

Dynamic Linkers Are the Narrow Waist of Operating Systems

PLOS'23

Charly Castes

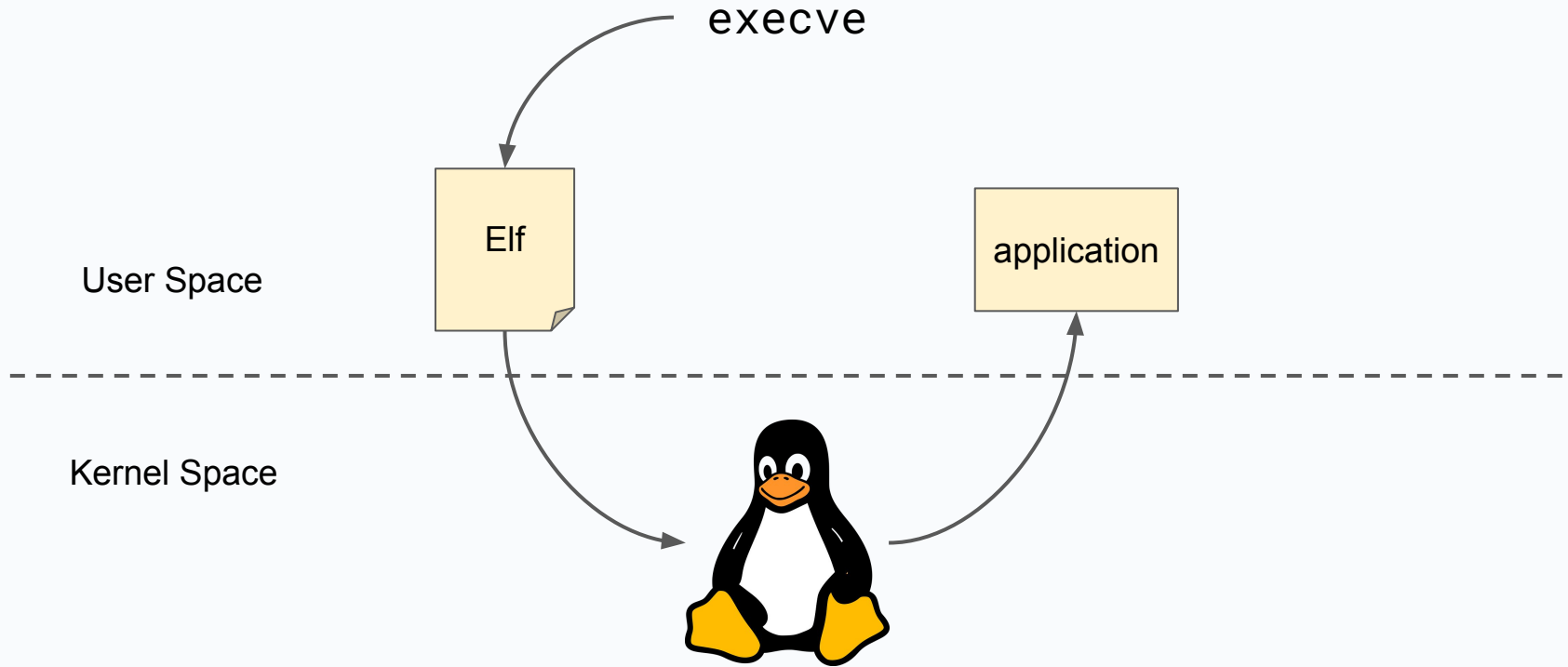
EPFL

Adrien Ghosn

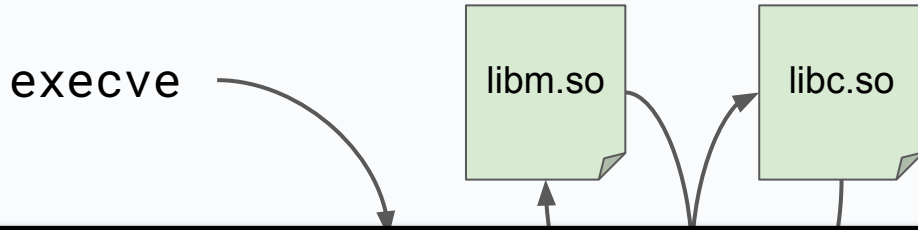
A Microsoft Azure

The dynamic linker needs some love

How do we load programs?

