Stack canaries/cookies

- Compiler-assisted protection scheme
- Tripwire-like defense against return address overwrites

- Defeats against sequential/contiguous spatial memory errors
X86 Segmentation

- MMU
- SEL unit
- Paging unit
- %cr3 → PT
- NA → PA, PERN, ...


x86 Segmentation

- MUU
- Seg. unit
- Paging unit
- %cr3 -> PT
- NA -> PA, PES

GDT / LDT -> Local

- Global Descriptor Table
- Segment Descriptor
- Base address
- Limit
Six segment registers
(for -11- selectors)

%cs       %fs
%ds       %gs
%es       %gs
%ss

Index the GDT/IDT
GDT / LDT

base  base  base  ...
limit  limit  limit  ...

%CS = 0x1

mov can be used to spill/fill seg. registers

seg. registers are 16-bit
Address Translation

1. `mov $0x1, 0x00010203`
2. `mov $0x4, 0x8(%eax)`

%eax = 0x00010200

0x00010208
Address Translation

mov $0xf, 0x00010203
mov $0x1, 0x8 (%eax)
%eax = 0x00010200

GDT [0xf].base (0x1000)

0x0001f203 0x0001f208