Mar 6 16:50	0	10	-5	invalid phase 1
22	bomb34	Mon Mar 6 22:11	0	17	-8	invalid phase 1
23	bomb61	Tue Mar 7 11:27	0	10266140	-40	invalid phase 1

Summary [phase:cnt] [1:1] [2:1] [3:3] [4:1] [5:3] [6:1] [7:1] [8:1] [9:3] total defused = 2/23

Usef Commands for Bomblab

- One way to do it by debugging using GDB
  - $ gdb bomb (run in gdb)
  - Set break point for each phase (e.g. (gdb) break phase_1) (this will help you not to explode the bomb)
  - Run the program ((gdb) run)

- Useful Commands for binary bomb
  - Print bomb's symbol table ($ objdump -t bomb)
  - Disassemble the code ($ objdump -d bomb)
  - Display printable strings ($ strings -t x bomb)

- You can save output of commands into file
  - Example : $ objdump -d bomb > bomb-assembly.txt

http://csapp.cs.cmu.edu/2e/docs/gdbnotes-ia32.pdf

Q&A

Thanks!