genua

Umsetzung moderner Speicherschutztechniken in OpenBSD

Jan Klemkow

18.05.2017

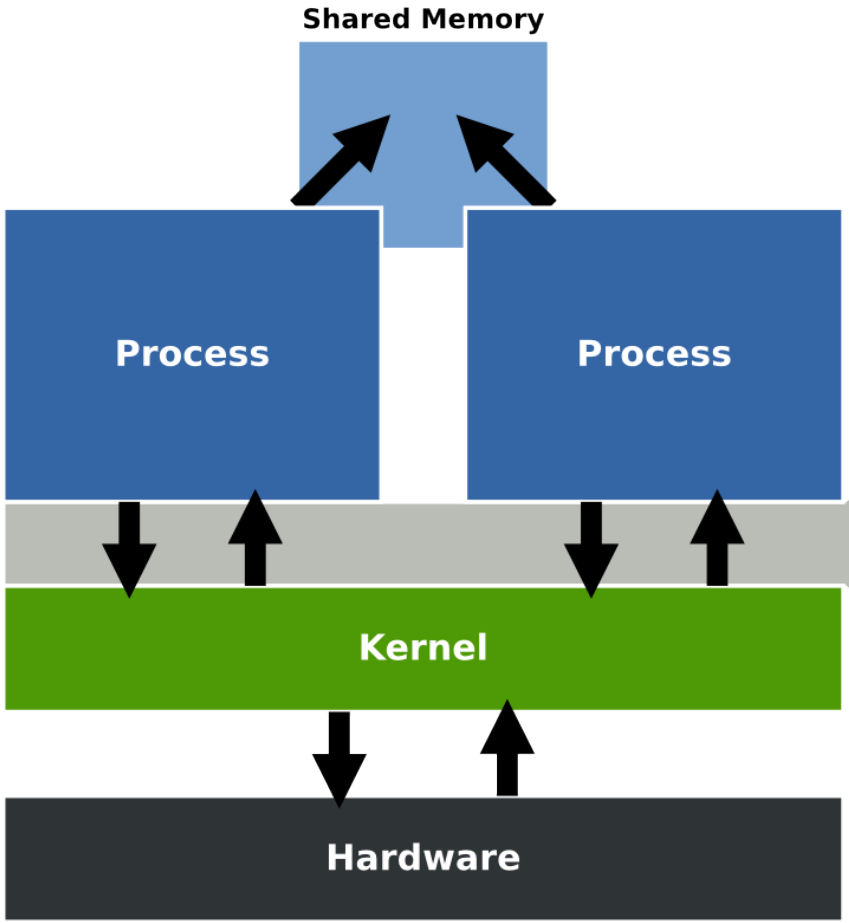
genua

- pledge(2)
- Data-Execution-Prevention
- Return-to-LibC
- fork(2) + exec(2)
- Signal-ROP

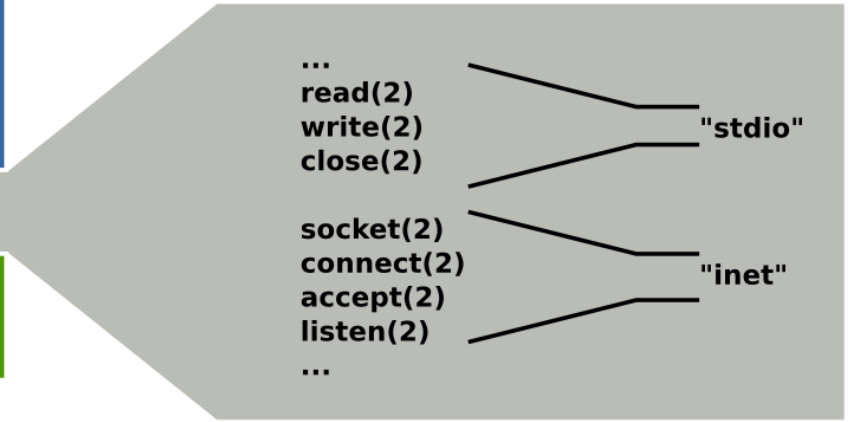
genua

pledge(2)

pledge(2)




```
pledge("stdio net", NULL);
pledge("stdio", NULL);
pledge("", NULL);
```