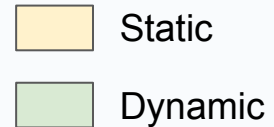
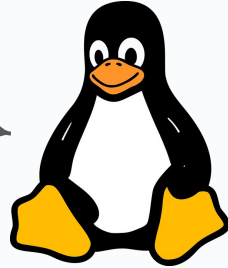


How do we load programs?



The dynamic linker interposes on all dynamic program instantiation

Kernel Space



Dynamic programs are the norm



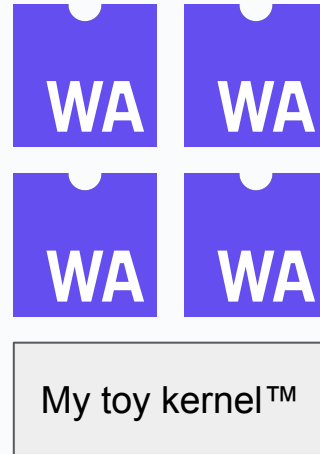
99% of ubuntu executables are dynamic programs



Why should we care?

Here is why I care

- Software Isolated Processes



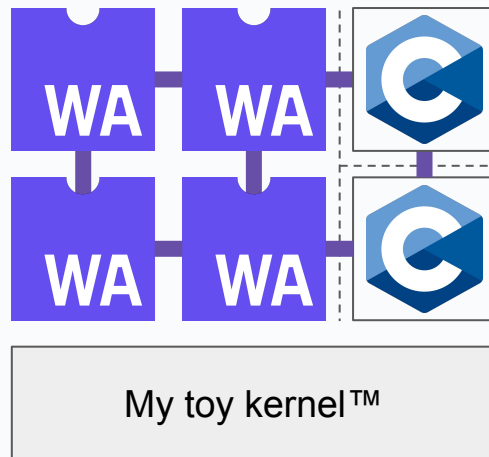
Here is why I care

- Software Isolated Processes
- Strongly typed Interfaces



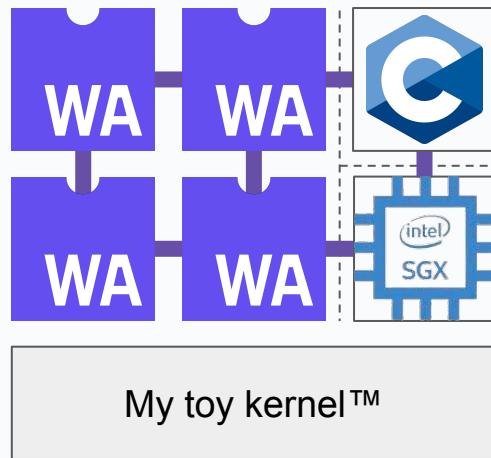
Here is why I care

- Software Isolated Processes
- Strongly typed Interfaces
- Unix processes, with sandboxing



Here is why I care

- Software Isolated Processes
- Strongly typed Interfaces
- Unix processes, with sandboxing
- Enclaves?



There was only two problems:

Implementing all
of this will take
me forever

No one will ever
use my system

Systems Software Research is Irrelevant



Systems software research has become a sideline to the excitement in the computing industry.

