作業一:核心進入點

中正大學 作業系統實驗室

指導教授: 羅習五





圖片來源

● 新垣結衣

- https://makey.asia/column.php?id=532
- http://pic.haibao.com/image/14284778.html?kw=%E6%96%B0%E5%9 E%A3%E7%BB%93%E8%A1%A3
- https://huaban.com/pins/835412722/

作業目標及負責助教

- 作業目標:
 - ●了解如何用QEMU及gdb+Eclipse對Linux kernel除錯
 - ◎藉由核心進入點,了解探索Linux kernel的技巧
- 負責助教:
 - ●請看網頁

核心進入點

Boot loader +··· start_kernel() 相當於main function 負責初始化Linux kernel 初始化system call進入點 初始化中斷進入點 OS

核心進入點

Boot loader +···

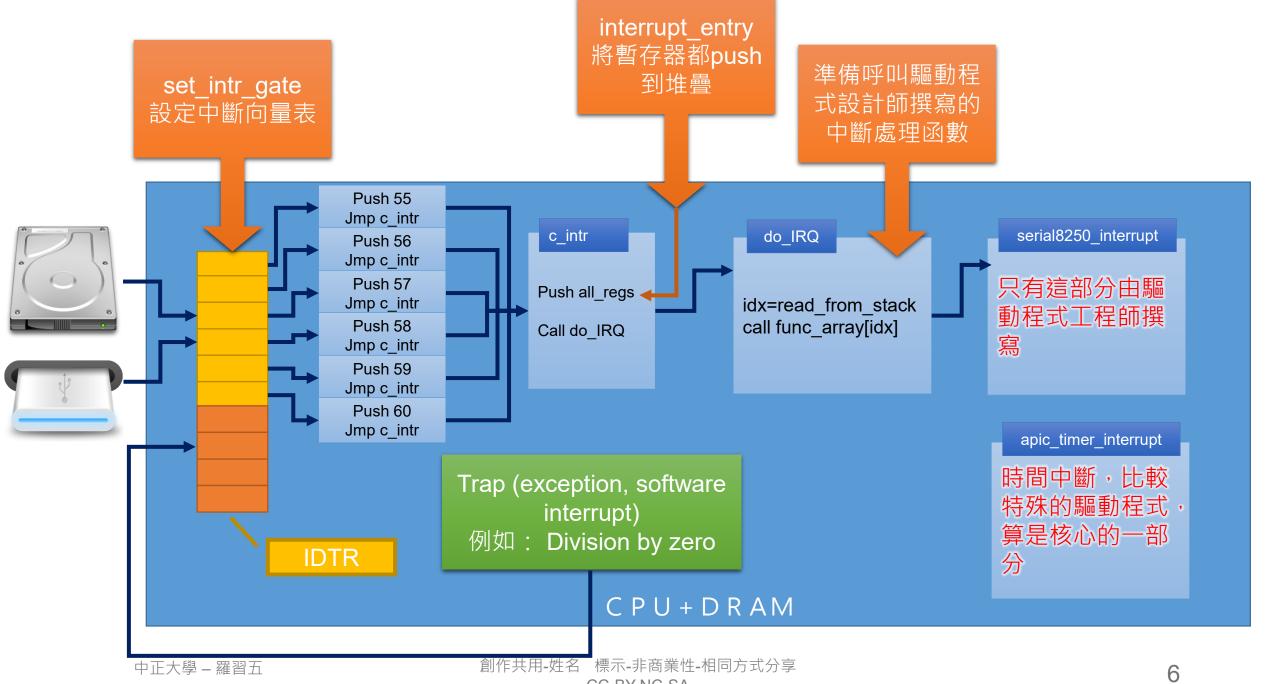
WRMSR — Write to Model Specific Register 通常使用頻率較少或者只適用某些處理器的暫存器,都必 須用WRMSR

start_kernel() 相當於main function 負責初始化Linux kernel 初始化system call進入點 初始化中斷進入點

syscall_init 使用WRMSR將 entry_SYSCALL_64 寫入CPU內部的暫存器 往後只要執行asm("syscall")就會跳到 entry_SYSCALL_64