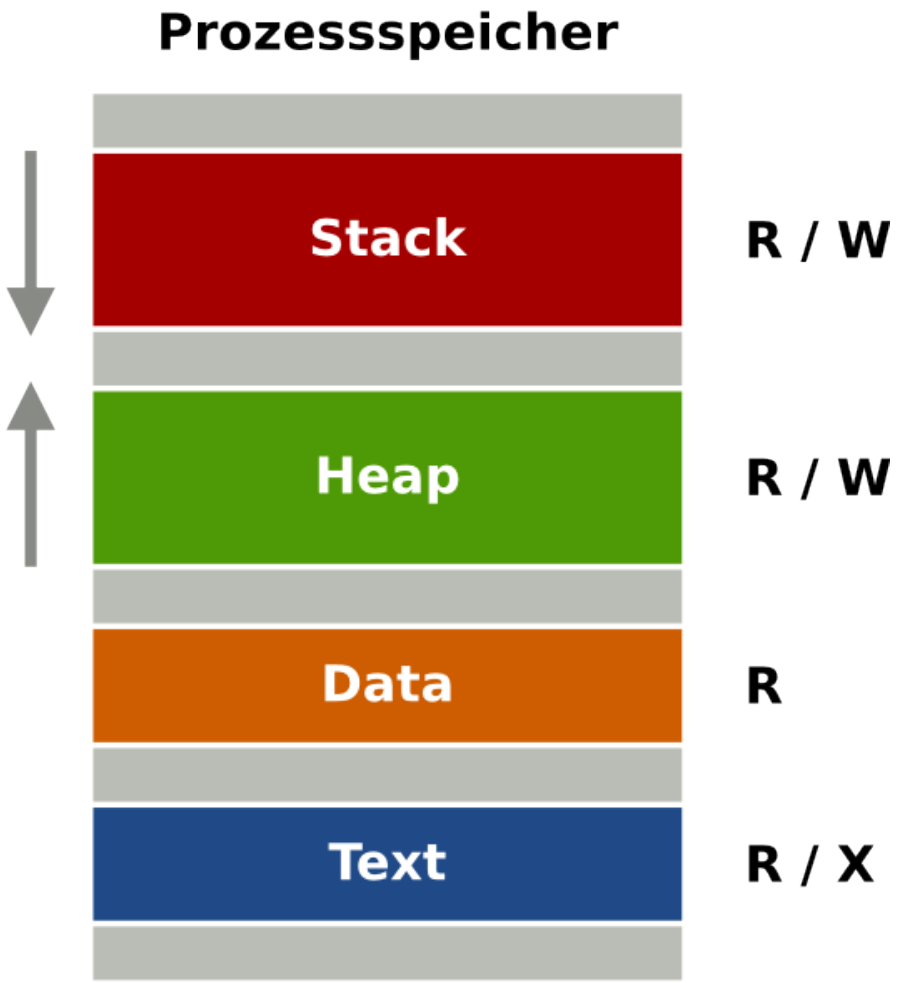


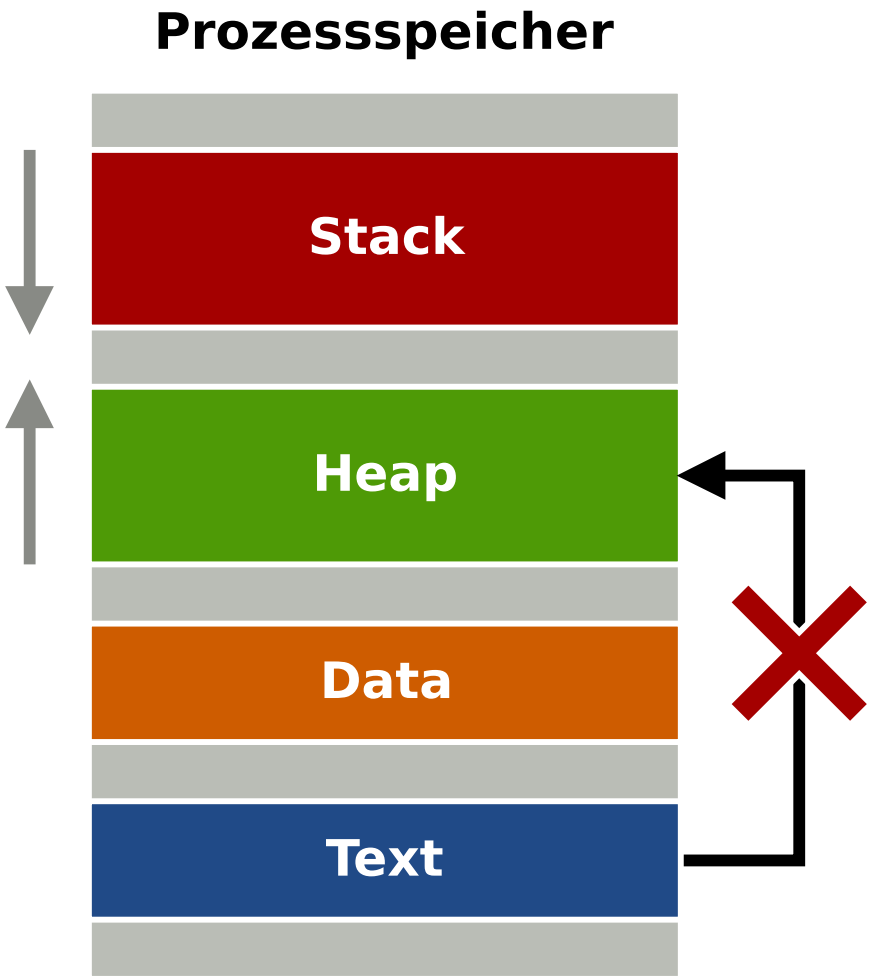
```
char *paths[] = {
        "/var/www/",
        "/home/alice/www",
        "/home/bob/www",
        NULL
};

pledge("stdio rpath inet", paths);
```