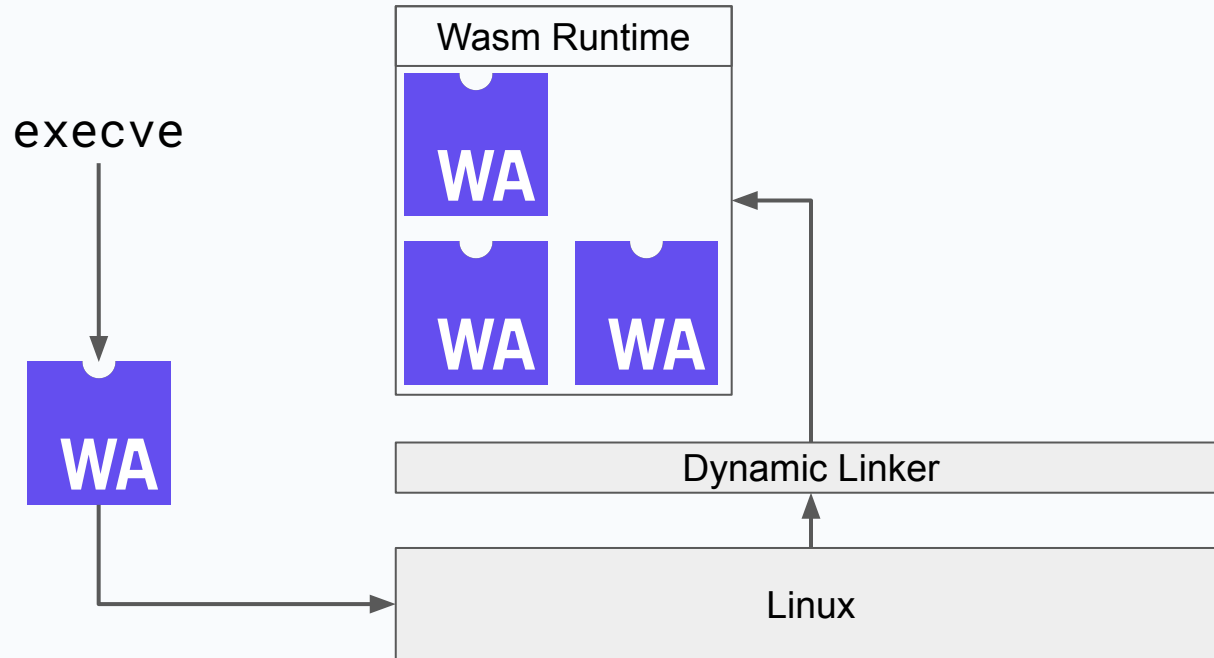
Rob Pike - *Feb 21, 2000*

But what if I could implement my system on Linux, and keep all the existing programs?

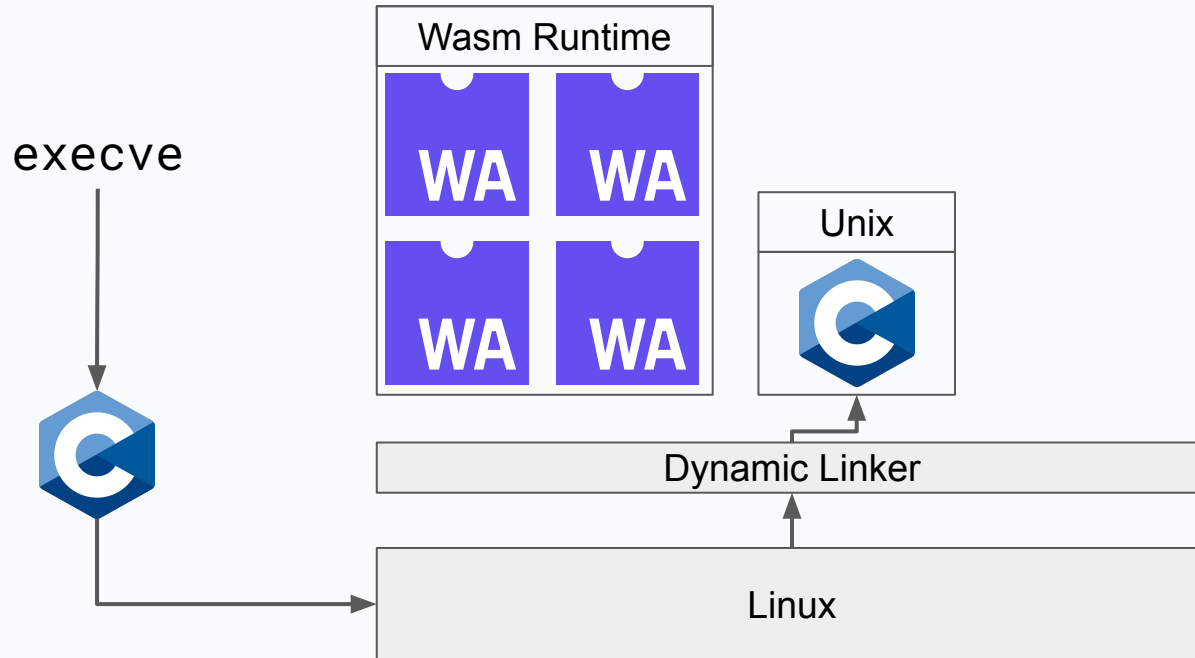
Then maybe people would use it...

