80x86 Protection Mode

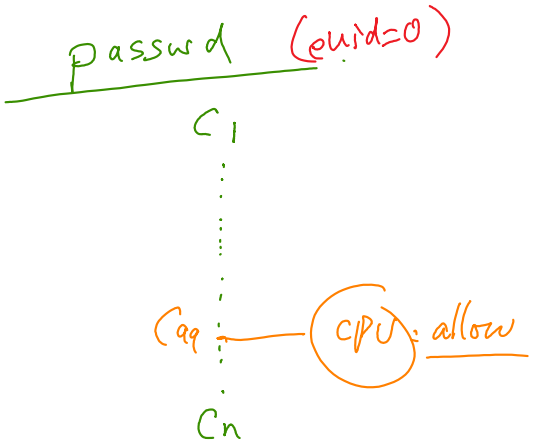
SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

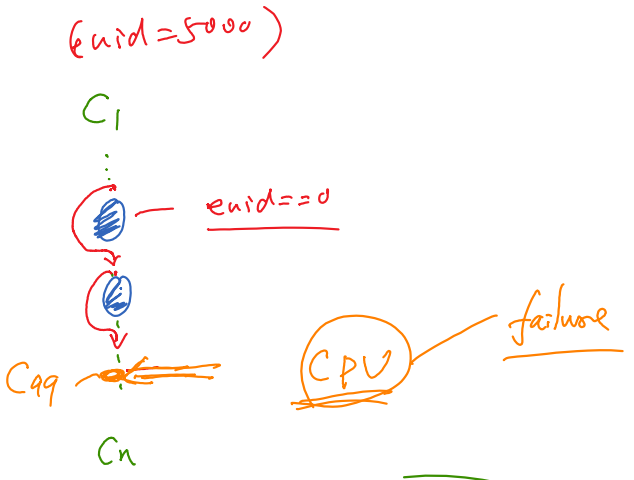
Why We Need Access Control in CPU

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

A Question

Why do we need access control inside in CPU?





In 8086 ~ 80286

80286 ~

Real Mode ??

No security

DOS

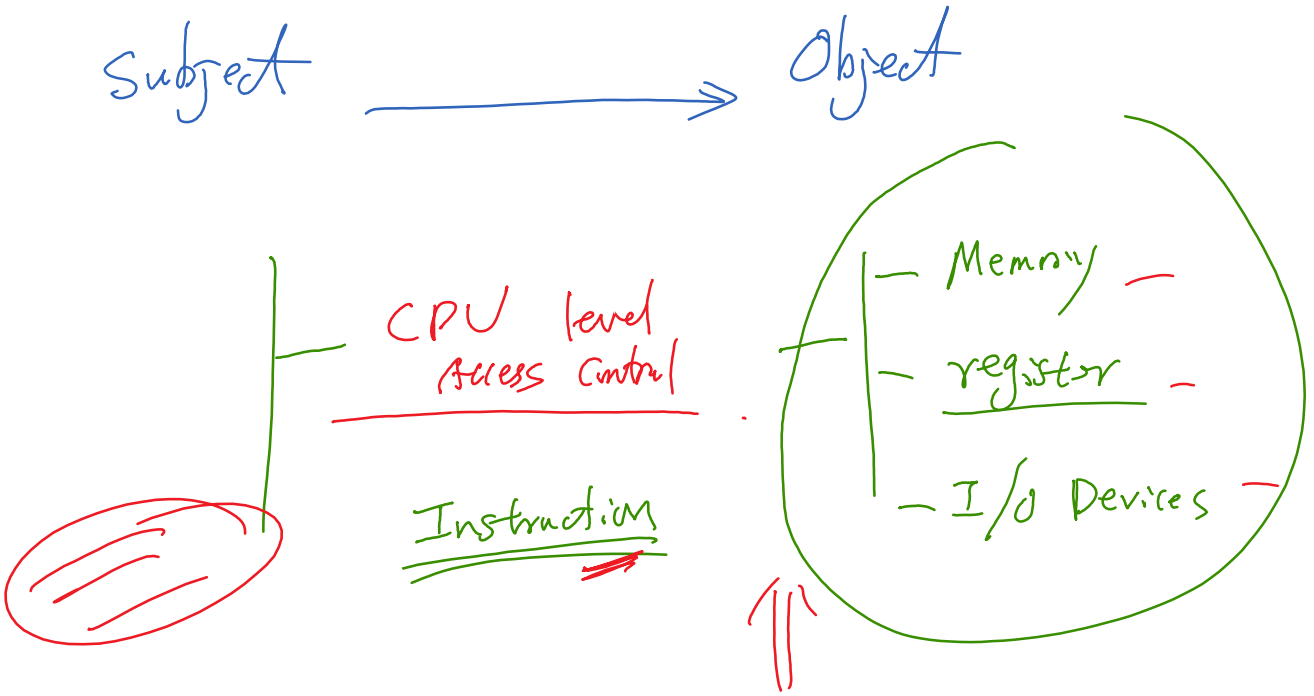
Protection Mode

CPU-Level Hardware } security

TCB: Trust Computing Base.