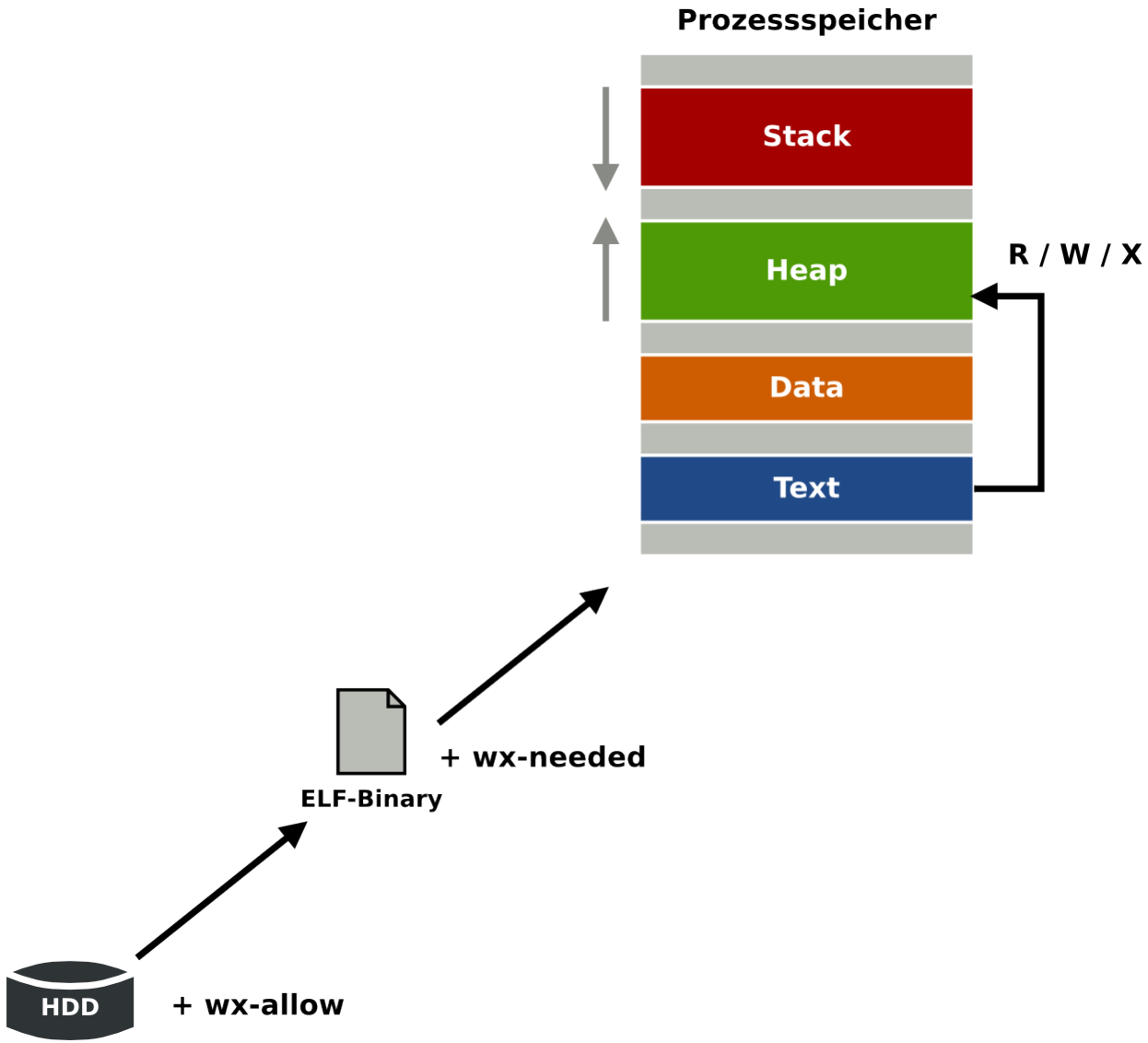
genua

Data-Execution-Prevention

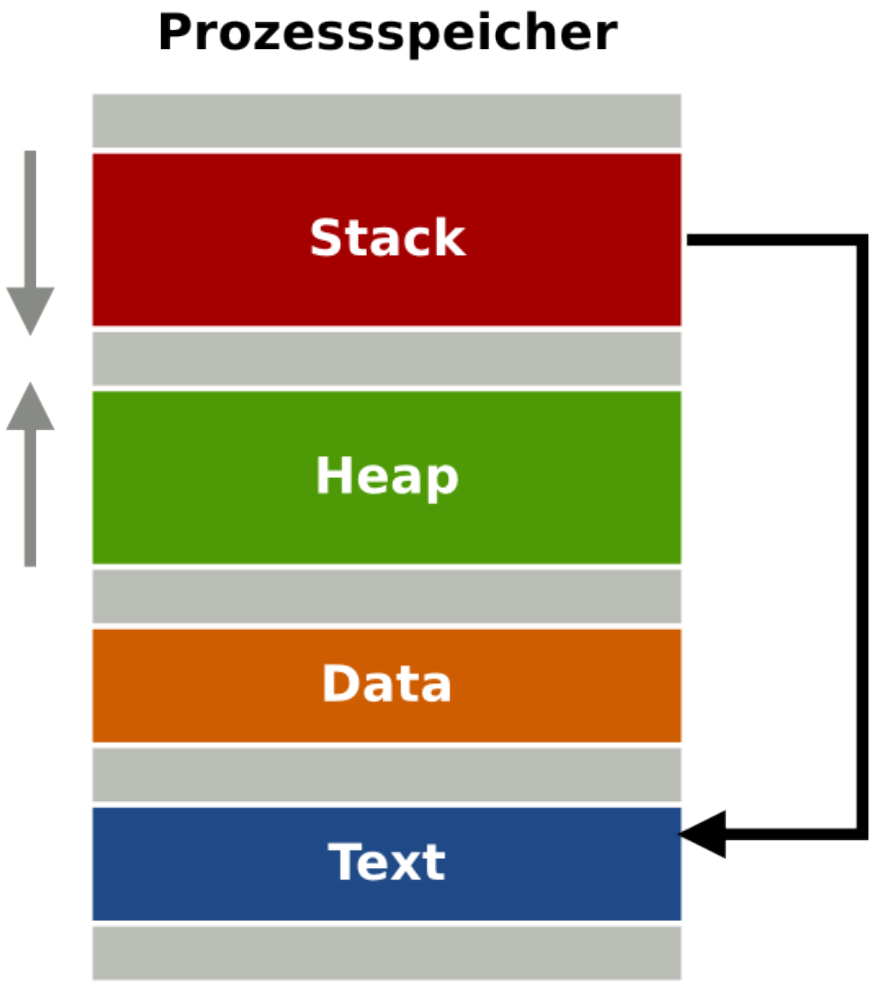

Prozessspeicher
Stack
R / W
Heap
R / W
Data
R
Text
R / X


Prozessspeicher
Stack
