

The K Project

LSE Team

Memory layout

Syscall handler

SBRK

Conclusion

The K Project

LSE Team

EPITA

April 26, 2017

1 / 13

LSE Team (EPITA) The K Project April 26, 2017

User memory layout

The K Project

LSE Team

Memory layout

Syscall handler

VGA

SBRK

Conclusion

Needed segments

- Code
- Data

Optional segments

■ Stack

LSE Team (EPITA) The K Project April 26, 2017 2 / 13



Sane memory layout

The K Project

LSE Team

Memory layout

Syscall handle

VCA

SBRK

Conclusion

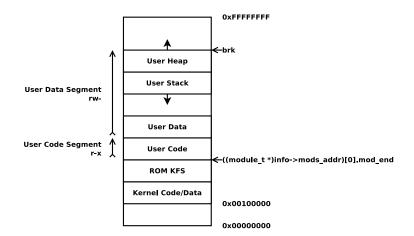


Figure: "Simple" example

LSE Team (EPITA) The K Project April 26, 2017 3 / 13



What is needed

The K Project

LSE Team

Memory layout

Syscall handle

VGA

SBRK

Conclusion

For every segments

- Find enough space with:
 - Multiboot's memory map
 - After the last module
- Should not overlap with each other

For the stack segment

■ Should expand down



Sane memory layout (again)

The K Project

LSE Team

Memory layout

Syscall handle

VGA

SBRK

Conclusion

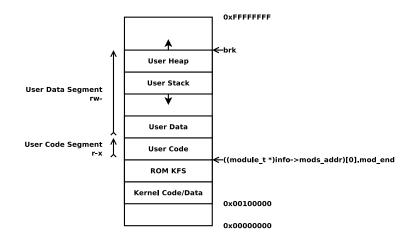


Figure: "Simple" example

LSE Team (EPITA) The K Project April 26, 2017 5 / 13

The K Project

LSE Team

Memor

Syscall handler

System manufe

CDDL

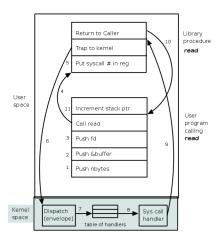


Figure: IA32 read syscall



Syscall Gate

The K Project

LSE Team

Memor layout

Syscall handler

- A unique syscall gate (0x80)
 - int 0x80
- eax: Syscall number
- ebx, ecx, edx: Syscall parameters



Implementation advices

The K Project

LSE Team

Memor layout

Syscall handler

SRRI

- Jump table
- Do not forget to translate the user addresses
- Check for invalid user pointers



VGA Syscalls

The K Project

LSE Team

Memor layout

Syscall handler

VGA

SBRK

Conclusion

setvideo

Swich between VGA text (3h) and graphic mode (13h)

swap_frontbuffer

Loads the user buffer into the graphic framebuffer



Syscall SBRK

The K Project

LSE Team

SBRK

Implementations advices

- man 2 sbrk
- Find some unused memory in the user data segment



Address space advices

The K Project

LSE Team

Conclusion

■ You can load and exec any ROM in "flat" mode.

- You can exec any ROM in kernel land
- GDB will not understand non-zero base address.



Summary

The K Project

LSE Team

Memory layout

Syscall handler

CDDI

Conclusion

SBRK

- Implement the syscall handler
- Wrap and enable each syscall
- Implement the VGA syscalls
- Implement sbrk

Notes

All of these will be needed in order to run the ROMs.



Contact

The K Project

LSE Team

Memory layout

Syscall handler

CDDL

. . . .

- #k (irc.rezosup.org)
- labos.lse with [K] tag
- k[at]lse.epita.fr
- xdbob[at]lse.epita.fr
- pierre.marsais[at]lse.epita.fr