These days { Intel SGX, ARM TrustZone } Hardware Security

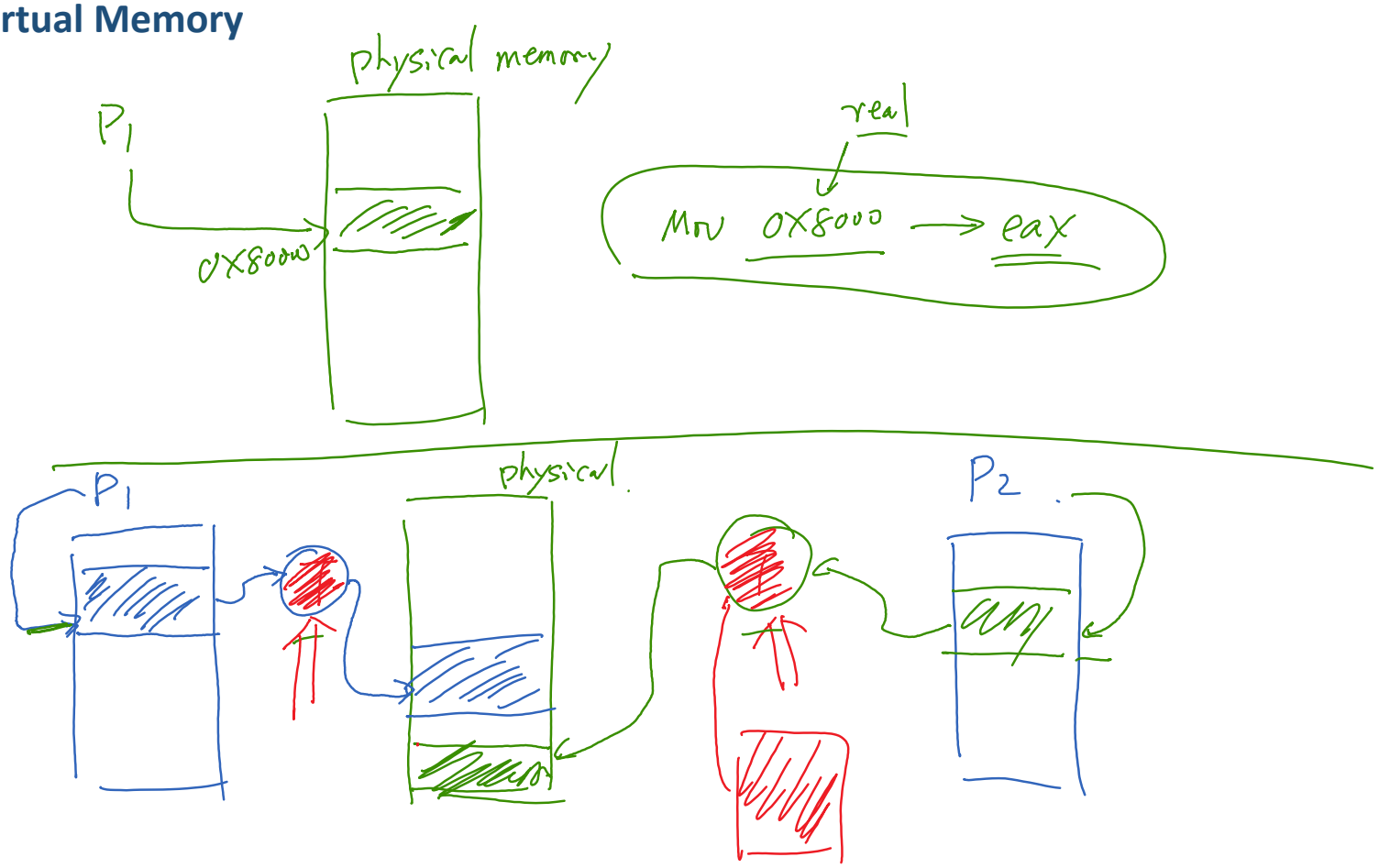
Access Control Overview



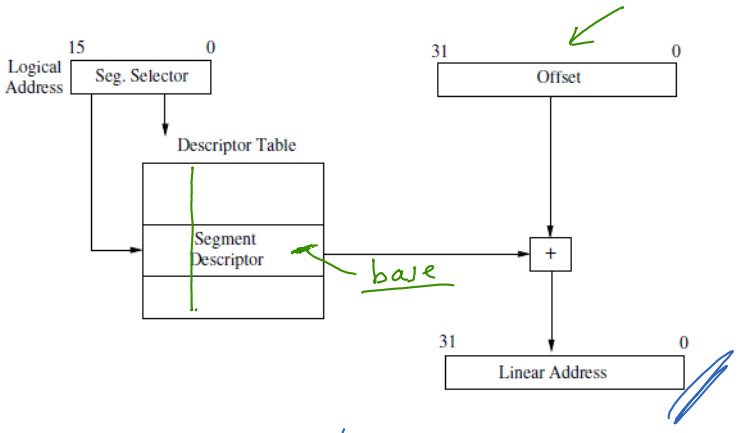
Memory Isolation

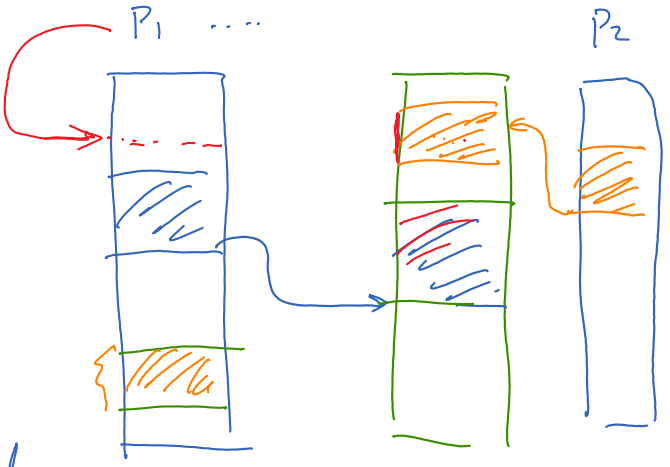
SYRACUSE
UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