Heap
Data
Text

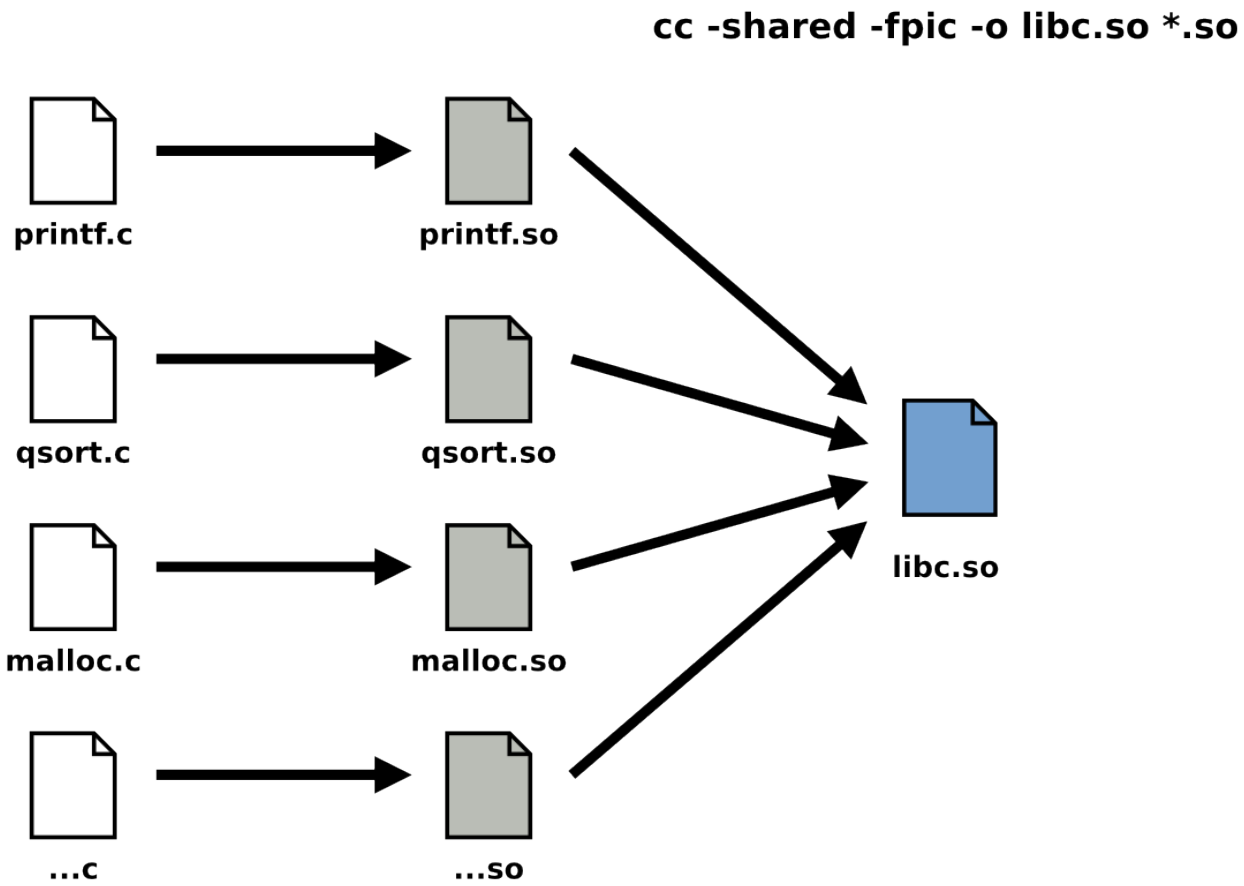
Data-Execution-Prevention



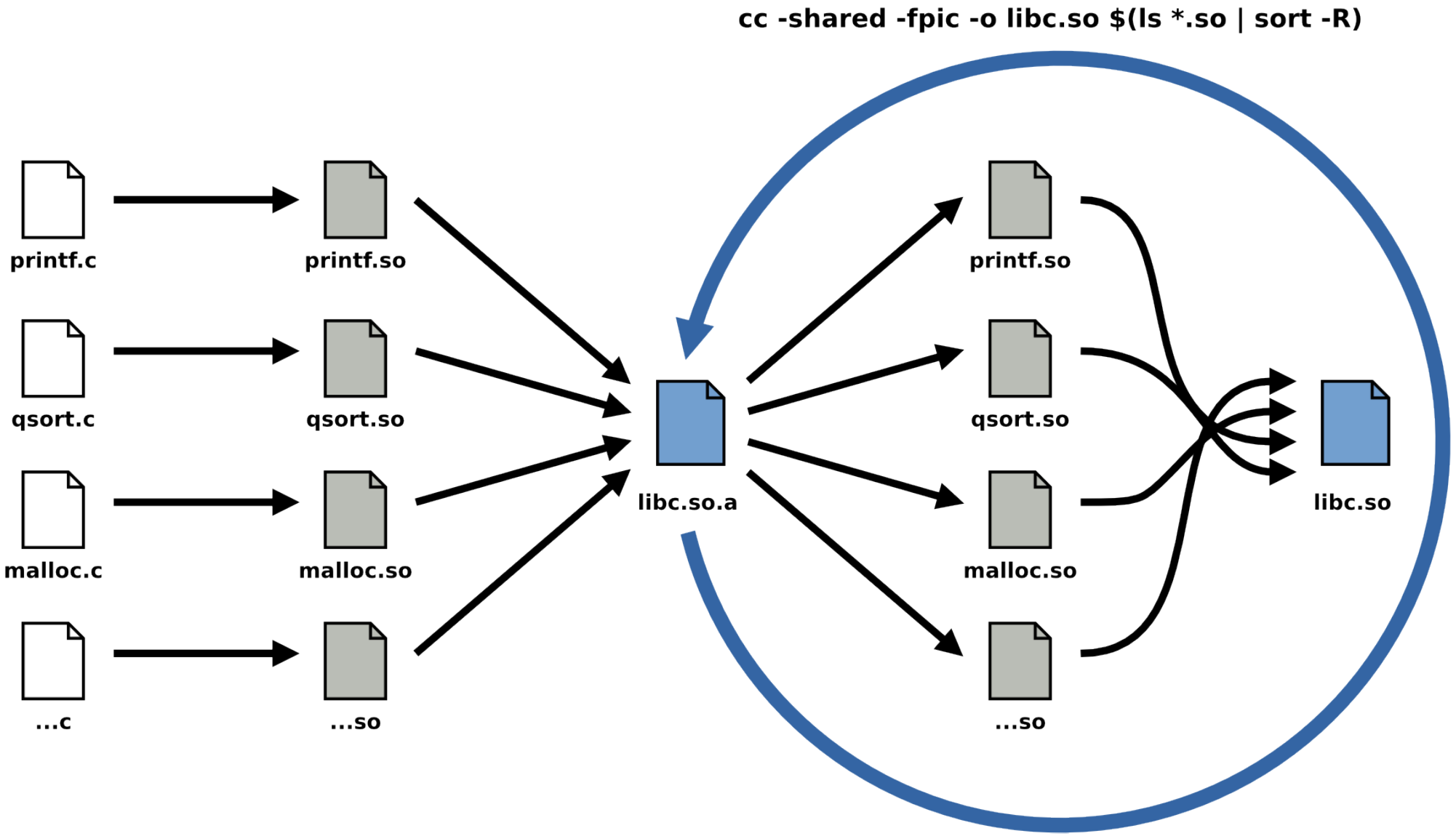
Return-to-LibC


Prozessspeicher
Stack
Heap
Data
Text

Return to LibC

