

Computer System- B Security

Introduction to OS Security

Memory Protection

Sanjay Rawat

bristol.ac.uk

We know that...

- Modern systems allow multiple processes to run concurrently.
- Virtual memory address space is used to facilitate this
- We need to make sure that
 - A process does not access memory not allocate to it.
 - One process (malicious) does not affect the other processes, including OS.

What we do

- Segmentation
 - refers to dividing a computer's memory into segments (code, data, ...) with specific access rights
- Virtual memory
 - Illusion that a process has full access to the entire memory address space
 - Abstracting the memory as VM and then dividing VM into blocks
 - Page table is used to translate virtual address to physical address

Intel x86 32/64

Segmentation and Paging mechanism

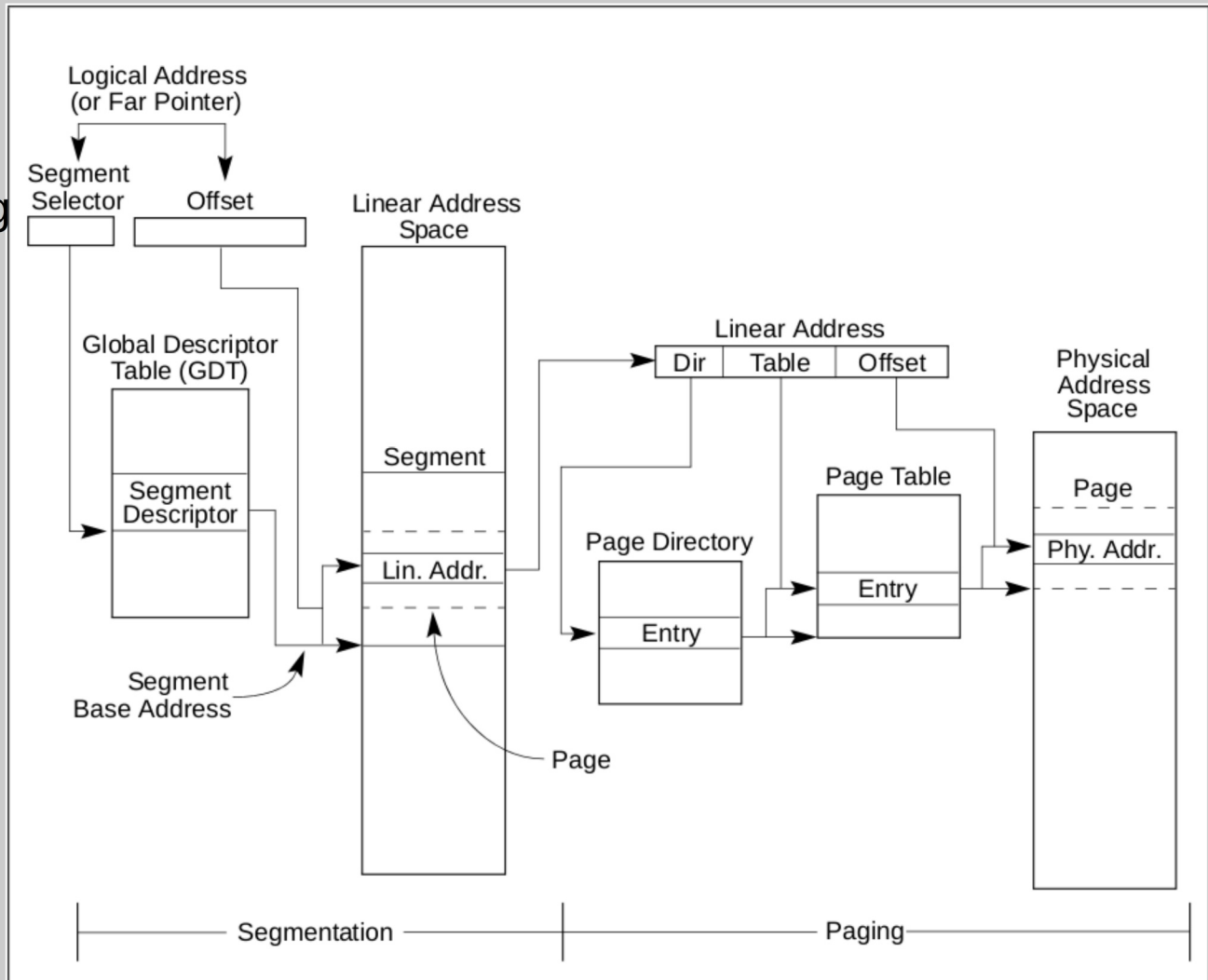
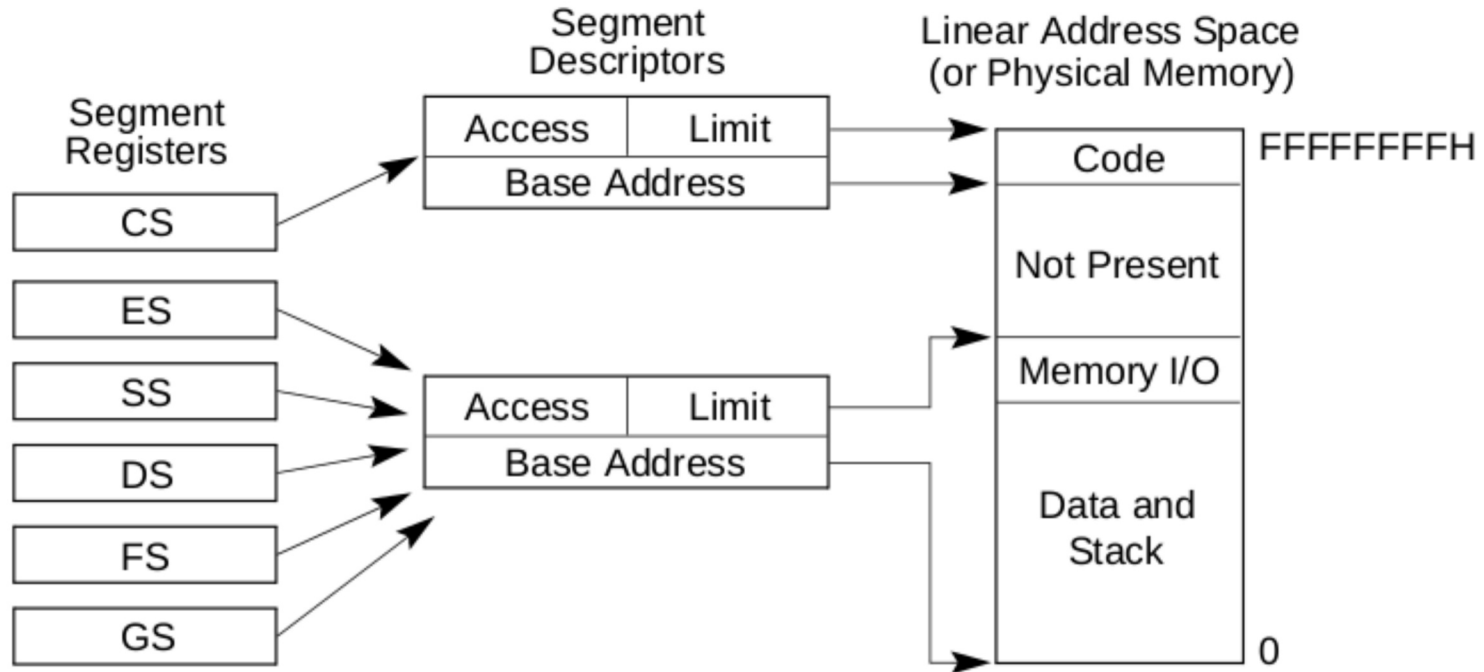