Virtual Memory



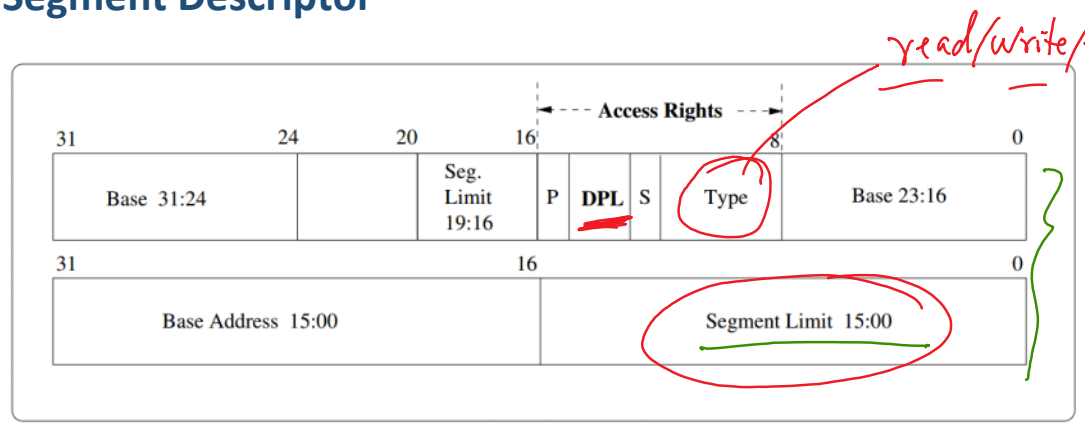
Logical Address to Linear Address

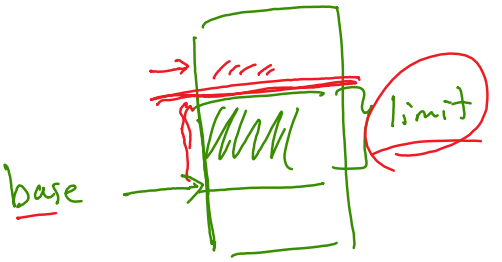




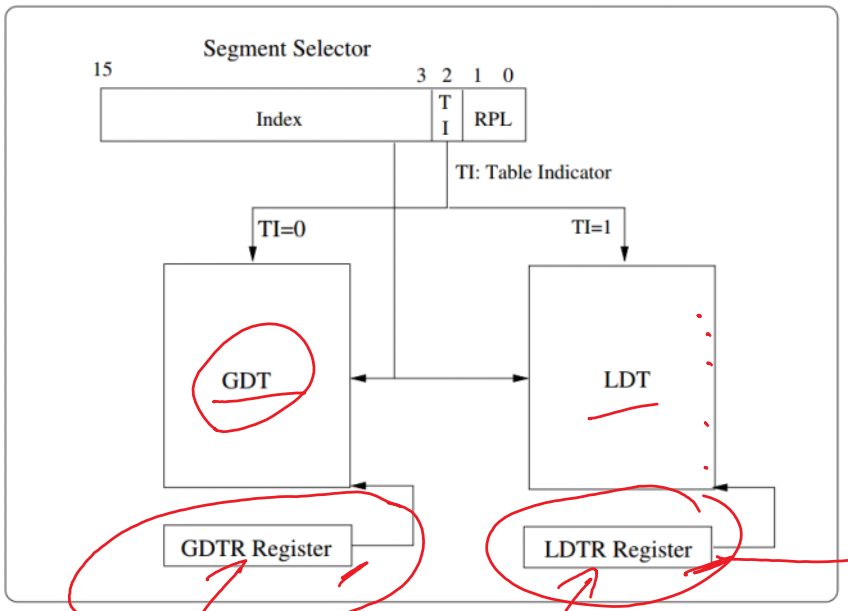
- capability-based access control.

Segment Descriptor





Descriptor Table

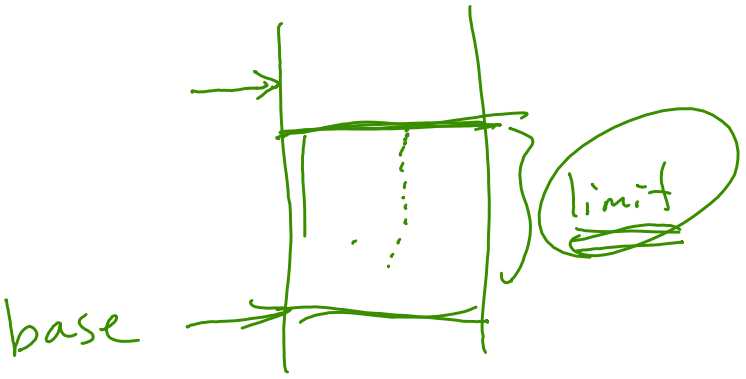


forge ticket

register protection

Question 1

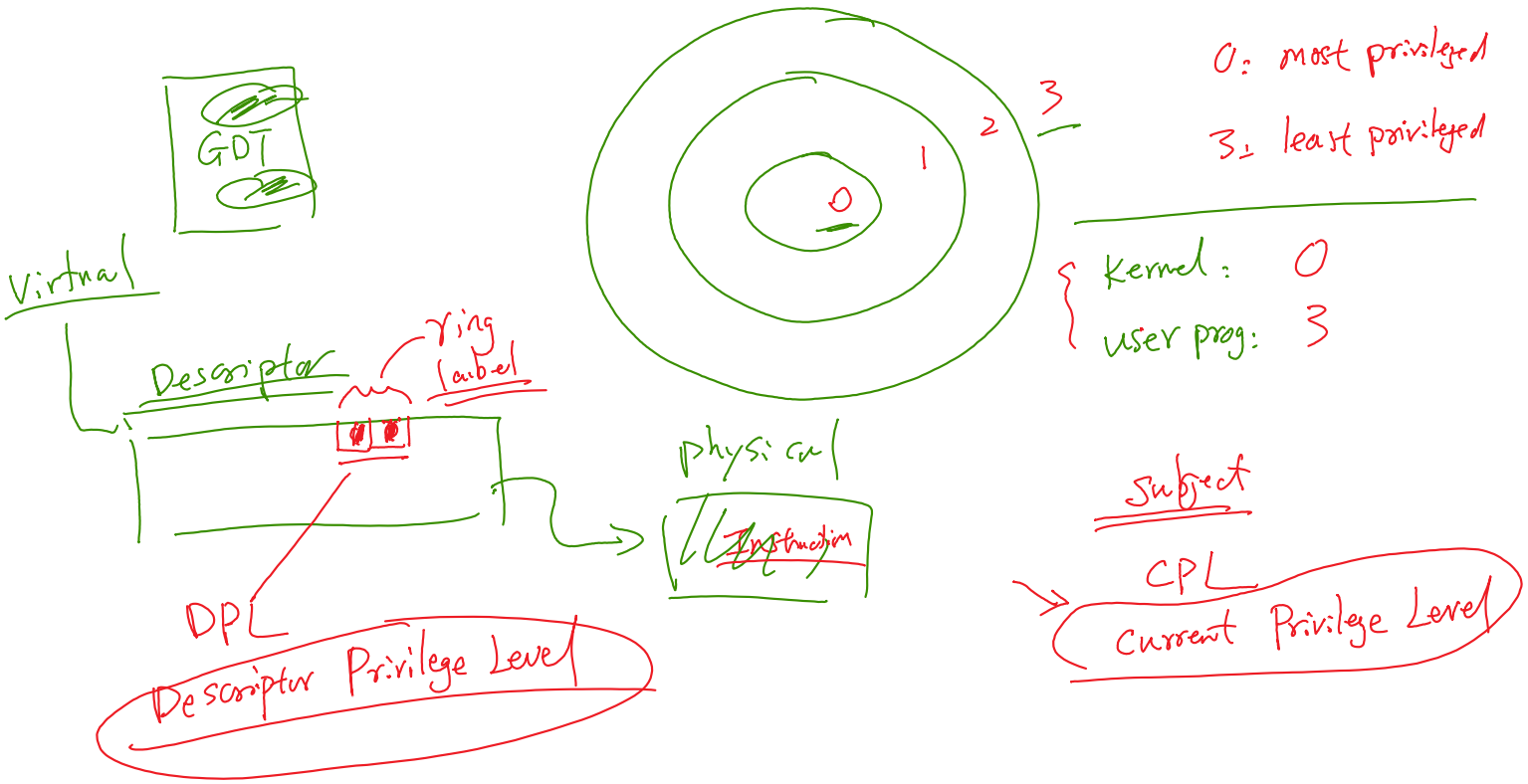
If a program is copying data to a buffer located toward the end of a segment, is it possible to overflow the segment as the result of buffer overflow?