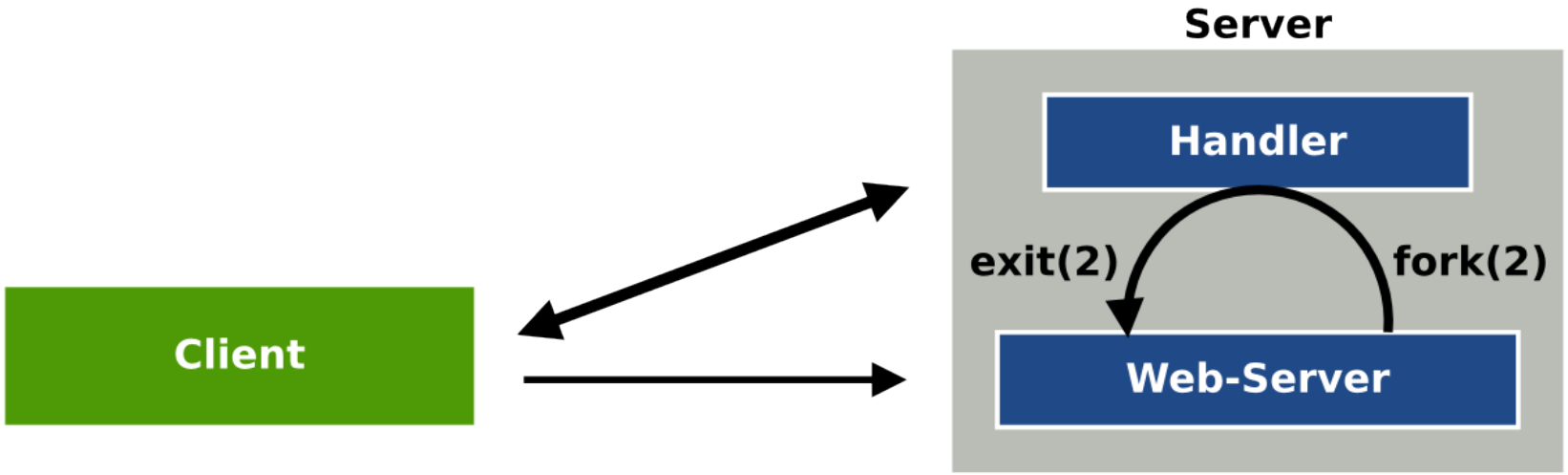


Anti - Return to LibC

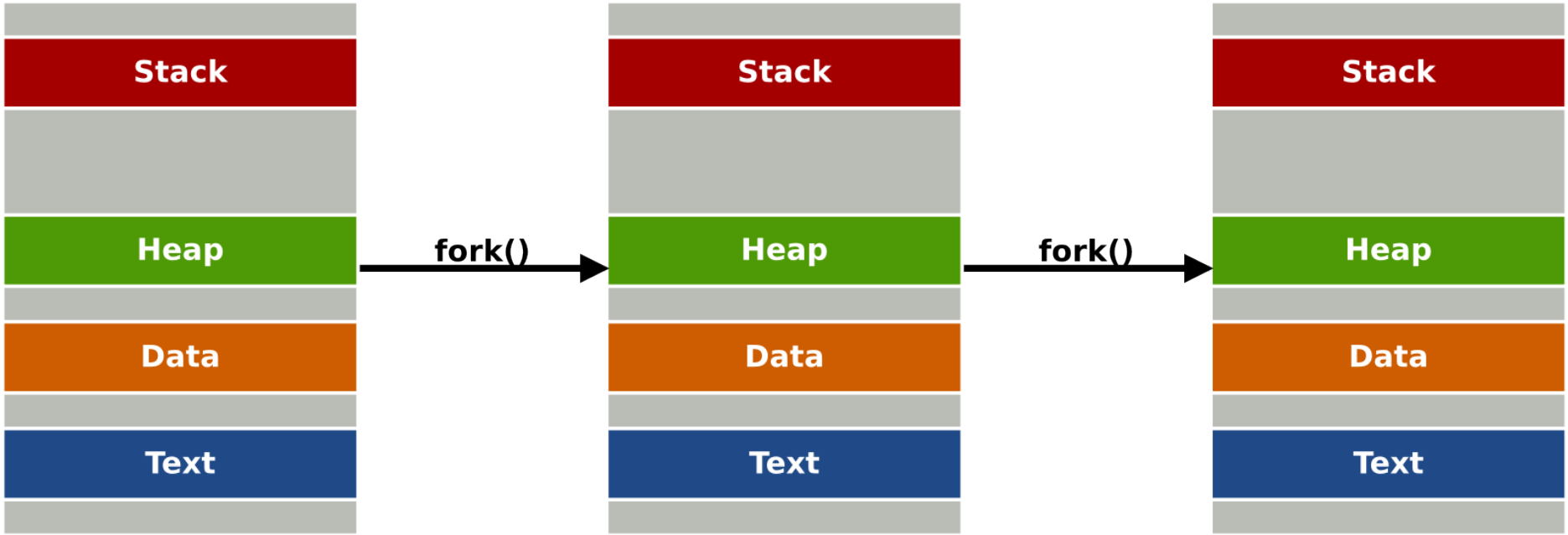


fork(2) + exec(2)

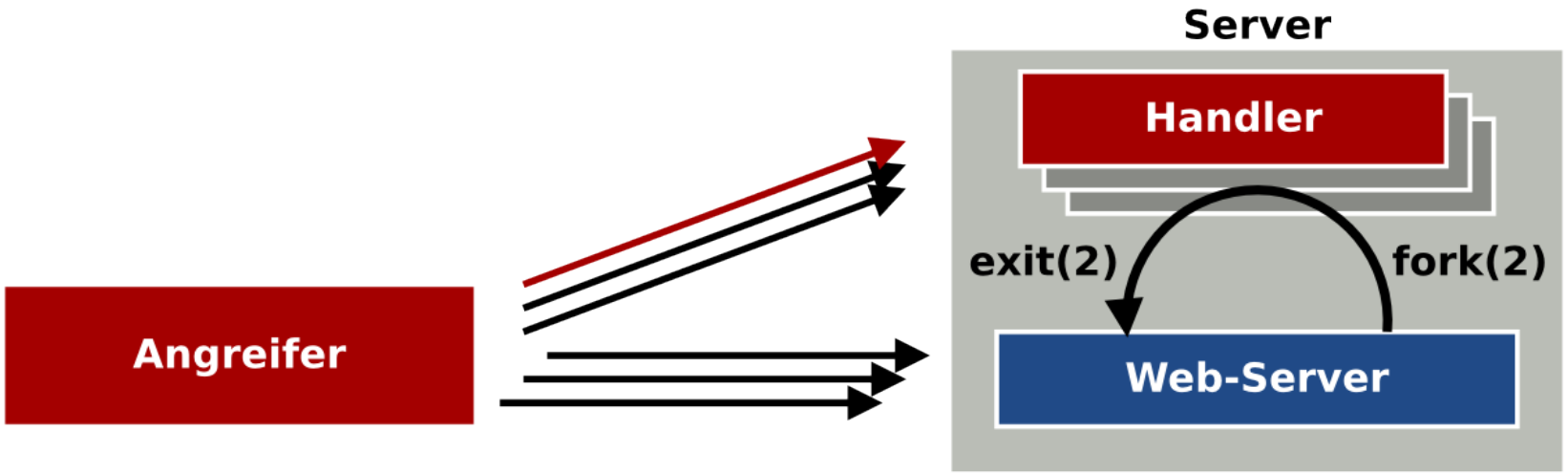
fork(2) + exec(2)



