Stack canaries/cookies

- Compiler-assisted protection scheme
- Tripwire-like defense against return address overwrites
- Defends against sequential/contiguous spatial memory errors
[STACK]

- ref. addr.
- SFP
- other spilled data (ref. values)
- canary

[HEAP]

- canary (master copy)

- local variables

Canary: random 4-byte value to master "copy" is placed in the heap as ASLR effectively randomizes its location.
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
(or -11- selectors)

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

Index the GDT/IDT
Address Translation

\[ \text{mov } \$0x1, \quad 0x00010203 \]
\[ \text{mov } \$0xf, \quad 0x8(\%eax) \]
\[ \%eax = 0x000010200 \]
\[ \text{mov } 0x000010208 \]
Address Translation

\text{mov} \$0x1, \text{0x00010203} +
\text{mov} \$0xf, \text{0x8}(%eax)
\text{eax} = \text{0x00010200}

\text{GDT} [\%fs].base
(\text{0x1000})

\text{0x00010203} \quad \text{0x00010208}
Stock Protector (GCC/ULMM)

- fno-stack-protector
- fstack-protector
- fstack-protector-strong
- fstack-protector-old
mov %gs: 0x14, %e8

%gs := 0x63

selector: (0xc = 12)

GDT[0xc].base + 0x14

LPTCB

...