genua

Techniken in OpenBSD zur Vermeidung von ROP-Angriffen

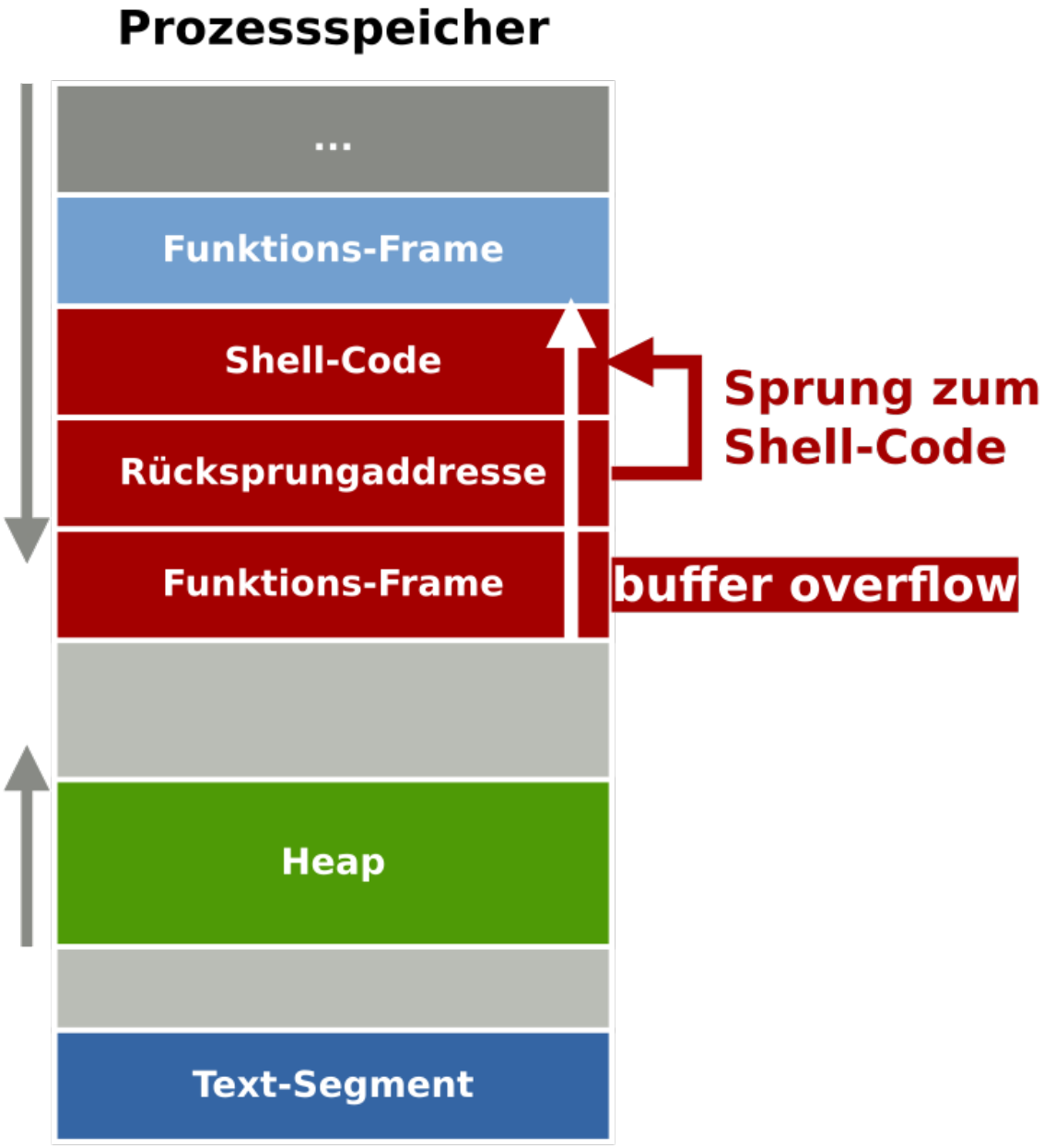
Jan Klemkow

04.09.2018

