STOS - Protected Mode

Gabriel Laskar <gabriel@lse.epita.fr>

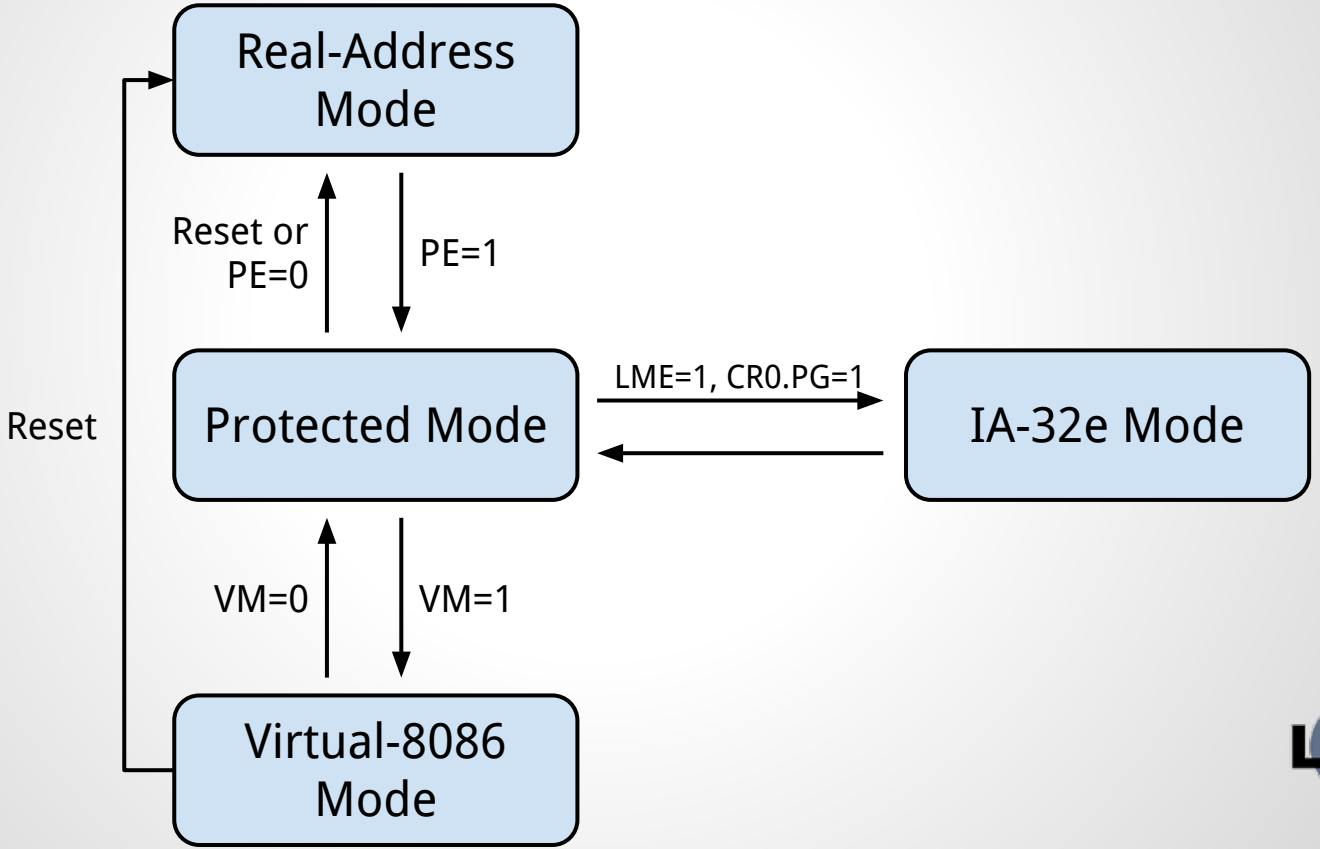
LSE Security System

Outline

- Protected mode
- GDT
- Assignment
- How to submit your results

LSE Security System

x86 modes


Real-Address Mode
Reset or PE=0
PE=1
Reset
Protected Mode
LME=1, CR0.PG=1
IA-32e Mode
VM=0
VM=1
Virtual-8086 Mode

