Discovery Series #10: Understanding x86-64 Control Transfer Instructions

Started: Oct 3 at 5:14pm

Quiz Instructions

Reminding you of the academic honor pledge that you signed.

*****Strongly recommend that your SASM is working before you proceed with the discovery series*****

This discovery series is to analyze branch and stack instructions.

Answer the given questions.

Question 1 5 pts

Given the code snippets below:

1. L1: xor al, al

2. times 128 NOP

3. jc short L1

4. xor rax, rax

5. ret

*note: line 2 means there are 128 NOP instructions between line 1 and line 3

After compilation, line 3 will generate an error "short jump is out of range".

a.) Why is the conditional jump out of range? How far can a backward short jump branch?

b.) What should be the maximum number of NOP instructions between lines 1 and 3 to remove the error?

c.) What type of unconditional jump should be used to solve this problem?

d.) Re-write the code snippet to solve the problem.

Edit View Insert Format Tools Table

12pt Paragraph

the NOP itself), the jump exceeds the maximum allowable range for a short jump, leading to the error.

B. To avoid the "out of range" error, the maximum number of NOPs between lines L1 and the `jc short L1` should be **126**. This allows the jump to be within the allowable range of -128 to +127 bytes.

C. To solve the problem, you can use a **near jump** or an **absolute jump** instead of a short conditional jump. An unconditional jump (`jmp`) does not have the same distance limitations as the short conditional jump.

D. L1:

```
    xor al, al
```

ol ▸ li ▸ p   186 words   </>

Question 2 5 pts

Given the code snippets below:

1. mov ax, 0x1111

2. mov bx, 0x2222

3. mov cx, 0x8888

4. push cx

5. push bx

6. push ax

7. call L1

8. INC AL

9. xor rax, rax

10. ret

11. L1: mov rbp, rsp

12. mov r8w, [rbp+ 8]

13. PRINT_HEX 2, r8w

14. NEWLINE

15. mov r9w, [rbp+ 10]

16. PRINT_HEX 2, r9w

17. NEWLINE

18. mov r10w, [rbp+ 12]

19. PRINT_HEX 2, r10w

20. ret 12

Fill in the correct value to make the code snippet run correctly (output correct and program will not crash)

No new data to save. Last checked at 5:23pm Submit Quiz