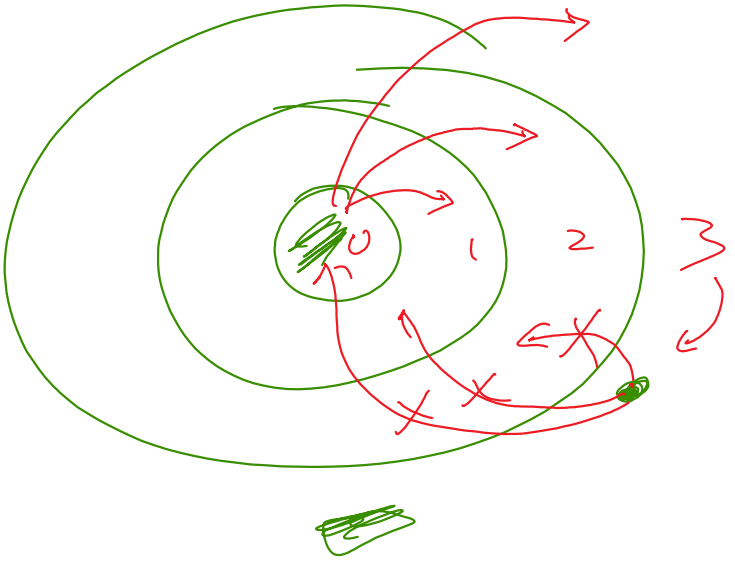
Rings

SYRACUSE UNIVERSITY
ENGINEERING & COMPUTER SCIENCE

Rings and Privilege Level



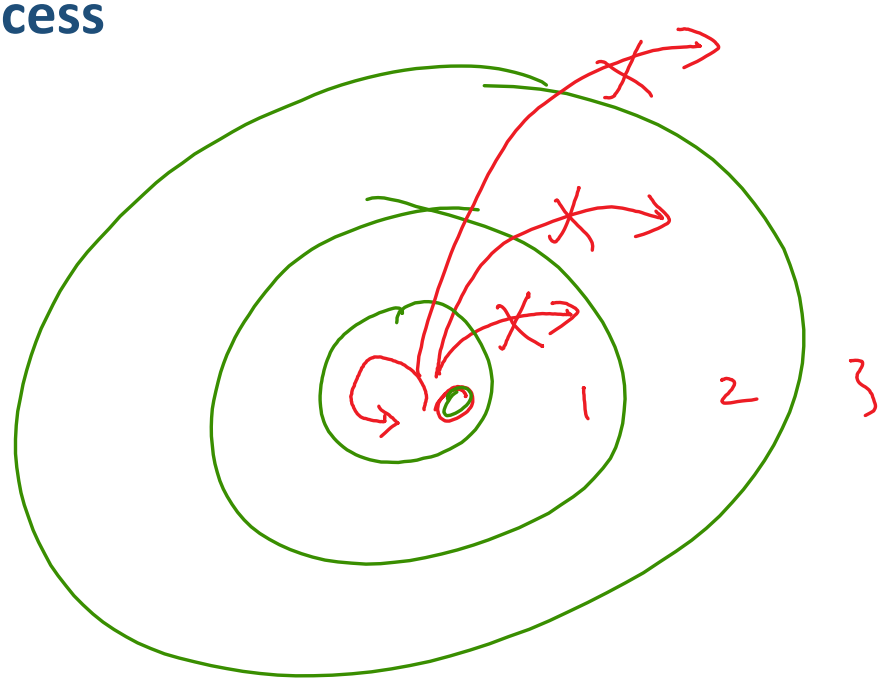
Data Access



- CPL : 0
- DPL : 0, 1, 2, 3

X CPL : 3
DPL : 0, 1, 2,

Code Access



JUMP

Register Access

General registers

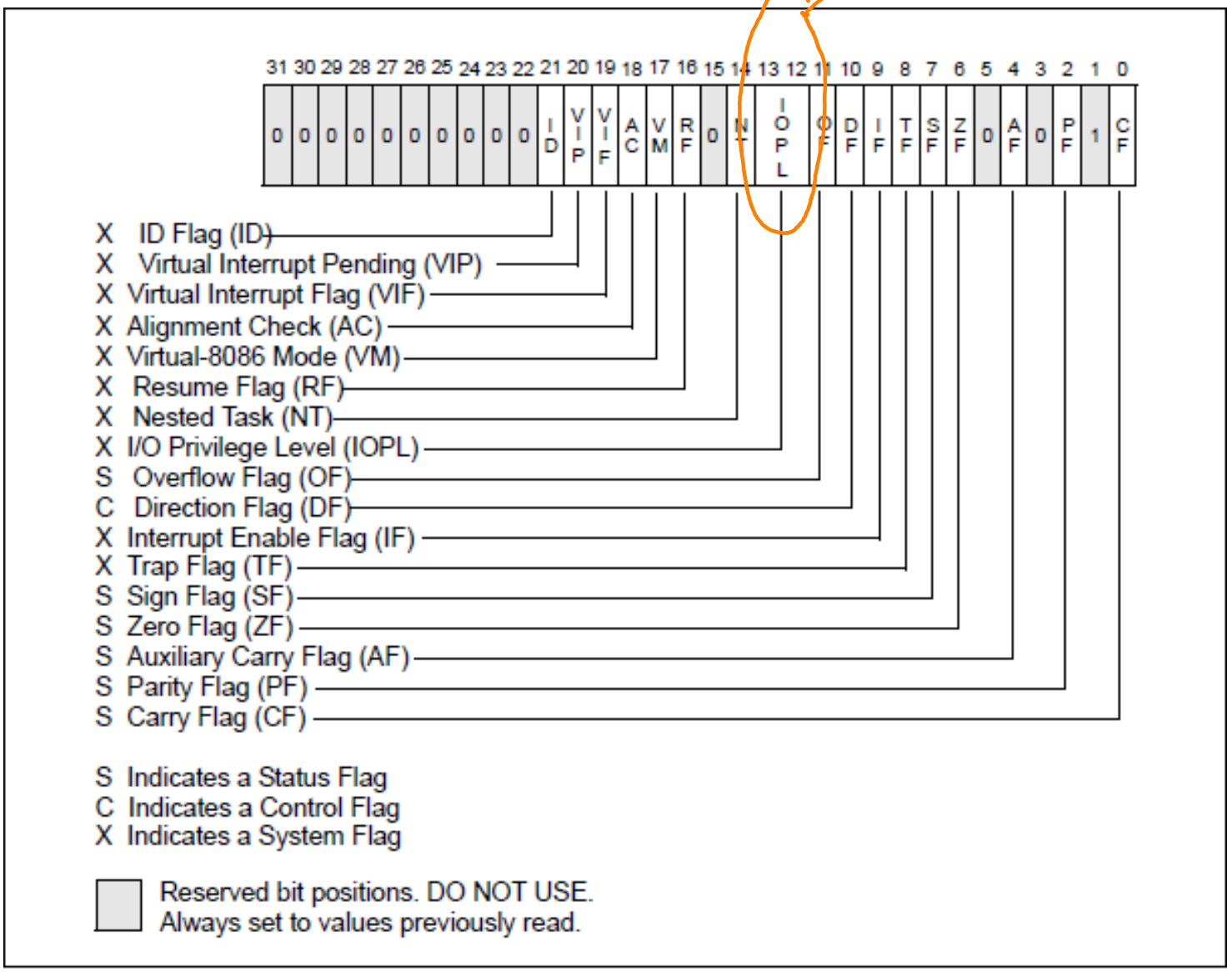
eax, ebx, ecx, cs, ds, ebp - -

Special-Purpose Registers

- GDTR
- LDTR
- PTBR: page table base register (CR3)