Real Mode vs Protected Mode

- 16-bit mode
- <1MB of Addressable Memory
- No HW protection

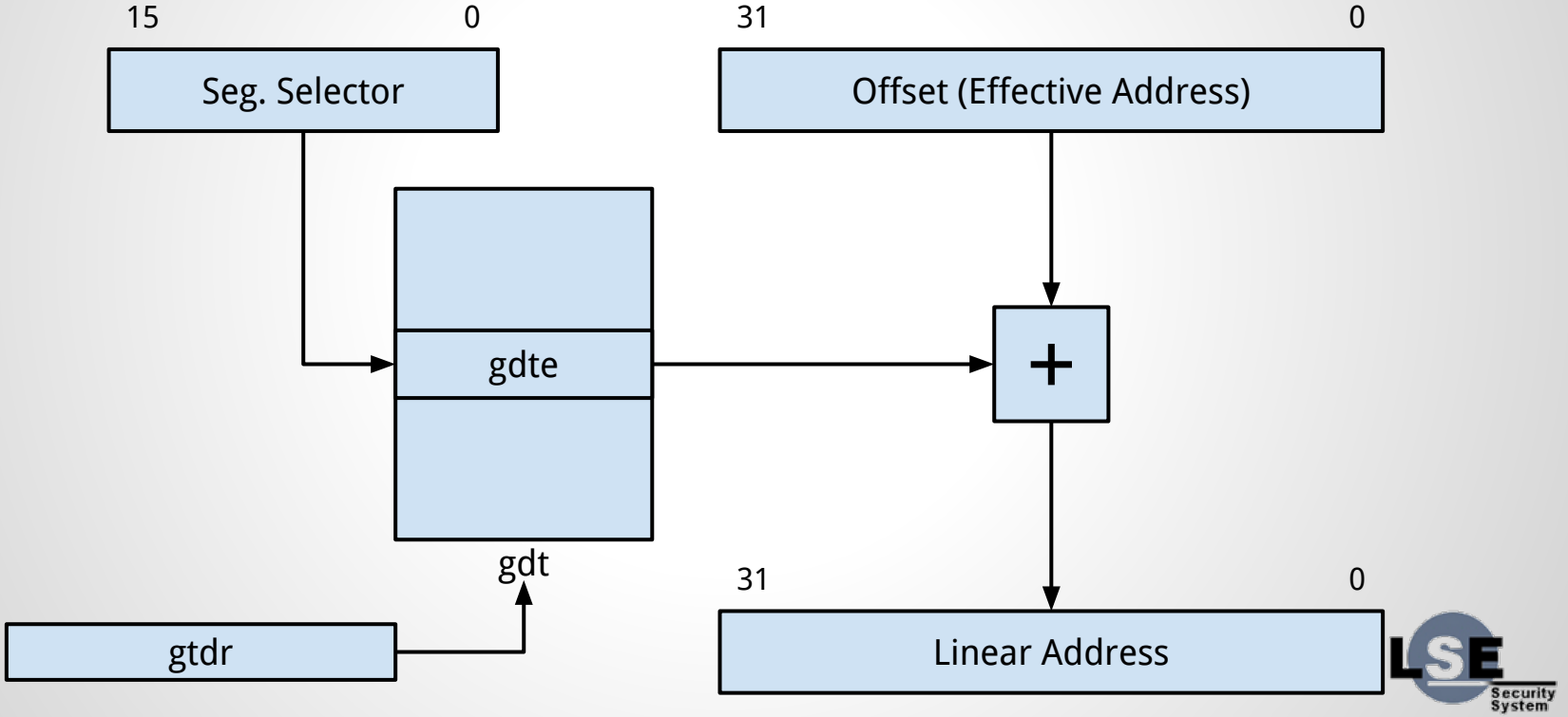
- 32-bit mode
- 4GB of Addressable Memory
- HW protection