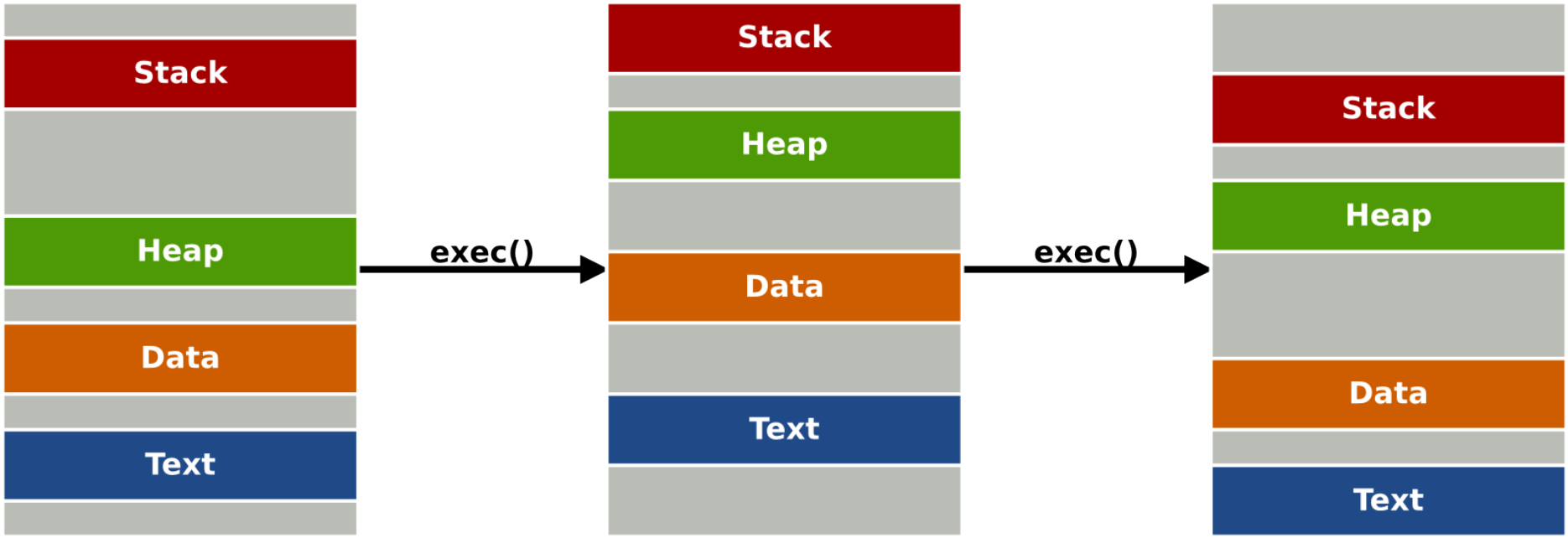
fork(2) + exec(2)


Stack
Heap
Data
Text
fork()
Stack
Heap
Data
Text
fork()
Stack
Heap
Data
Text

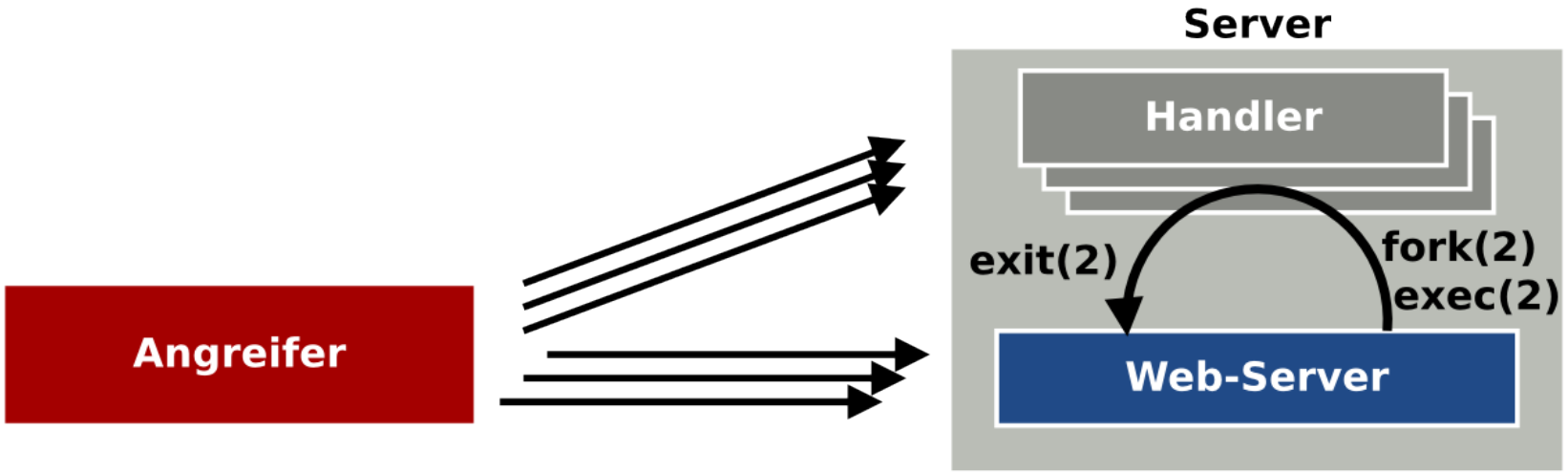
fork(2) + exec(2)



fork(2) + exec(2)