Fig from:
Intel 64 & IA-32 Manual
Vol. 3, sec 3.1

Segment based protection



Segmentation Registers

Visible Part		Hidden Part		
Segment Selector		Base Address, Limit, Access Information		
				CS
				SS
				DS
				ES
				FS
				GS

Segment descriptor

Descriptor privilege level (DPL)

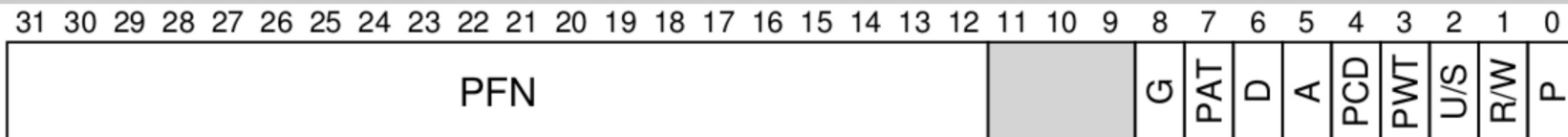
Current privilege level (CPL)

Privilege ring 0 - 3

Paging Based Protection

- Paging provides finer mapping of linear address to physical address → finer protection at page level
- Apart from mapping and swapping in/out, page entries also provide protection

32-bit page entries



Bit Position(s)	Contents
0 (P)	Present; must be 1 to map a 4-KByte page
1 (R/W)	Read/write; if 0, writes may not be allowed to the 4-KByte page referenced by this entry (see Section 4.6)
2 (U/S)	User/supervisor; if 0, user-mode accesses are not allowed to the 4-KByte page referenced by this entry (see Section 4.6)
3 (PWT)	Page-level write-through; indirectly determines the memory type used to access the 4-KByte page referenced by this entry (see Section 4.9)
4 (PCD)	Page-level cache disable; indirectly determines the memory type used to access the 4-KByte page referenced by this entry (see Section 4.9)
5 (A)	Accessed; indicates whether software has accessed the 4-KByte page referenced by this entry (see Section 4.8)
6 (D)	Dirty; indicates whether software has written to the 4-KByte page referenced by this entry (see Section 4.8)
7 (PAT)	If the PAT is supported, indirectly determines the memory type used to access the 4-KByte page referenced by this entry (see Section 4.9.2); otherwise, reserved (must be 0) ¹
8 (G)	Global; if CR4.PGE = 1, determines whether the translation is global (see Section 4.10); ignored otherwise
11:9	Ignored
31:12	Physical address of the 4-KByte page referenced by this entry

Page level protection Summary

- Page-level protection can be used alone or with segments.
- When combined, page-level read/write protection allows more protection granularity within segments.
- The processor performs two page-level protection checks:
 - Restriction of addressable domain (supervisor and user modes).
 - Page type (read only or read/write)
- An Intel 64 or IA-32 processor with the **execute-disable bit** capability can prevent data pages from being used by malicious software to execute code
 - If the execute-disable bit of a memory page is set, that page can be used only as data.

TLB Level Protection

- The access control bits are almost same as we have for PTE.
-

Virtual	Phy.	valid	prot
100	250	1	r