Operating Systems.
CS3510

INSTRUCTOR: DR. CHESTER REBERIO

ASSIGNMENT 3

Team QEMU SABE CS13B055 (Sasi Kiran) CS13B051 (Shiva Krishna Reddy)

SOME POINTS NOTED :

- Entry point into the hello was found using the :
  - (e->env_tf).tf_eip = ELFHDR->e_entry ;
  - This corresponds to cmp operation in the user program assembly.
- We find the next breakpoint . i.e calling the int $0x30 which is a system call corresponding to the address 0x800add
  - i.e --------> 0x800add: int $0x30

EXERCISE QUESTIONS :

- **1. What is the purpose of having an individual handler function for each exception/interrupt? (i.e., if all exceptions/interrupts were delivered to the same handler, what feature that exists in the current implementation could not be provided?**
  - Separate handler for each function is small compared to one whole big function, so it can be present at different locations in memory not necessarily contiguous which offers a better memory usage compared to a big handler. This also reduces interrupt latency to some extent.

- **2. Did you have to do anything to make the user/softint program behave correctly? The grade script expects it to produce a general protection fault (trap 13), but softint's code says int $14. *Why* should this produce interrupt vector 13? What happens if the kernel actually allows softint's int $14 instruction to invoke the kernel's page fault handler (which is interrupt vector 14)?**
    - User process has a CPL of 3.Whereas the DPL for handling page fault is 0. Hence it gives a GPF for trying to cause a page fault in user mode.

- **3.The breakpoint test case will either generate a breakpoint exception or a general protection fault depending on how you initialized the breakpoint entry in the IDT (i.e., your call to SETGATE from trap_init). Why? How do you need to set it up in order to get the breakpoint exception to work as specified above and what incorrect setup would cause it to trigger a general protection fault?**
    - It depends on the DPL set for the breakpoint handler.If DPL is 0 we get a GPF , whereas if DPL is 3 we get a breakpoint exception.This is because it is the user process that generates breakpoints.

- **4.What do you think is the point of these mechanisms, particularly in light of what the user/softint test program does?**
    - This mechanism prevents user program from accessing privileged data like kernel data and hence offers protection. In the light of user/softint test program, this mechanism prevents user from loading pages corresponding to sensitive data from disk and gives it access only to those pages loaded by user program.

- **5.What causes the page fault when backtrace is called?**
  - The page fault occurs because the user mappings are not present in kernel page directory and current page directory in cr3 is kernel's.