Stack
Heap
Data
Text
exec()
Stack
Heap
Data
Text
exec()
Stack
Heap
Data
Text

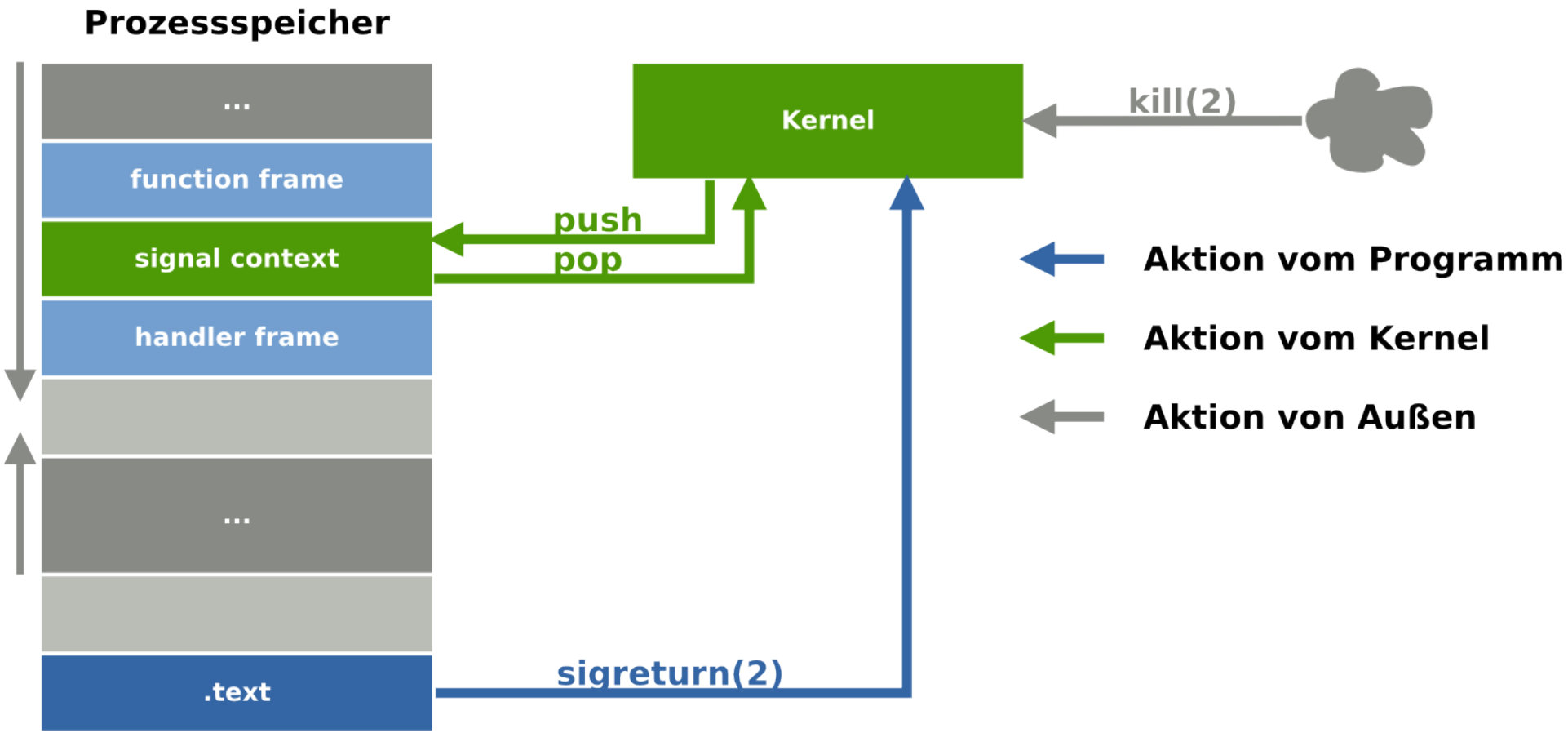
fork(2) + exec(2)



