

The K Project

LSE Team

Protected Mode

Overview

Segment selectors reloading

Protected mode

onclusion

The K Project Memory Management

LSE Team

EPITA

mars 10, 2017

LSE Team (EPITA) The K Project mars 10, 2017 1/20



The K Project

LSE Team

Protected Mode

Overvie

Segment selectors

Protecte

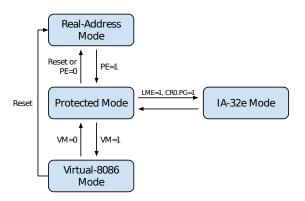


Figure:



Address translation

The K Project

LSE Team

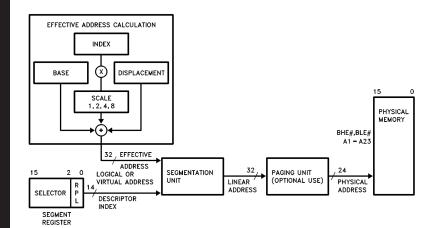
Protected

Overview

Overvie

Segmen

Protecte





Segmentation

The K Project

LSE Team

Protected

Overview

Segment selector

Protecto

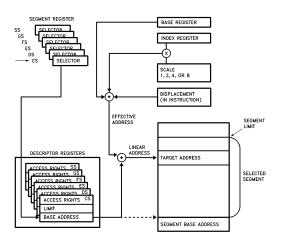


Figure:



Segment selectors

The K Project

LSE Team

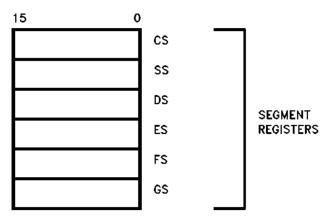
Protected

Overview

Segmen selector

Protecte

. . .





GDT: Structure overview

The K Project

LSE Team

Protected Mode

Overvie[®]

GDT

Segmen selector reloadin

Protected mode

mode

Conclusio

■ The GDT (Global Descriptor Table) is an array that contains information about every segment.

- Segment Descriptor:
 - base address
 - limit (segment size)
 - segment type (code or data)
 - access rights

First entry must be null. (Don't forget to memset your GDT memory area before setting it)



GDT Entries

The K Project

LSE Team

Protected Mode

Overvie

GDT

Segmen selector reloadin

Protecte mode

onclusion

■ Null segment

■ Kernel Code segment

■ Kernel Data segment

■ Userland Code segment

■ Userland Data segment

■ Task State Segment (don't worry about that right now)



GDT Entry

The K Project

LSE Team

Protected Mode

Overvie

GDT

Segment selectors reloading

Protecte

mode

Conclusion

```
31
                  24 23 22 21 20 19
                                       16 15 14 13 12 11
                                                             8 7
                                  Seg.
                                              D
     Base 31:24
                     G /
                          LV
                                  Limit
                                          Р
                                                  S
                                                       Type
                                                                   Base 23:16
                                                                                     4
                                              Р
                        В
                                 19:16
31
                                       16 15
           Base Address 15:00
                                                    Segment Limit 15:00
                                                                                    0
```

L — 64-bit code segment (IA-32e mode only)
AVL — Available for use by system software

BASE — Segment base address

D/B — Default operation size (0 = 16-bit segment: 1 = 32-bit segment)

DPL — Descriptor privilege level

G — Granularity

LIMIT — Segment Limit

P — Segment present

— Descriptor type (0 = system; 1 = code or data)

TYPE — Segment type



Entry Types and Permissions

The K Project

LSE Team

Protected

Overvie

GDT

Segmen selectors

Protecte

mode

Type Field					Descriptor	Description
Decimal	11	10 E	9 W	8 A	Type	
0	0	0	0	0	Data	Read-Only
1	0	0	0	1	Data	Read-Only, accessed
2	0	0	1	0	Data	Read/Write
3	0	0	1	1	Data	Read/Write, accessed
4	0	1	0	0	Data	Read-Only, expand-down
5	0	1	0	1	Data	Read-Only, expand-down, accessed
6	0	1	1	0	Data	Read/Write, expand-down
7	0	1	1	1	Data	Read/Write, expand-down, accessed
		С	R	Α		
8	1	0	0	0	Code	Execute-Only
9	1	0	0	1	Code	Execute-Only, accessed
10	1	0	1	0	Code	Execute/Read
11	1	0	1	1	Code	Execute/Read, accessed
12	1	1	0	0	Code	Execute-Only, conforming
13	1	1	0	1	Code	Execute-Only, conforming, accessed
14	1	1	1	0	Code	Execute/Read, conforming
15	1	1	1	1	Code	Execute/Read, conforming, accessed



GDTR register

The K Project

LSE Team

Protected

Overvie

GDT

Segmen

selectors reloading

Protecte mode

47 16 15 0 32-bit Base Address Limit



Loading GDT

The K Project

LSE Team

Protected

Overviev

GDT

Segment selectors reloading

Protected

nouc



Segment selectors

The K Project

LSE Team

Protected

Overvie

Segment selectors reloading

Protected

noue





Segment selectors

The K Project

LSE Team

Protected

Overviev

OVEIVIE

Segment selectors

reloading

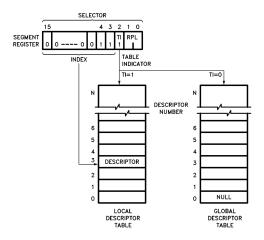


Figure:



The K Project

LSE Team

Protected

Overview

Overviev

Segment

Protected mode

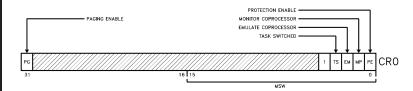


Figure:



The K Project

LSE Team

Protected

Overviev

Overvier

Segment selectors reloadin

Protected

mode

onclusio

You have to use an auxilliary register to set cr0:

```
movl $0x42, %cr0 ; It _won't_ assemble
```

movl \$0x42, %eax

movl %eax, %cr0 ; OK



The K Project

LSE Team

Protected

mode

Likewise, setting data in segment register:

movw \$0x42, %ax

movw %ax, %ds

movw %ax, %fs

movw %ax, %gs

movw %ax. %ss

16 / 20



The K Project

I SF Team

Protected Mode

Overvie

GDT

selectors reloading

Protected mode

Conclusion

```
Methode 1

pushl $0x42 ; push %cs on the stack

pushl $1f ; push %eip on the stack

lret ; far return
```

After the lret you will get

; here, with cs set to 0x42

```
Methode 2
```

1:

```
ljmp $0x42, %1 ; long jump 1:
```



Summary

The K Project

LSE Team

Protected Mode

Overviev

. . .

Segmen selector reloadin

Protecte mode

- Build GDT
- Load GDT
- Set PE flag in CRO
- Reload segment selectors



Advices

The K Project

LSE Team

Protected

Overview

Overviev

Segmen selector reloadin

Protecte mode

- Use packed struct and bitfields
- Write a GDT Pretty Printer



Contact

The K Project

LSE Team

Protected Mode

Overviev

CDT

Segmen selectors reloadin

Protecte mode

- #k (irc.rezosup.org)
- epita.cours.k
- k[at]lse.epita.fr
- naam[at]lse.epita.fr
- nurelin[at]lse.epita.fr