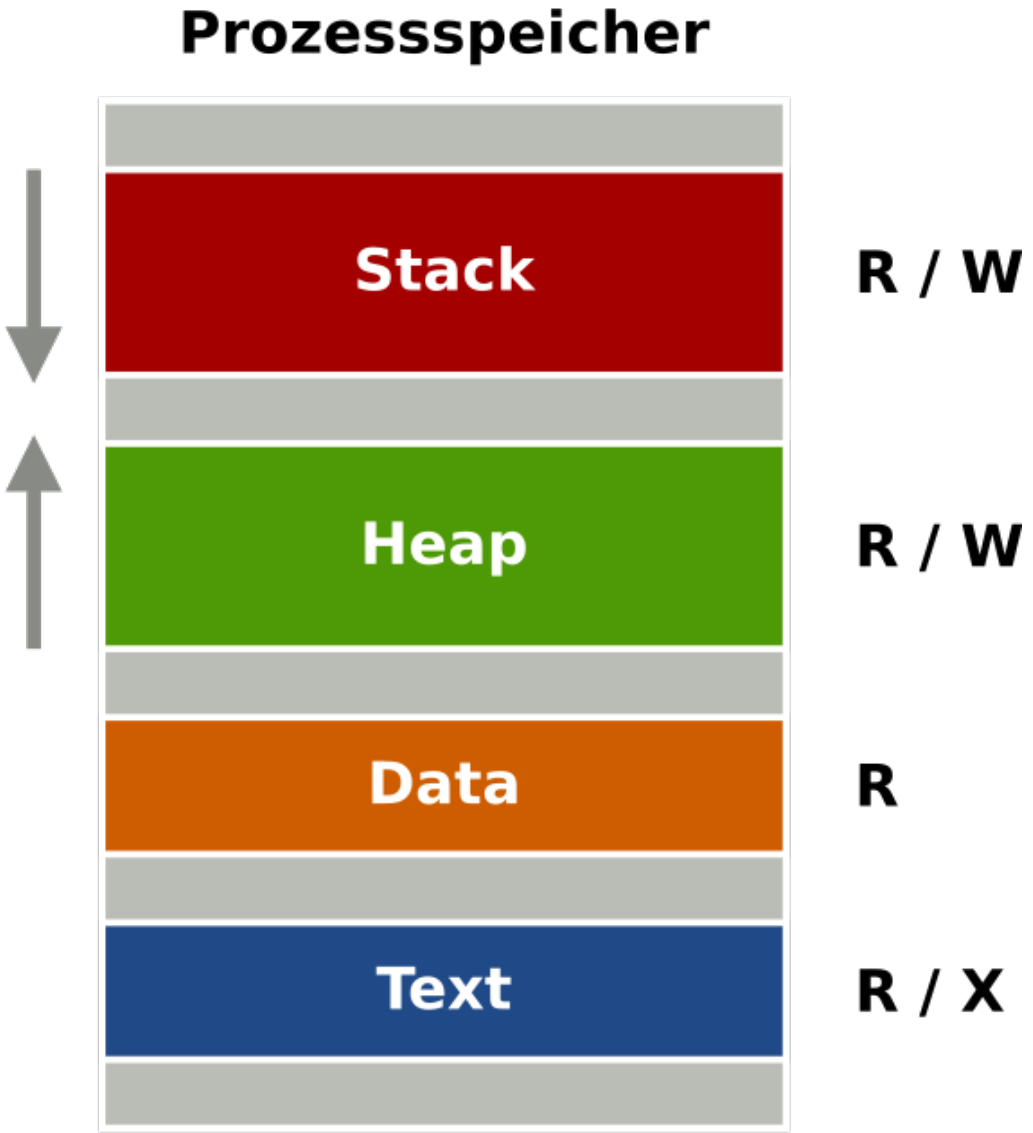
Inhalt

- ROP
- Stack-Canaries
- ASLR
- Trap-Sled
- Signal-ROP

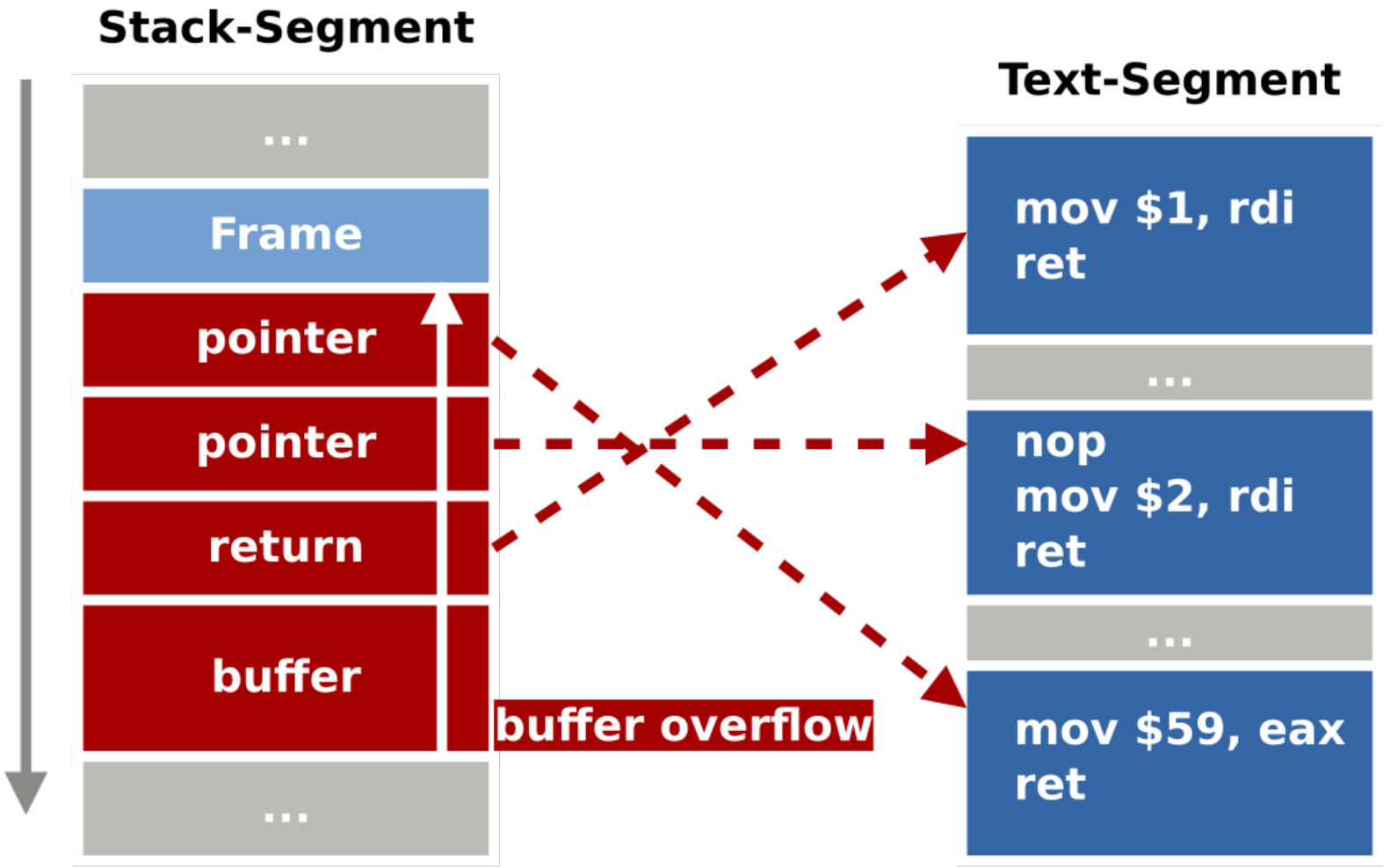