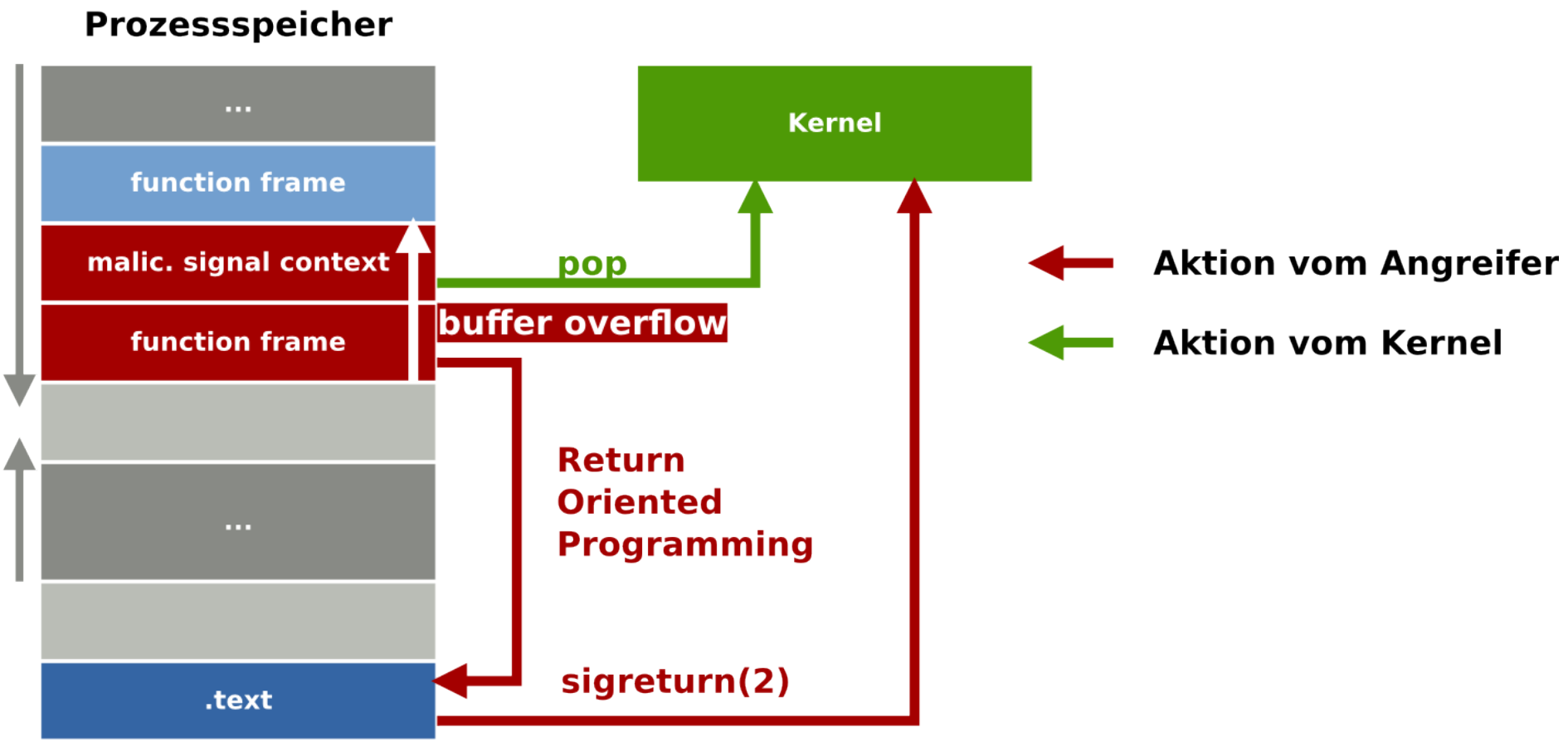
genua

Signal Return-Oriented-Programming

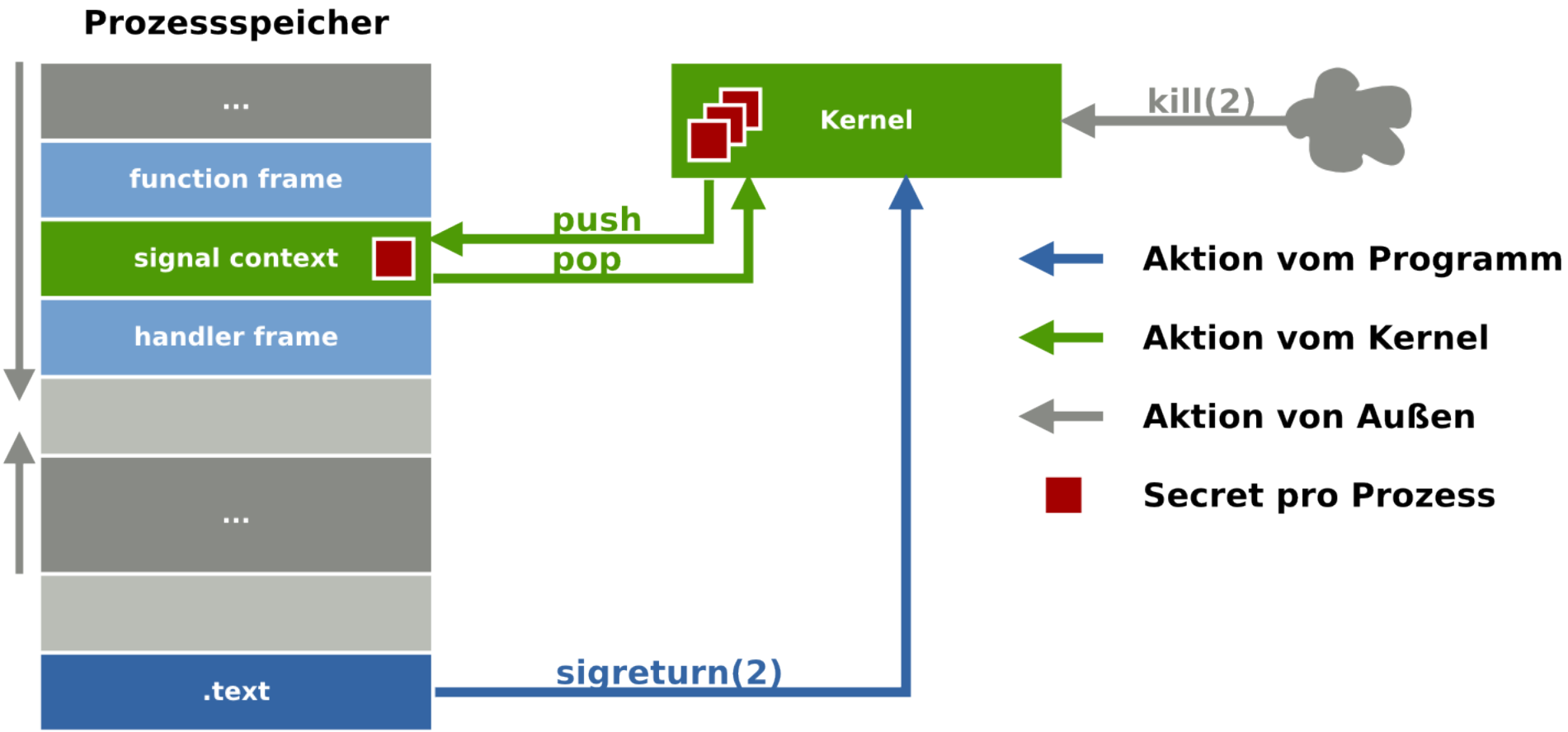
Signal Return Oriented Programming



Signal Return Oriented Programming



Signal Return Oriented Programming

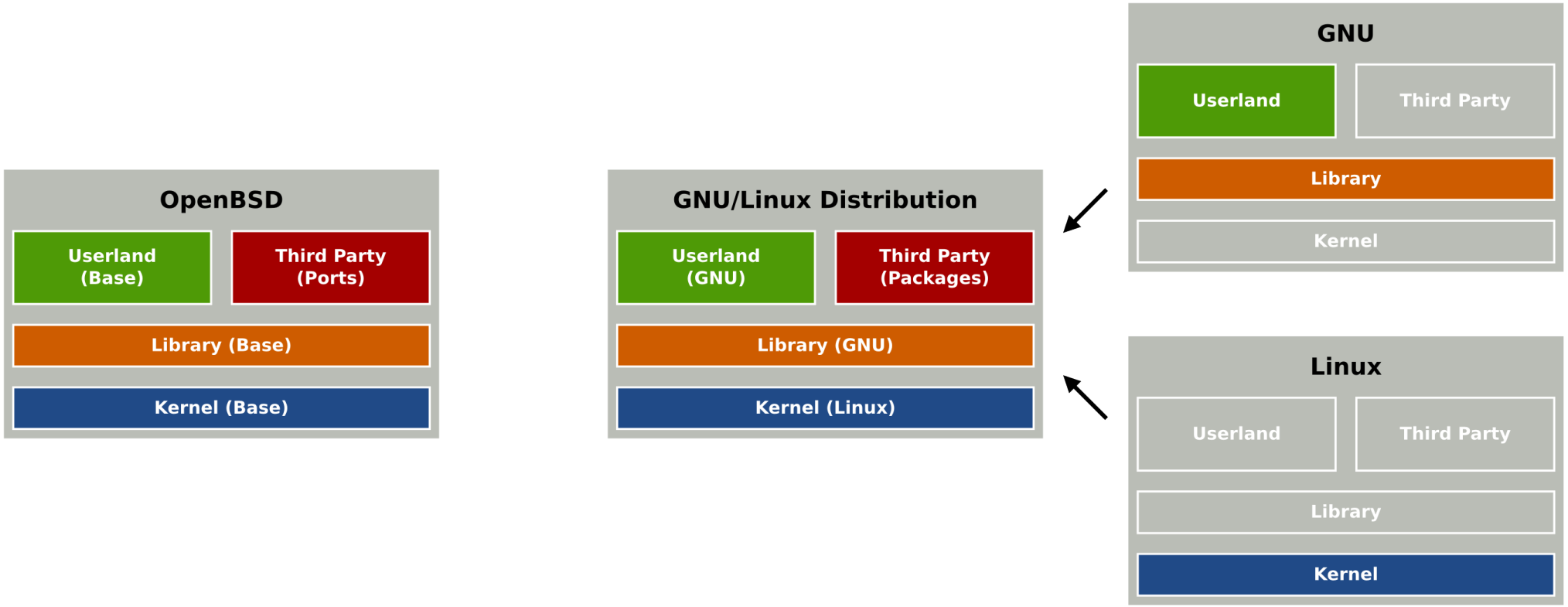


Auswirkungen auf das Open-Source-Ökosystem

genua

- **Software-Abstürze**
- **Lokales Patching**
- **Kommunikation mit Upstream**
- **9.000 Ports**
  - OpenOffice
  - Firefox

Auswirkungen



Fragen?