

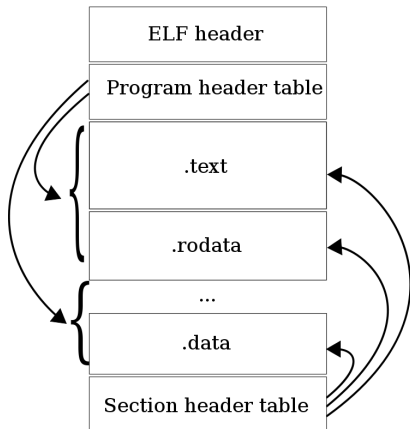
The K Project

Userland

LSE Team

EPITA

May 06, 2019



- `.text`: program code
- `.rodata`: readonly data (ex: Constant strings)
- `.data`: global data
- `.bss`: uninitialized data
- `.symtab`: symbols table
- `.init`: executable code for the initialization of the program
- `.fini`: executable code for the program termination

The K Project

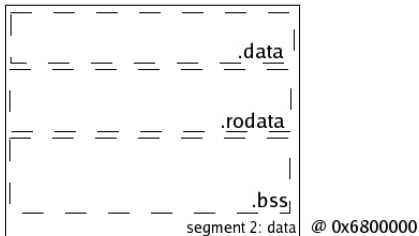
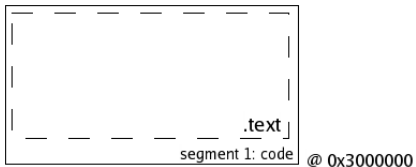
LSE Team

Binary loading

TSS

Jump to
userland

Conclusion



The K Project

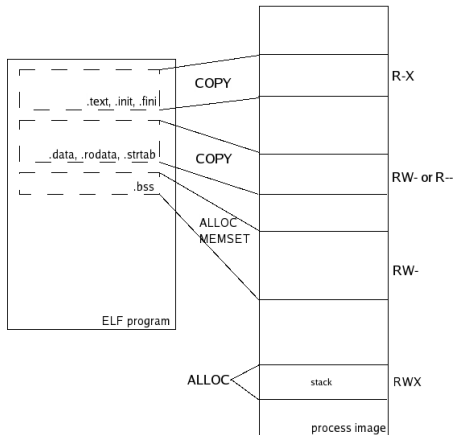
LSE Team

Binary loading

TSS

Jump to
userland

Conclusion



- Program headers can be found directly from Elf header with these fields:
 - `e_phoff`: offset to program header structure array
 - `e_phentsize`: program header structure size in array
 - `e_phnum`: number of program header structures in array

- Program header structure then contains the following informations:
 - `p_type`: program header type
 - `p_flags`: memory flags associated with program header
 - `p_vaddr`: expected virtual memory address of program header
 - `p_off`: program header offset in Elf
 - `p_memsz`: in memory size of program header
 - `p_filesz`: in file size of program header. It can differ from `p_memsz`, then the remaining part must be filled with 0

The K Project

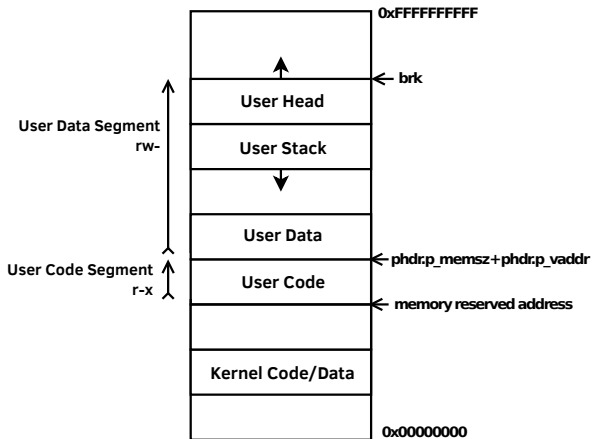
LSE Team

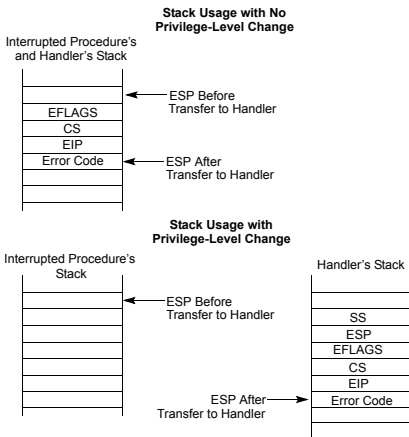
Binary loading

TSS

Jump to
userland

Conclusion





The K Project

LSE Team

Binary loading

TSS

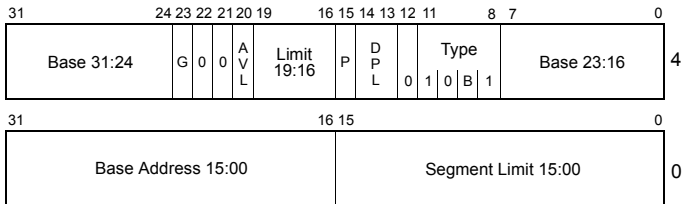
Jump to
userland

Conclusion

31	15	0	
I/O Map Base Address	Reserved		100
Reserved	LDT Segment Selector		96
Reserved	GS		92
Reserved	FS		88
Reserved	DS		84
Reserved	SS		80
Reserved	CS		76
Reserved	ES		72
	EDI		68
	ESI		64
	EBP		60
	ESP		56
	EBX		52
	EDX		48
	ECX		44
	EAX		40
	EFLAGS		36
	EIP		32
	CR3 (PDBR)		28
Reserved	SS2		24
	ESP2		20
Reserved	SS1		16
	ESP1		12
Reserved	SS0		8
	ESP0		4
Reserved	Previous Task Link		0

Reserved bits. Set to 0.

TSS Descriptor



- AVL Available for use by system software
- B Busy flag
- BASE Segment Base Address
- DPL Descriptor Privilege Level
- G Granularity
- LIMIT Segment Limit
- P Segment Present
- TYPE Segment Type

The K Project

LSE Team

Binary loading

TSS

Jump to
userland

Conclusion

```
movw $0x10, %ax  
ltr %ax /* The second GDT entry describe the TSS */
```

The K Project

LSE Team

Binary loading

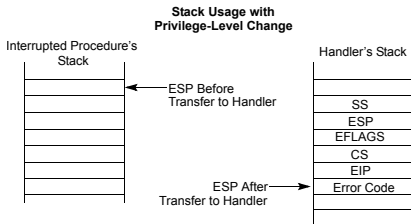
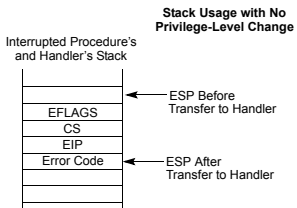
TSS

Jump to
userland

Conclusion

- GDT should then contain:
 - Null descriptor
 - Kernel code segment
 - Kernel data segment
 - Userland code segment
 - Userland data segment
 - TSS

- To jump to Userland, register values must be:
 - `cs`, `ds`, `ss`, `es`
 - `esp` must be set to a task stack address
 - `eip` must be set to program entry point



The K Project

LSE Team

Binary loading

TSS

Jump to
userland

Conclusion

- Did you notice DS and ES are *not* on the stack ?

The K Project

LSE Team

Binary loading

TSS

Jump to
userland

Conclusion

- `k[at]lse.epita.fr`
- `labos.lse` with `[K]` tag
- `#k` (`irc.rezosup.org`)
- `guillaume.pagnoux[at]lse.epita.fr`
- `tom.decrette[at]lse.epita.fr`