✨ Dynamic Linker ✨

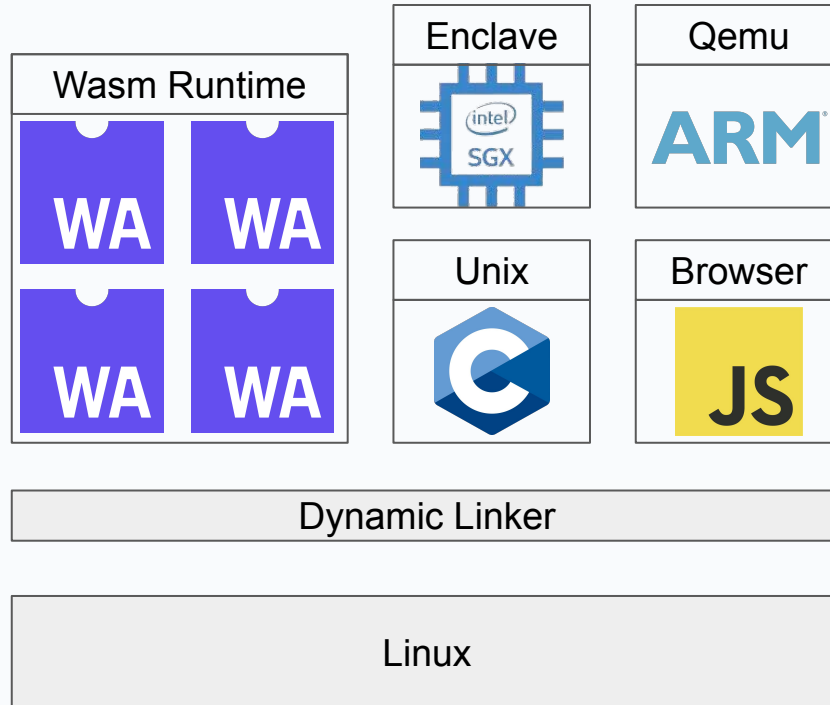
Using the dynamic linker



Using the dynamic linker



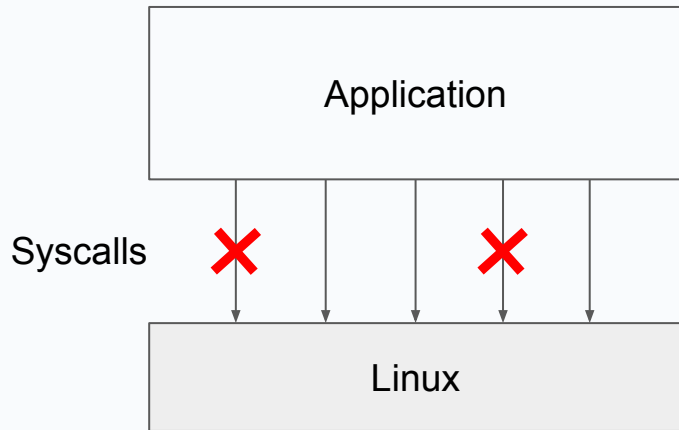
Using the dynamic linker



One more example

Scaling seccomp filters

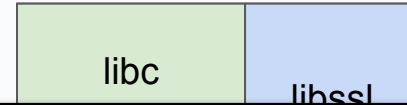
Seccomp is a mechanism to filter system calls



Scaling seccomp filters

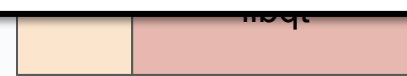
Extensive research to create

good seccomp filters, but:



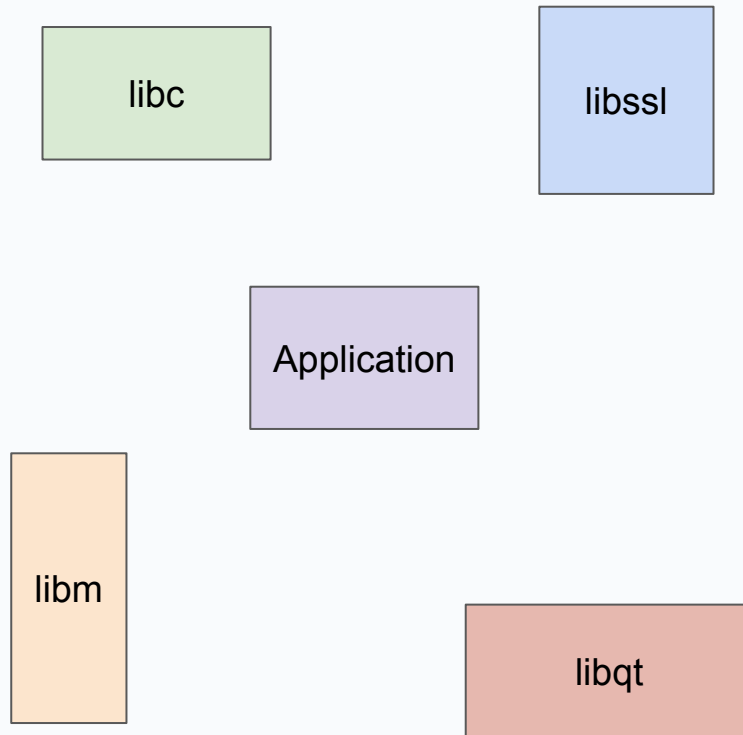
Can we make seccomp filters scale to a whole distribution?