Buffer-Overflow mit Shell-Code



Data-Execution-Prevention

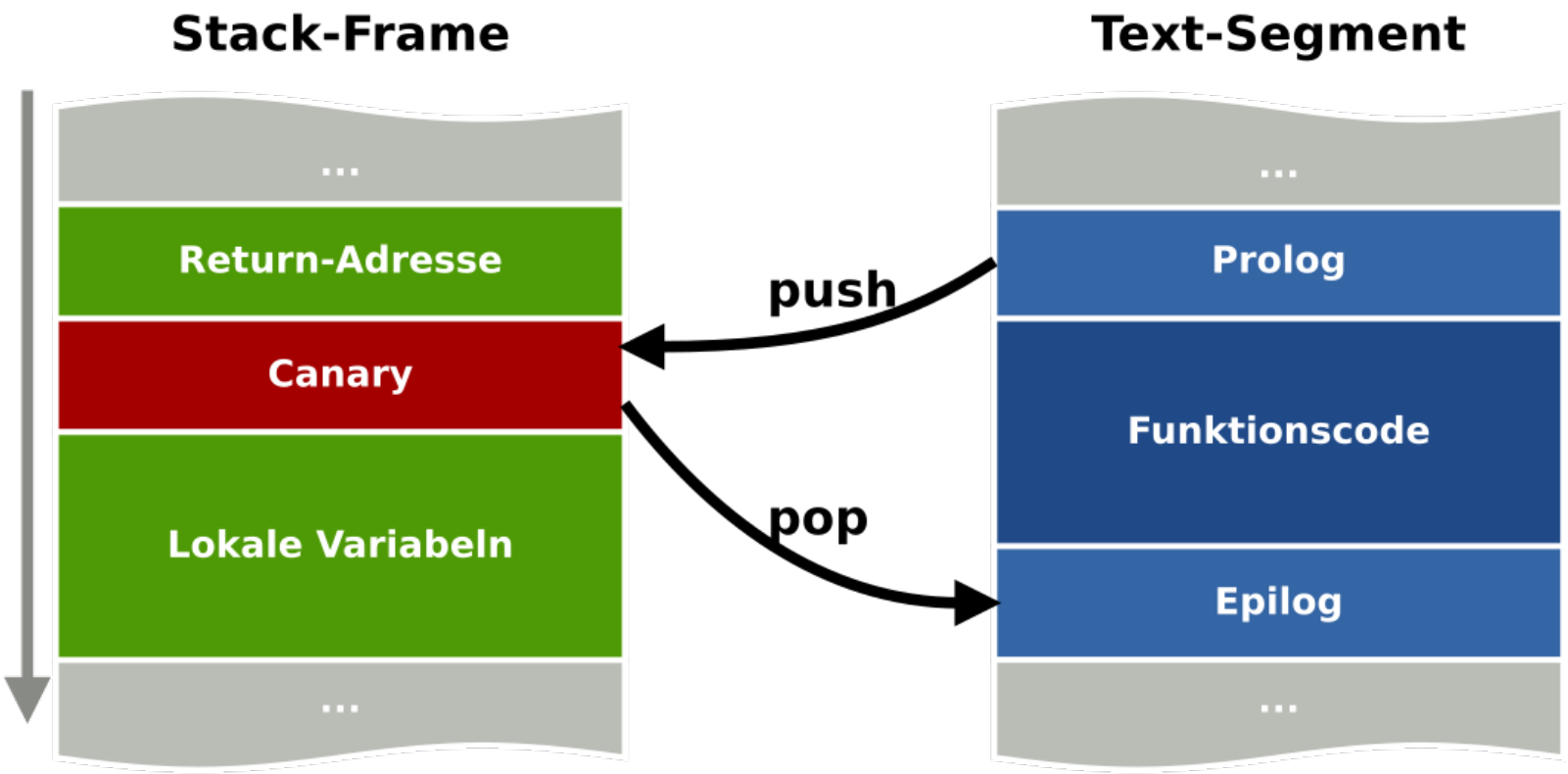


Buffer-Overflow mit ROP



