Question Set 0x03

HQS Challenge

January 20, 2016

These following questions pertain to a 32-bit system architecture (use the e-prefixed register names not the r-prefixed ones.

1. What register stores the address of the next instruction to be executed?
2. This register is broken down into single-bit pieces representing the Carry Flag, Parity Flag, etc.
3. What three registers are sub-pieces of the register eax and what are their sizes, in bits?
4. This register stores the current address for the stack.
5. This register is similar to the stack pointer but is instead called the base pointer
6. Explain the difference between esp and ebp in the context of a programs execution

These following questions pertain to a 64-bit system architecture (use the r-prefixed register names

1. What is the hierarchy of registers from 64-bit through 8-bits, use rax
2. Given the register `r15b` - what is the register size? What is the name of the full size register?
3. For r15, what are the lower 32 and lower 16 bit equivalent registers called?
4. True or false. In 64 bit architecture, all of the same registers exist but, are sub parts of larger 64-bit registers.

Solutions

1. eip
2. EFLAGS
3. ax (16), ah (8), al(8)

4. esp

5. ebp

6. esp keeps track of the current address. When new space is allocated esp moves. ebp instead keeps track of the function frame, it only changes when a function is called or returned.

1. rax-eax-ax-ah-al

2. 8 bits, r15

3. r15d (32) and r15w (16)

4. True, one area of concern might be with the EFLAGS register. This is renamed RFLAGS but still contains the EFLAGS portion.