Ring 0

IO Access

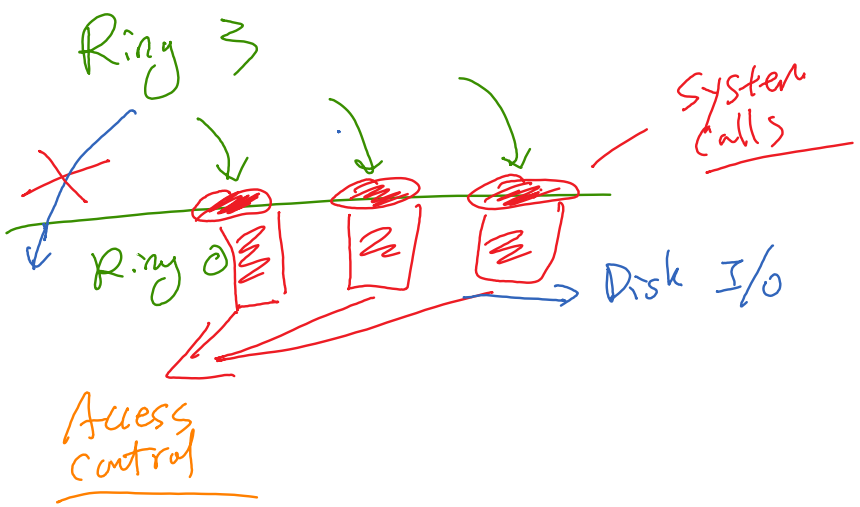


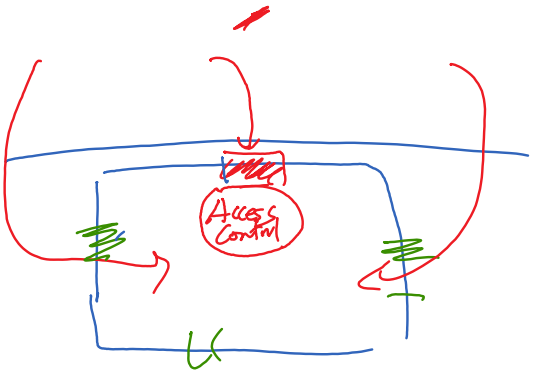
EFLAGS Register

System Calls

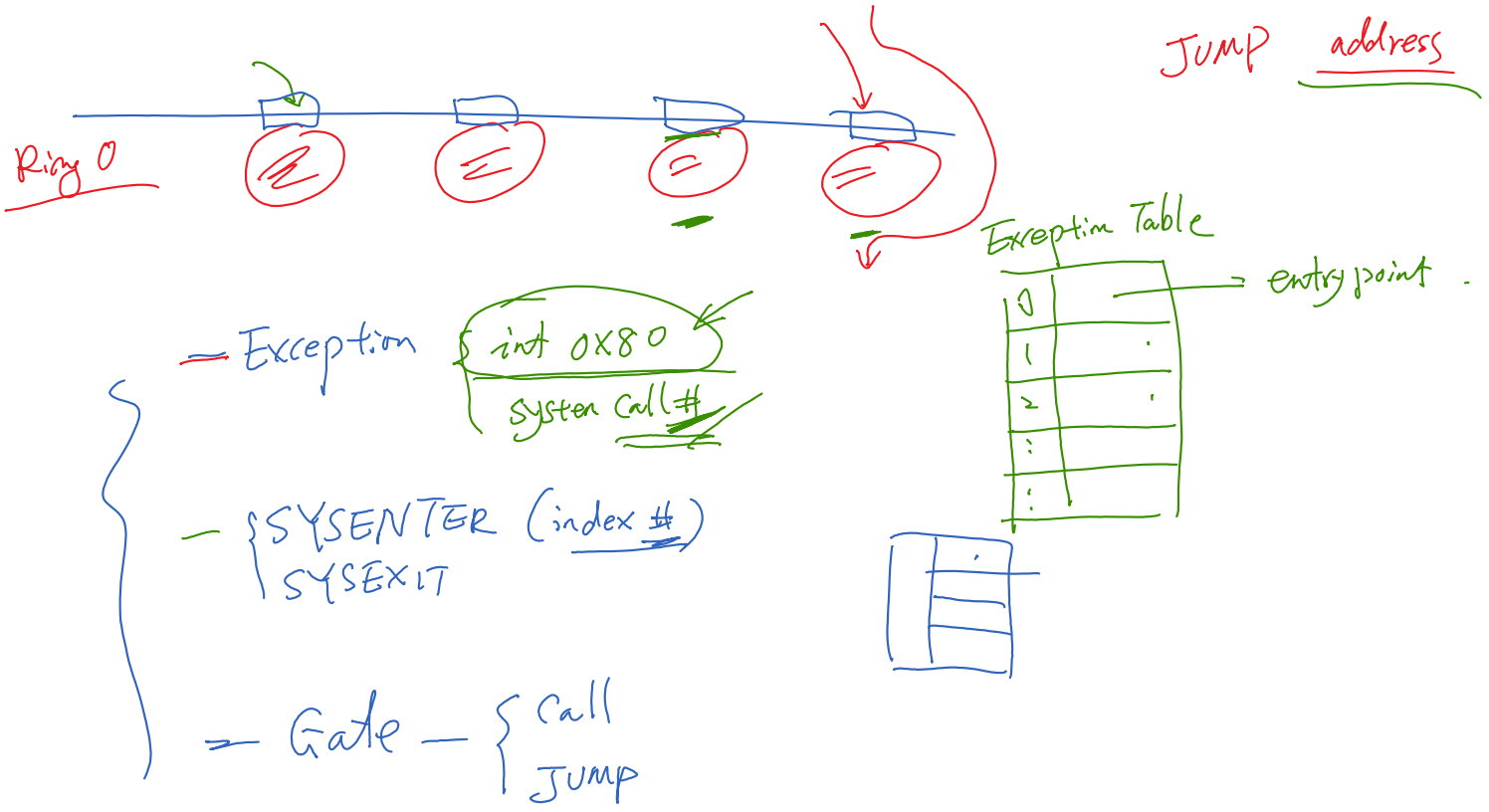
SYRACUSE
UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