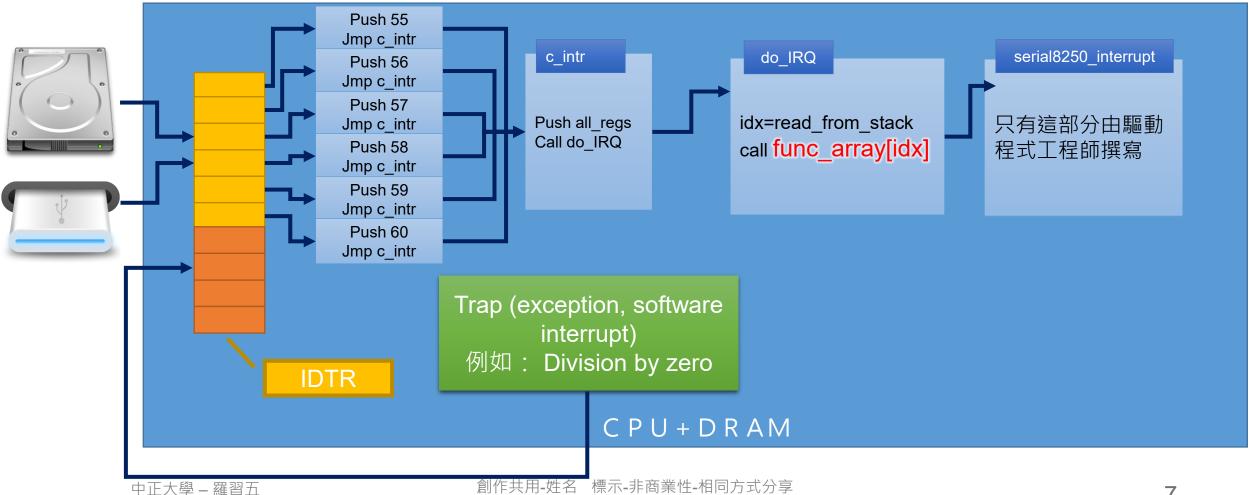
https://www.felixcloutier.com/x86/wrmsr

OS



CC-BY-NC-SA

從OS開發者看「註冊中斷」



CC-BY-NC-SA

關於堆豐

不管是system call、trap、interrupt,在呼响用
 叫第一個○函數時,堆疊一定是長這樣子

```
struct pt_regs {
 * C ABI says these regs are callee-preserved. They aren't saved on kernel entr
 * unless syscall needs a complete, fully filled "struct pt regs".
        unsigned long r15;
        unsigned long r14;
        unsigned long r13;
        unsigned long r12;
        unsigned long rbp;
        unsigned long rbx;
/* These regs are callee-clobbered. Always saved on kernel entry. */
        unsigned long r11;
        unsigned long r10;
        unsigned long r9;
        unsigned long r8;
        unsigned long rax;
        unsigned long rcx;
        unsigned long rdx;
        unsigned long rsi;
        unsigned long rdi;
 * On syscall entry, this is syscall#. On CPU exception, this is error code.
 * On hw interrupt, it's IRO number:
        unsigned long orig rax;
/* Return frame for iretq */
        unsigned long rip;
        unsigned long cs;
        unsigned long eflags;
        unsigned long rsp;
        unsigned long ss;
/* top of stack page */
};
```



作業系統概論^{基於GNU/Linux}

中正大學,資工系,作業系統實驗室,副教授羅習五,shiwulo@gmail.com

附錄



Control Registers

CR0	
CR2	
CR3	
CR4	
CR8	
	CR2 CR3 CR4

System-Flags Register

RFLAGS

Debug Registers

DR0
DR1
DR2
DR3
DR6
DR7

Descriptor-Table Registers

GDTR	
IDTR	
LDTR	

Task Register

TR

Extended-Feature-Enable Register

EFER

System-Configuration Register SYSCFG

System-Linkage Registers

STAR
LSTAR
CSTAR
SFMASK
FS.base
GS.base
KernelGSbase
SYSENTER_CS
SYSENTER_ESP
SYSENTER_EIP

Debug-Extension Registers

DebugCtl
LastBranchFromIP
LastBranchToIP
LastIntFromIP
LastIntToIP

Memory-Typing Registers

MTRRcap
MTRRdefType
MTRRphysBasen
MTRRphysMaskn
MTRRfixn
PAT
TOP_MEM
TOP_MEM2

Performance-Monitoring Registers

TSC	
PerfEvtSeln	
PerfCtrn	

Machine-Check Registers

Model-Specific Registers

System_Registers_Diag.eps

Figure 1-7. System Registers

相同方式分享

Intel的系統暫存器

● 大概介紹86的語法

https://software.intel.com/content/www/us/en/develop/articles/introduction-to-x64-assembly.html?wapkw=