Verbesserte Stack-Canaries

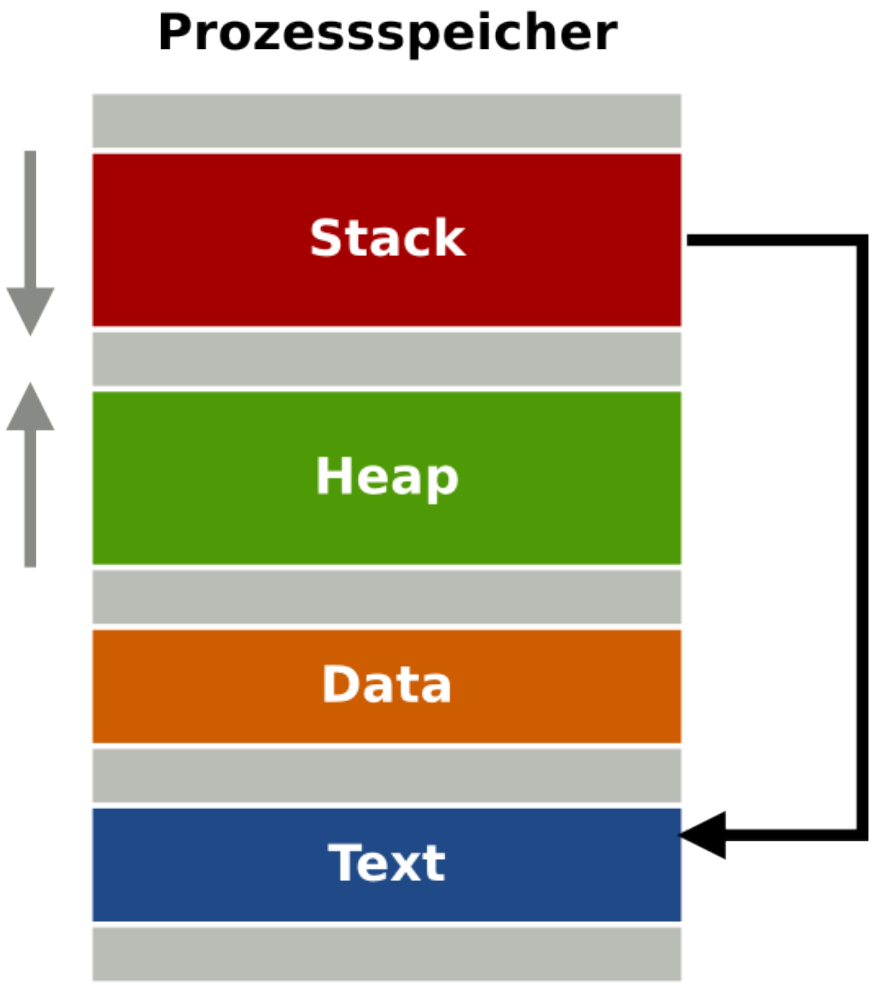
Verbesserte Stack-Canaries



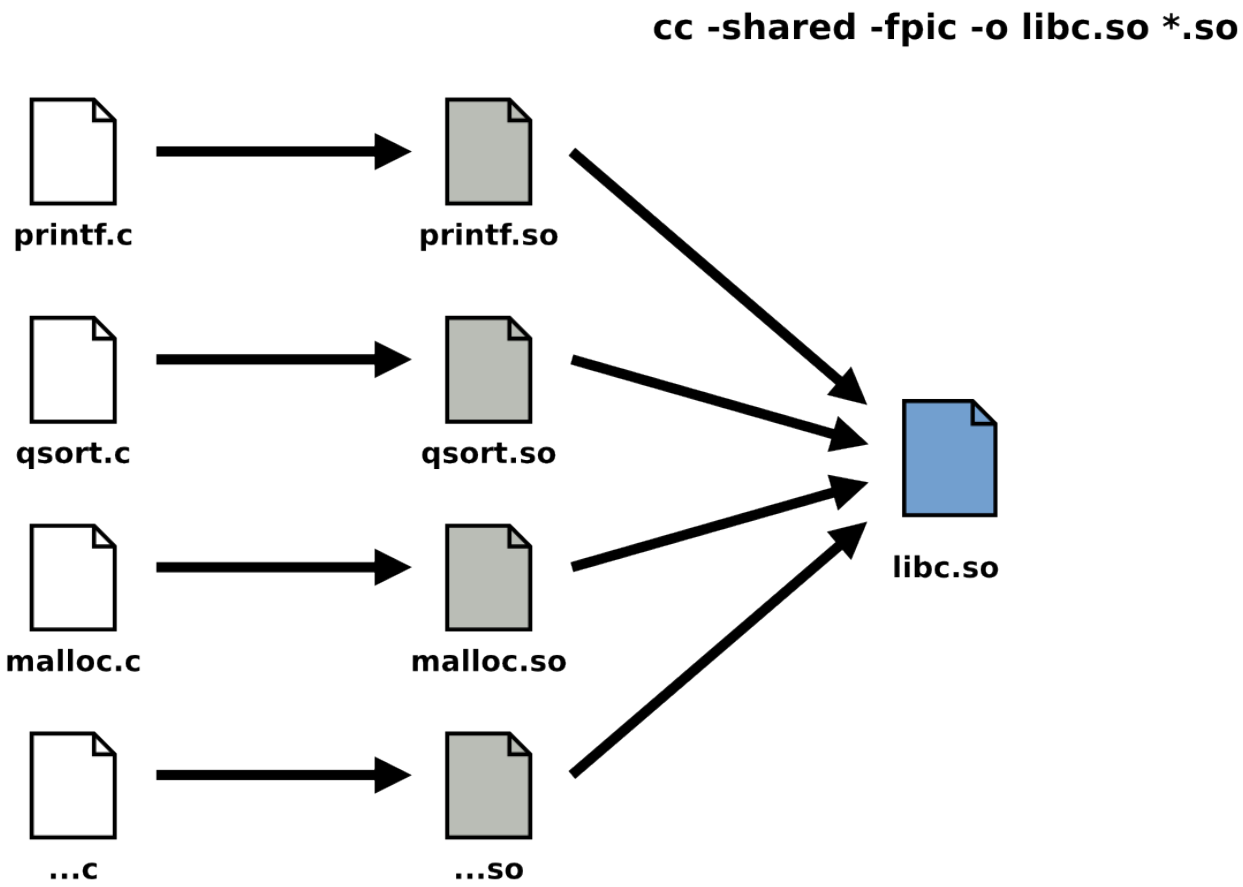