Needs for Cross-Ring Invocation

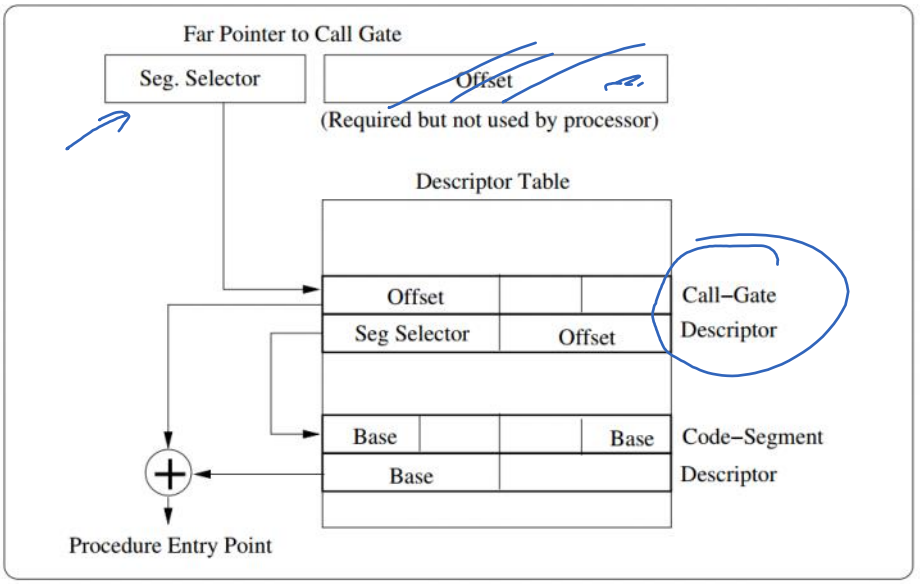




System Calls



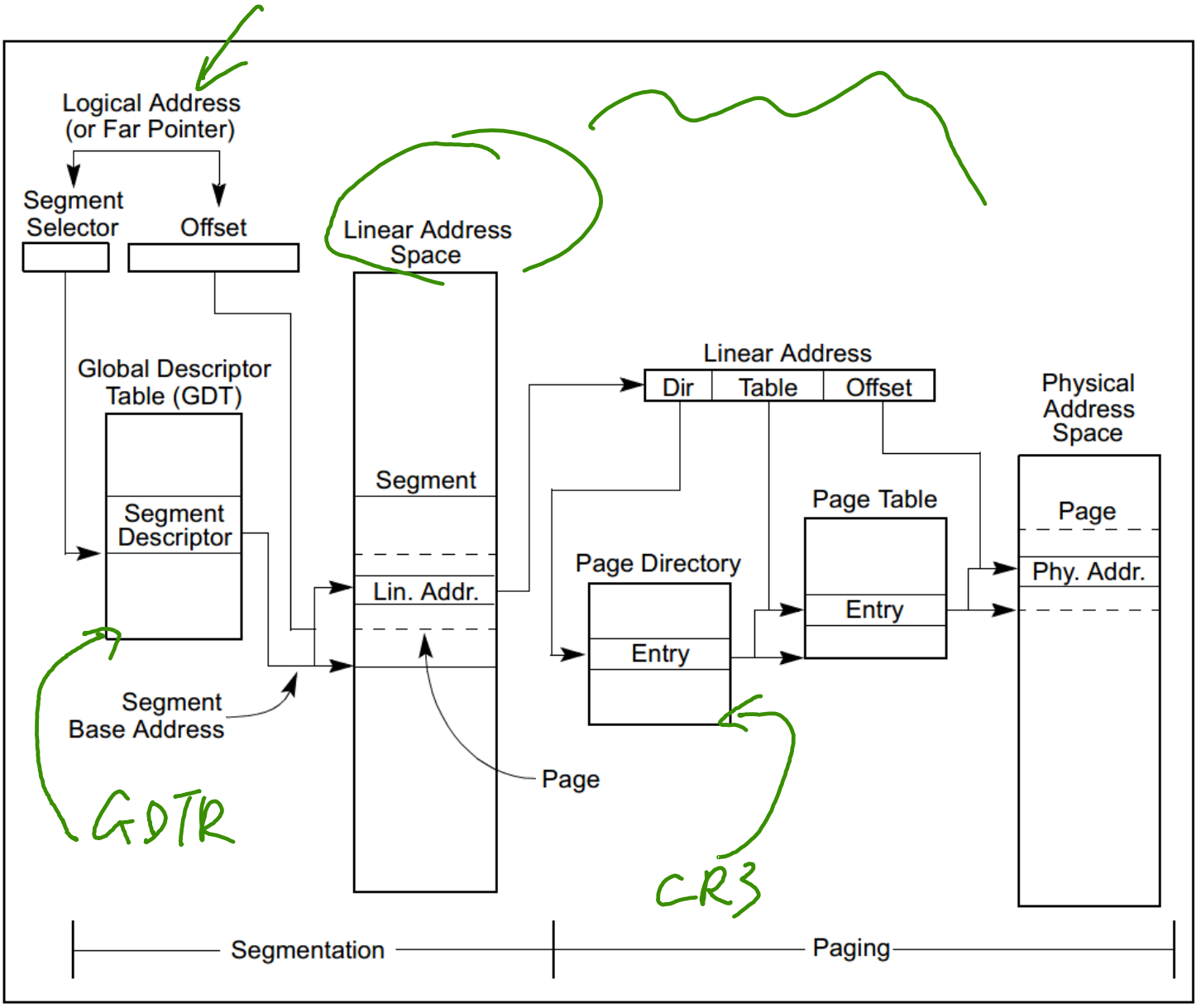
Call Gates


Far Pointer to Call Gate
Seg. Selector
Offset
(Required but not used by processor)
Descriptor Table
Offset
Call–Gate
Seg Selector
Offset
Descriptor
Base
Base
Code–Segment
Base
Descriptor
Procedure Entry Point

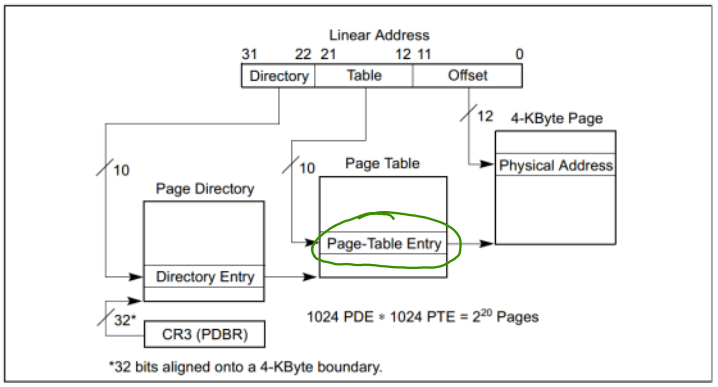
Paging

SYRACUSE
UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

Combining With Paging



Access Control



page-table entry

- R/W bit — { 0 : read-only
  1 : r/w
- U/S bit — { 0 : Supervisor Level (Kernel)
  1 : user-level

