https://play.google.com/store/apps/details?id=jp.co.namura.magnifier&hl=zh_HK https://www.pngfind.com/mpng/iRhTJTh tux-linux-logo-start-menu-linux-icons-hd/

作業二: 觀察中斷

中正大學 作業系統實驗室

指導教授: 羅習五





圖片來源

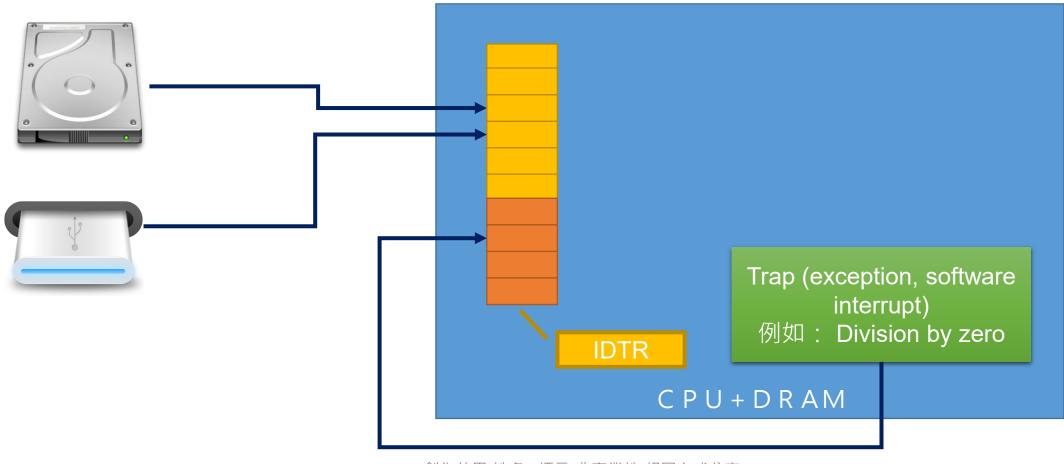
● 新垣結衣

- 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Linux怎樣設定中斷向量表
 - ○了解驅動程式中,關於中斷的部分
 - 了解如何追蹤Linux、 反組譯等技巧
- 負責助教:
 - ●請看網頁

從硬體看x86的中斷



創作共用-姓名 標示-非商業性-相同方式分享 CC-BY-NC-SA

從「軟體」看x86的中斷

- 1. 怎麼樣向OS註冊中斷?
- 2. 中斷向量的運作流程?

1. 怎麼樣向OS註冊中斷?



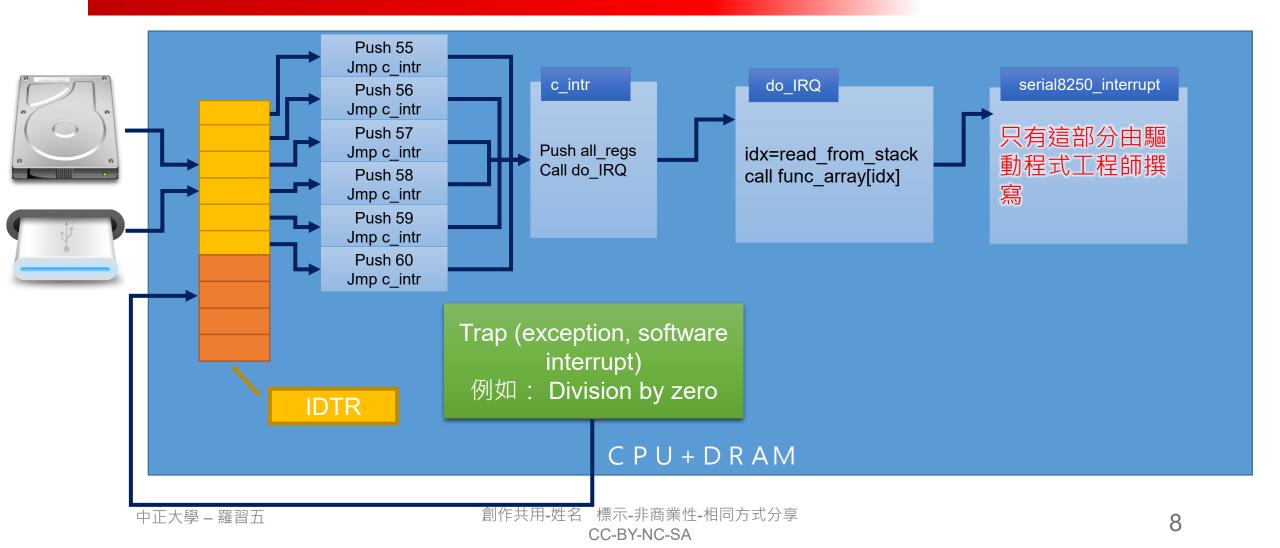
- API: request IRQ
 - 這部分的投影片都以serial8250為例,這是很簡單的驅動程式
 - ●軟硬體都很簡單,幾乎不會出錯,因此常常用來做○S的除錯工具

 - ◎在這個例子中,最重要的參數是 serial8250_interrupt ,請注意這是一個 C函數

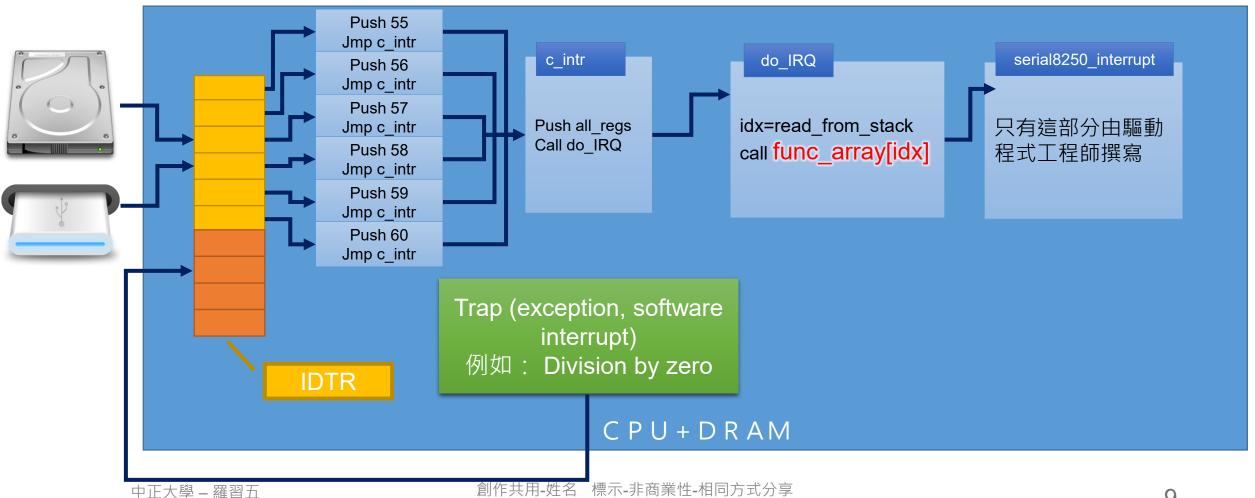
2. 中斷向量的運作流程?

- 對驅動程式設計師而言,只要硬體發生中斷,那麼OS就會呼叫「serial8250_interrupt」,大部分的驅動程式都是用「C」撰寫而成
- 幾乎沒人用組合語言,組合語言的部分、CPU直接相關的部分, 都由Linux代為處理

從OS開發者看中斷流程



從OS開發者看「註冊中斷」



創作共用-姓名 標示-非商業性-相同方式分享 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=