genua

Verbessertes ASLR

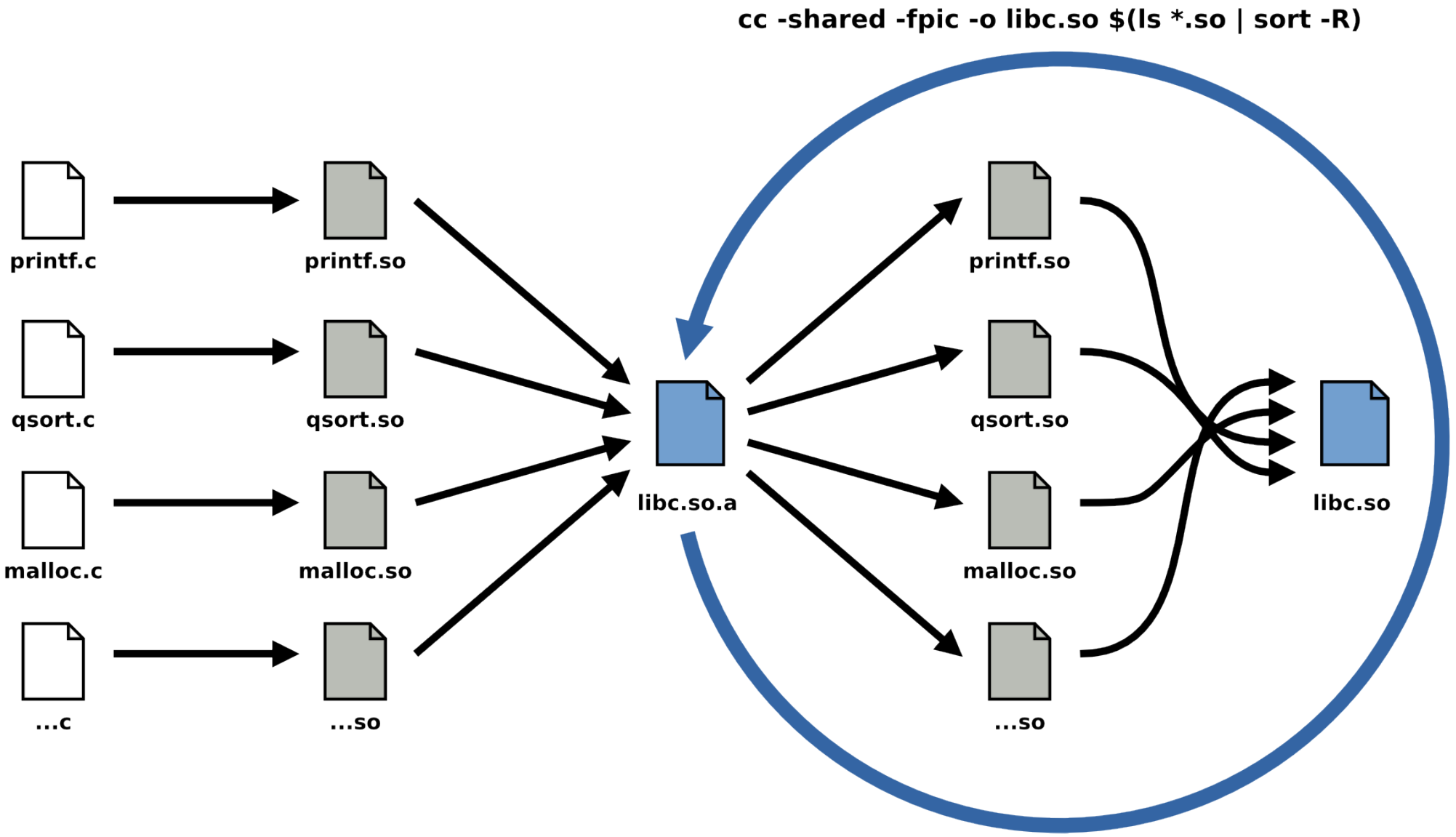
Return to LibC



Return to LibC

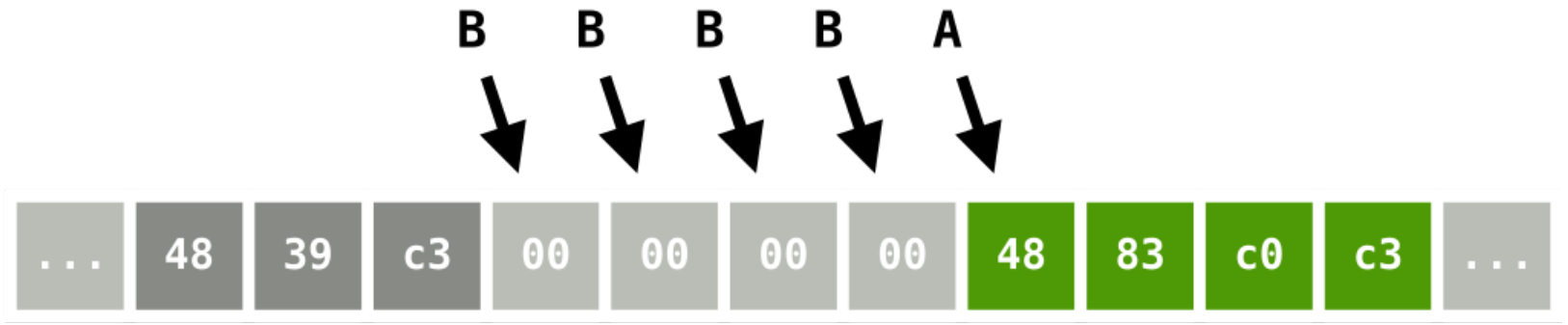