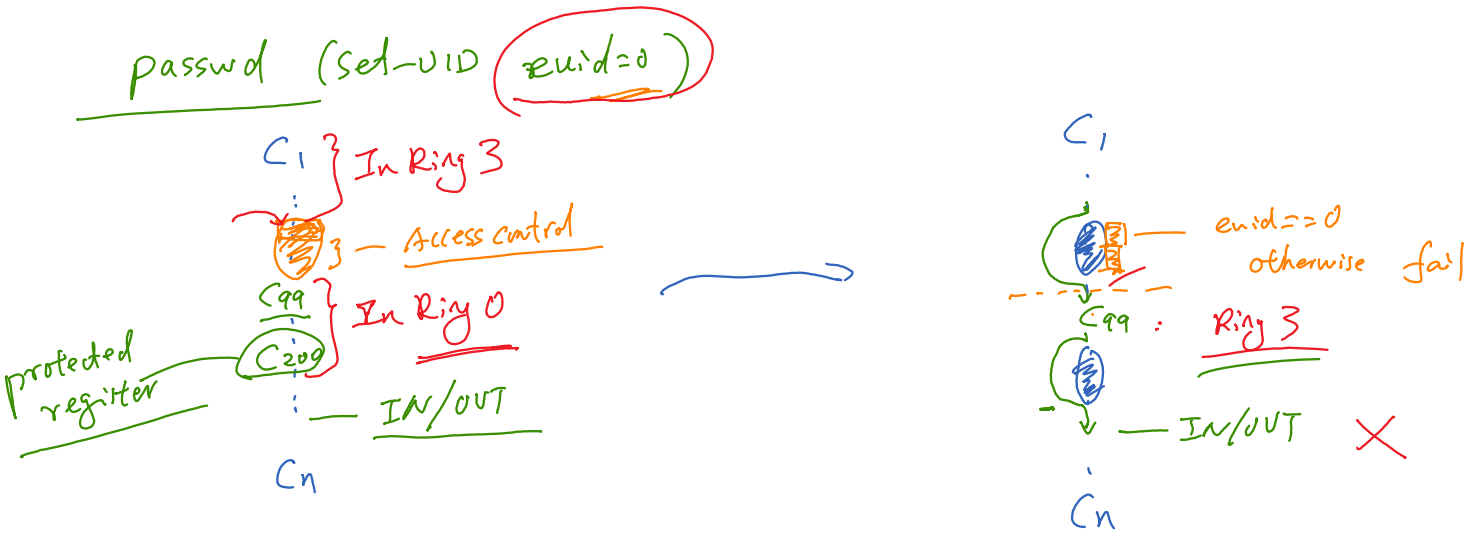
If CPL = 0, 1, 2 . supervisor level

CPL = 3 user-level

Review


SYRACUSE UNIVERSITY
FOUNDED A·D· 1870
SYRACUSE
UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

Back to Initial Question

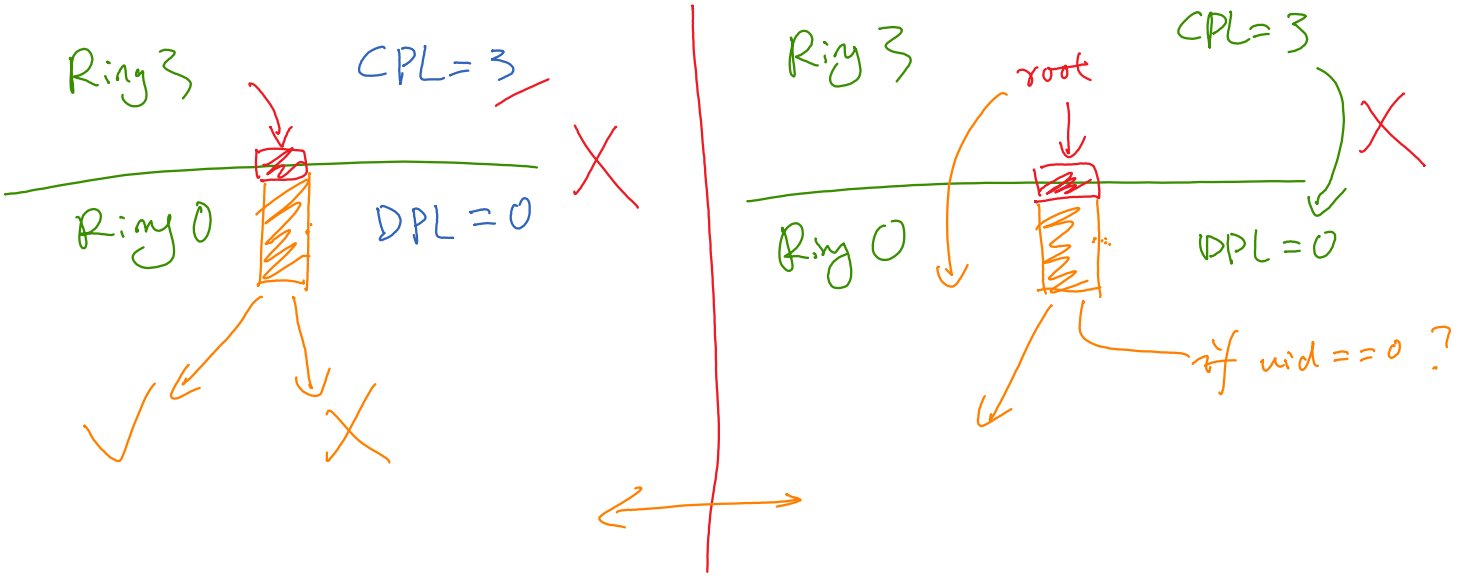


80x86 Protection Mode Questions

SYRACUSE
UNIVERSITY
ENGINEERING
& COMPUTER