→ have to re-compute all filters when a library change

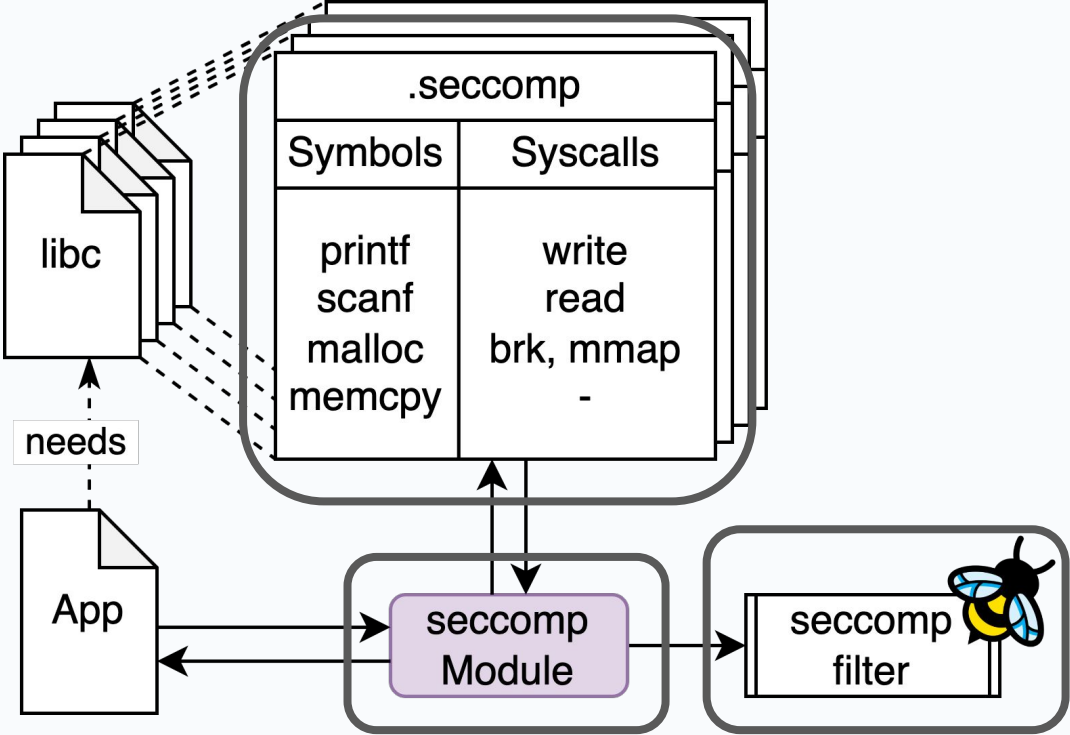


Scaling seccomp filters

We can compute per-library filters, and combine them transparently!



Example: Scaling seccomp filters

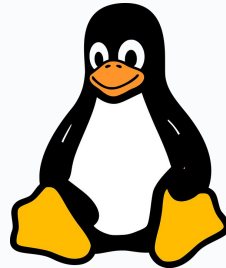
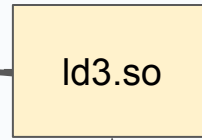
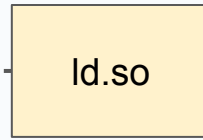
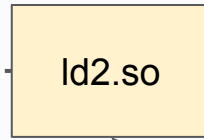


The dynamic linker is a narrow waist

And we can leverage it to evolve our systems

Conclusion

60,000+
packages



And even
add more

30,000,000+
LoC