Anti - Return to LibC



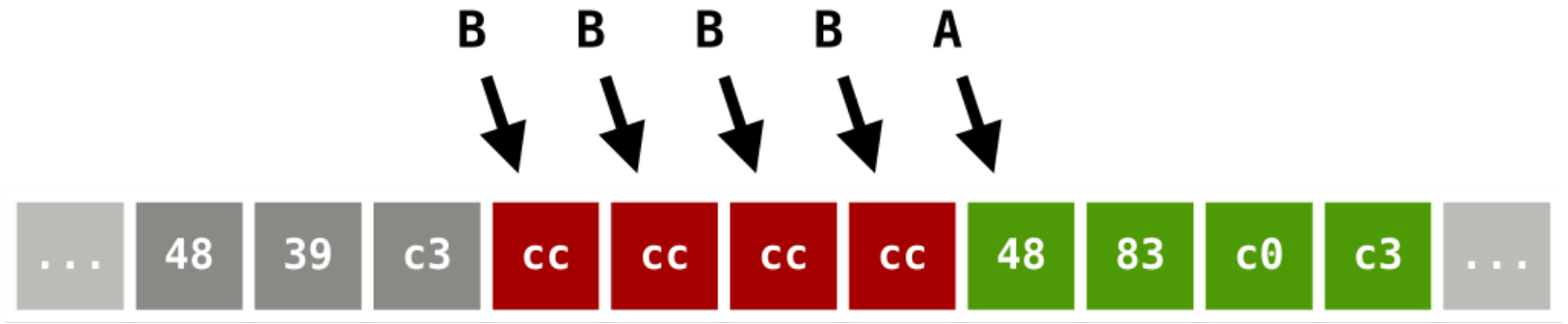
Trap-Sled

NOP-Sled



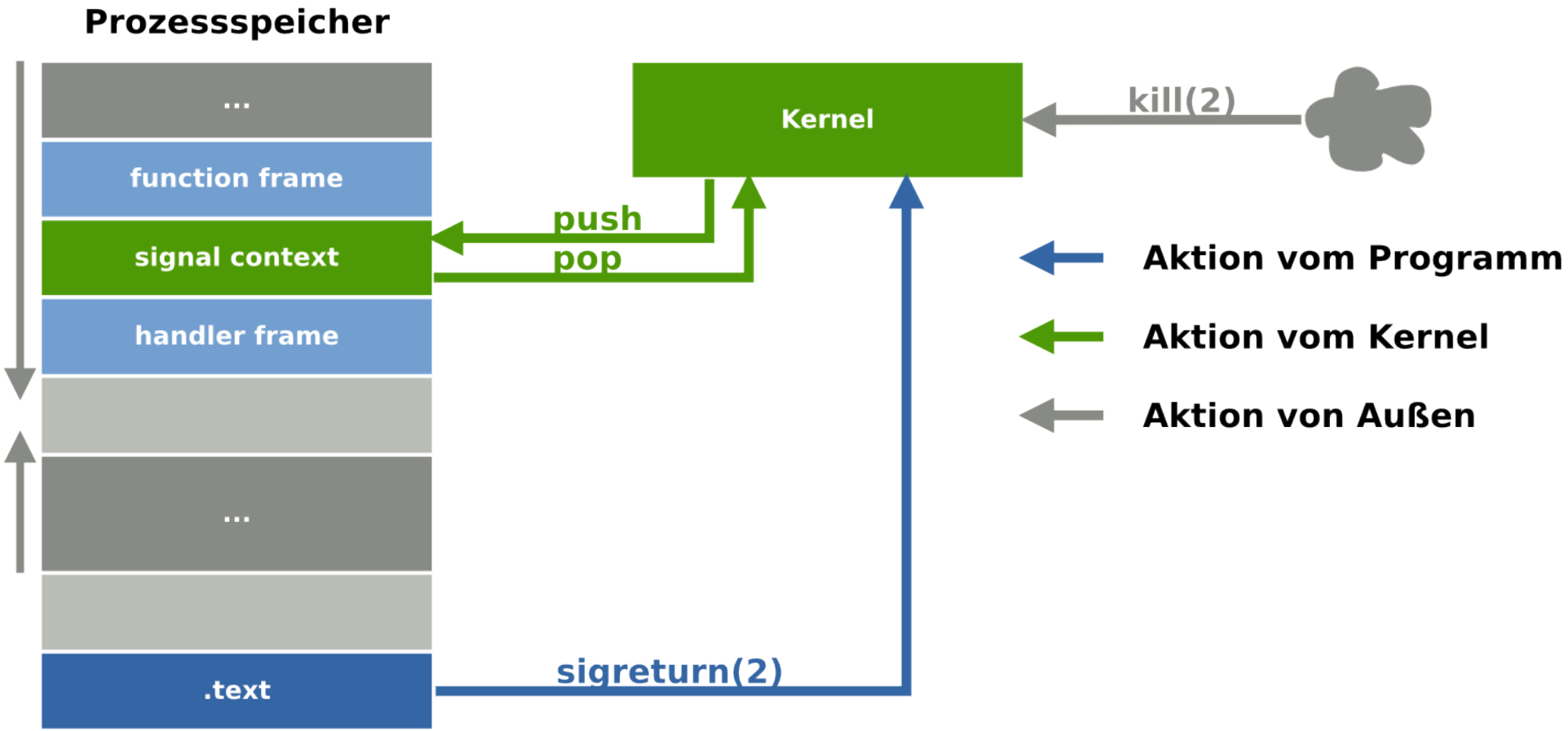