SCIENCE

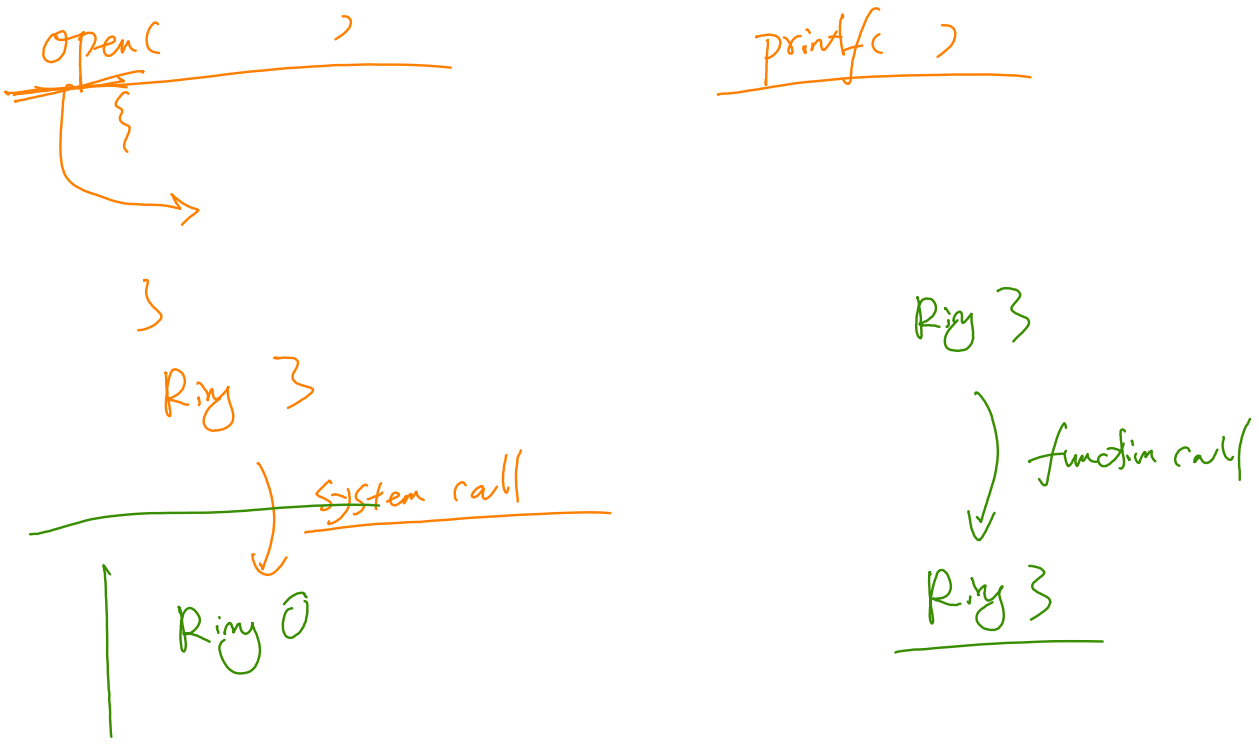
Question 2

Why can't a program directly write to the kernel memory? What if the program is running with the root privilege?



Question 3

What are the differences between system calls and library calls?



Summary

- 80x86 protection mode
- Memory protection
- Rings
- How OS depends on the protection mode