

The K Project

LSE Team

Memory layout

Syscall handler

V G/ (

SBKK

Conclusion

The K Project

LSE Team

EPITA

May 06, 2019

LSE Team (EPITA) The K Project May 06, 2019 1/13



User memory layout

The K Project

LSE Team

Memory layout

Syscall handler

SBRK

Conclusion

Needed segments

- Code
- Data

Optional segments

■ Stack

2/13



Sane memory layout

The K Project

LSE Team

Memory layout

Syscall handle

CDDIZ

Conclusion

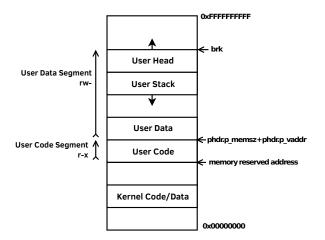


Figure: "Simple" example

LSE Team (EPITA) The K Project May 06, 2019 3/13



What is needed

The K Project

LSE Team

Memory layout

Syscall handle

V/C A

SBR

Conclusion

For every segments

- Find enough space using the given memory allocator
- 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 handler

SBBK

Conclusion

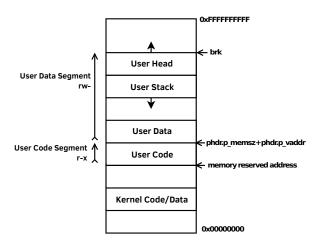


Figure: "Simple" example

LSE Team (EPITA) The K Project May 06, 2019 5 / 13



The K Project

LSE Team

Memory layout

Syscall handler

SBRK

Conclusio

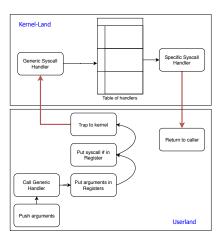


Figure: Syscall Processing



Syscall Gate

The K Project

LSE Team

Memor layout

Syscall handler

VGA

SBRK

Conclusion

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



Implementation advices

The K Project

LSE Team

Syscall handler

■ 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 handle

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

Memor layout

Syscall handle

VGA

SBRK

Conclusion

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 handle

Conclusion

■ 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.

The K Project

LSE Team

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