Trap-Sled

genua

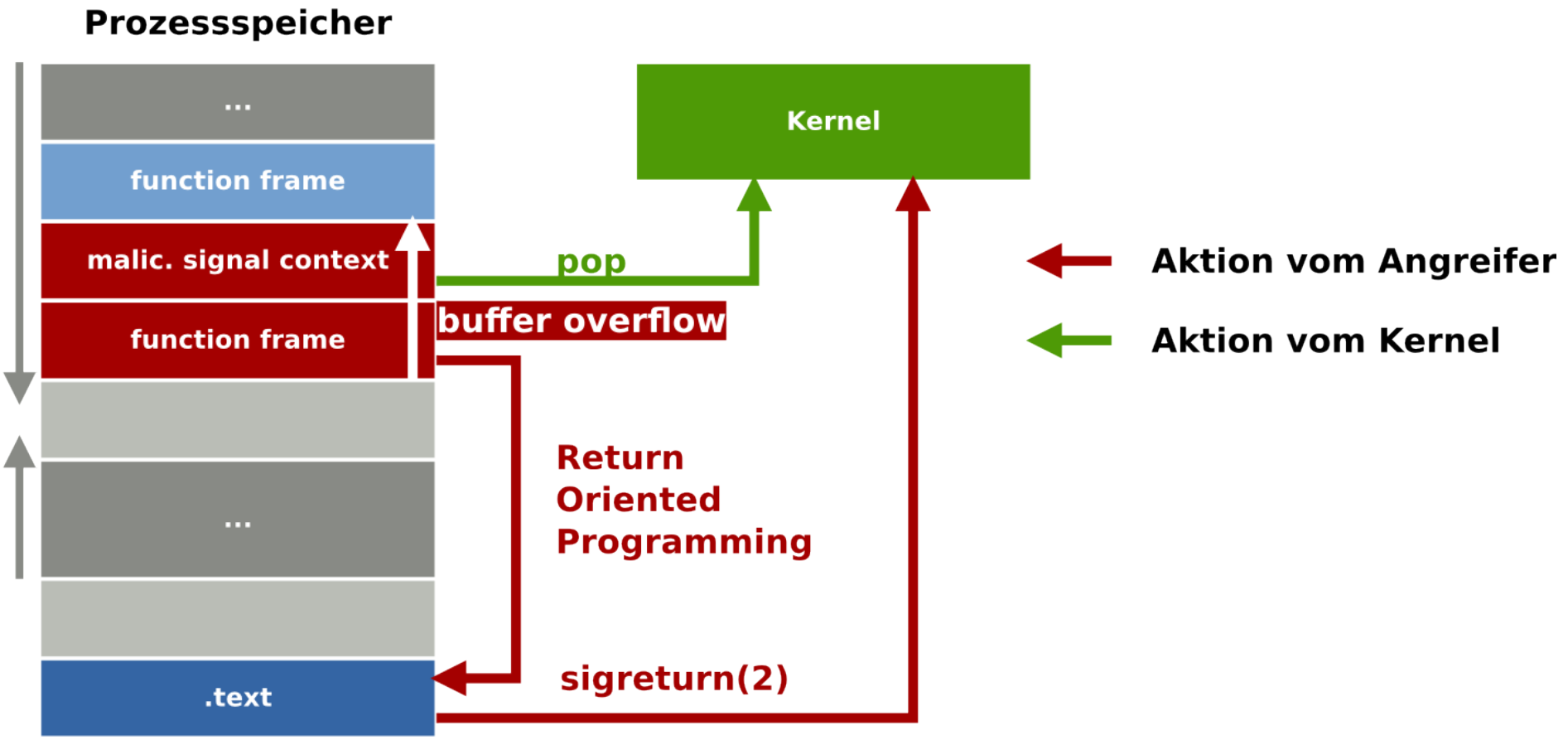


Signal Return-Oriented-Programming

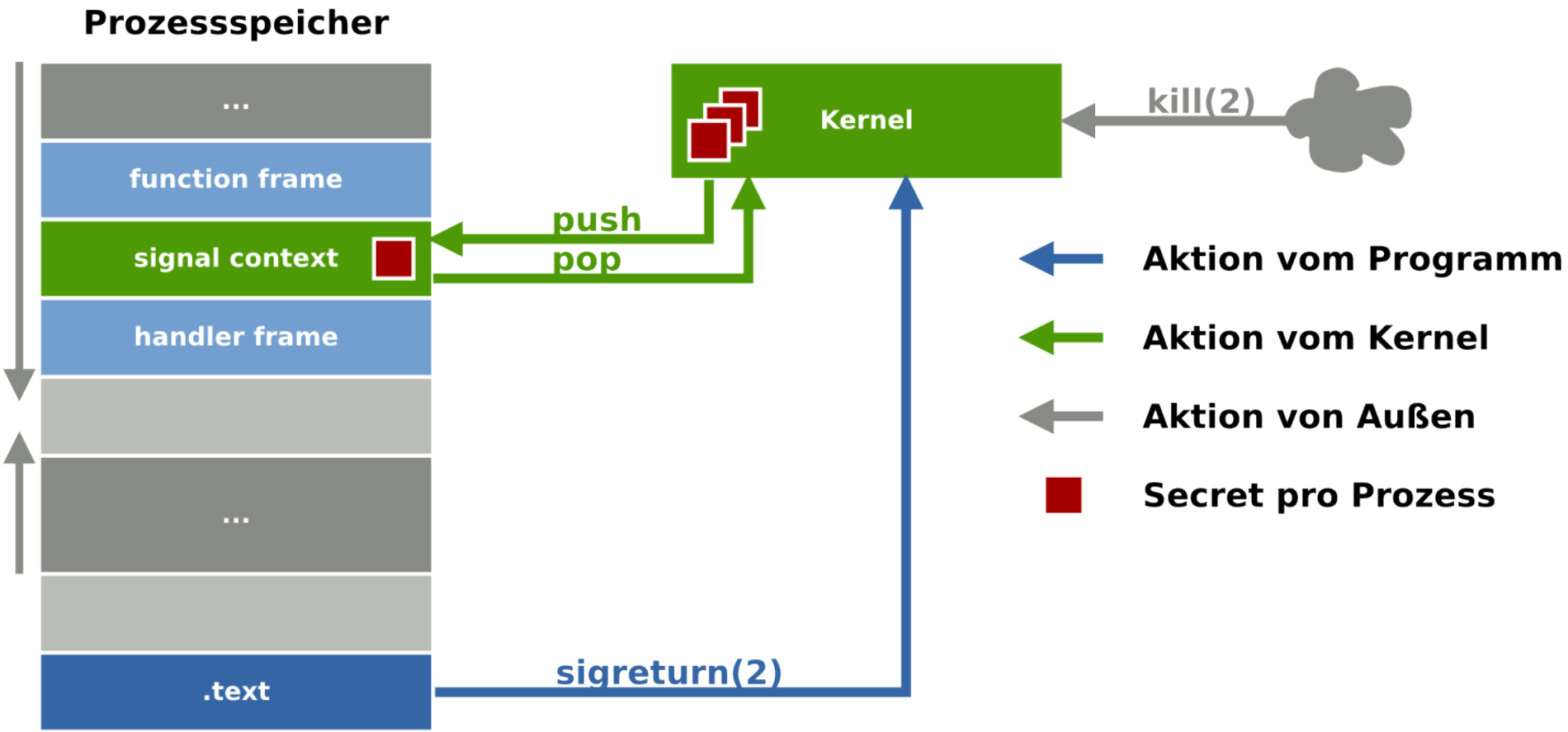
Signal Return Oriented Programming



Signal Return Oriented Programming



Signal Return Oriented Programming



Fragen?