LSE Security System

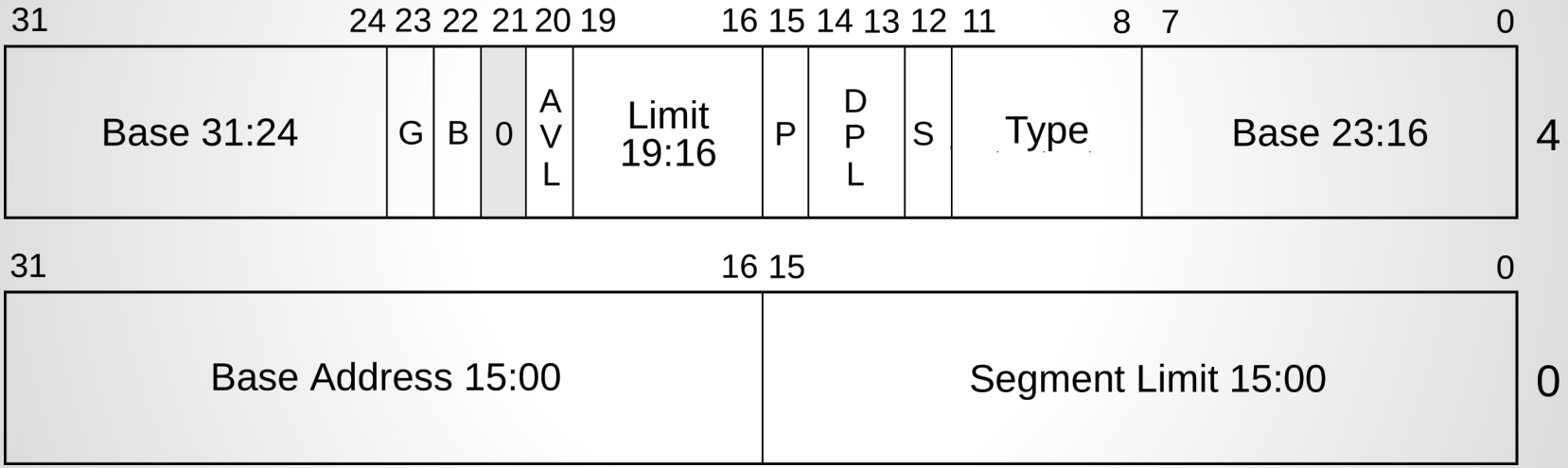
Segmentation

- Address translation
- Work with contiguous memory areas
- Allow multiple address space

Address translation when PE=1



GDT entries


31
24 23 22 21 20 19
16 15 14 13 12 11
8 7
0
Base 31:24
G
B
0
A V L
Limit 19:16
P
D P L
S
Type
Base 23:16
4
31
16 15
0
Base Address 15:00
Segment Limit 15:00
0

Segment Selectors

- Tied to GDT entries
- 2 parts, public part and shadowed part
- Provide basic permissions on zones
- Each segment selector describe memory access for some instructions

Segment Selector

Descriptions of segment selectors

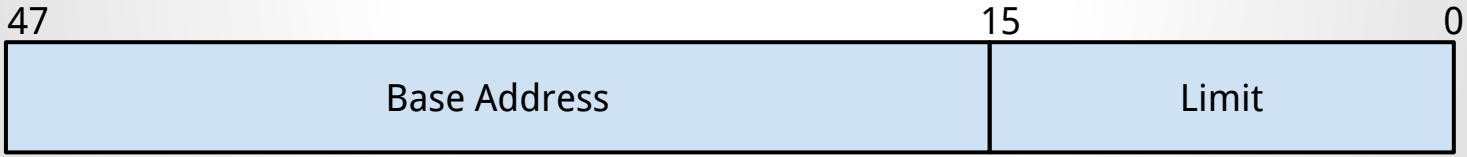
- %cs : access to code (%eip, call, ret ...)
- %ss : access to stack data (%esp, push, pop)
- %ds : access to memory and %edi
- %es : access to %esi
- %fs : user-defined
- %gs : user-defined

LSE Security System

TLS and per-cpu variables

- `%fs`, `%gs` can be used to implement TLS or per-cpu variables.
- One page mapped, and referenced by segment selector

GDTR Register



LSE Security System

Load a new GDT

```
struct gdtr gdtr = {
    .base = gdt;
    .limit = sizeof(gdt) - 1;
};

__asm__("lgdt %0\n"
    : /* no output */
    : "m" (gdtr)
    : "memory");
```

LSE Security System

How to activate the Protected Mode

- Build a GDT
- Load a GDT
- Set PE flag in `%cr0`
- Reload segment selectors

What do we need in STOS

- PM module
- Everything is described on the website

LSE Security System

How to submit your work

- We will test the “result” branch of your git repository
- You must also send a patch series of your work to stos-1@lse.epita.fr

LSE Security System