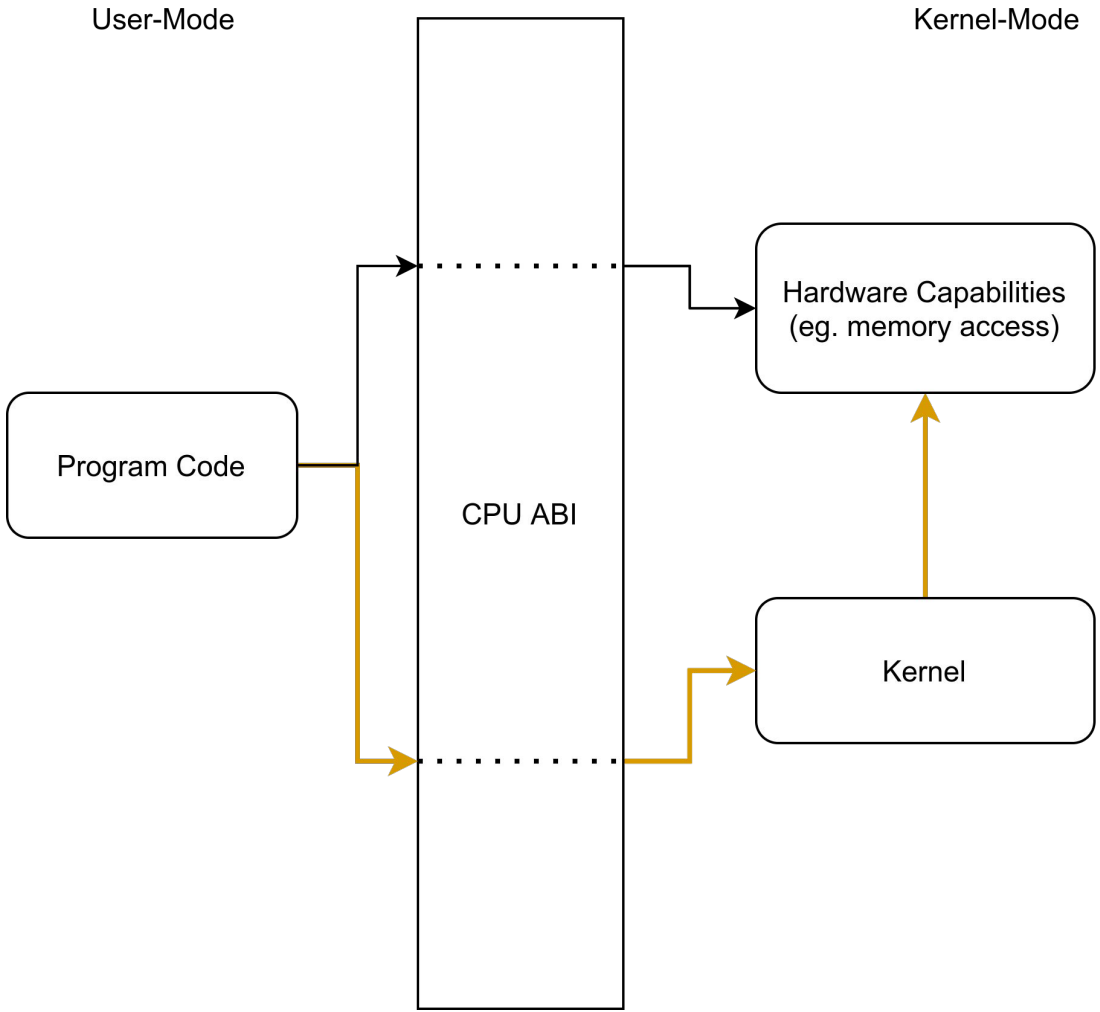
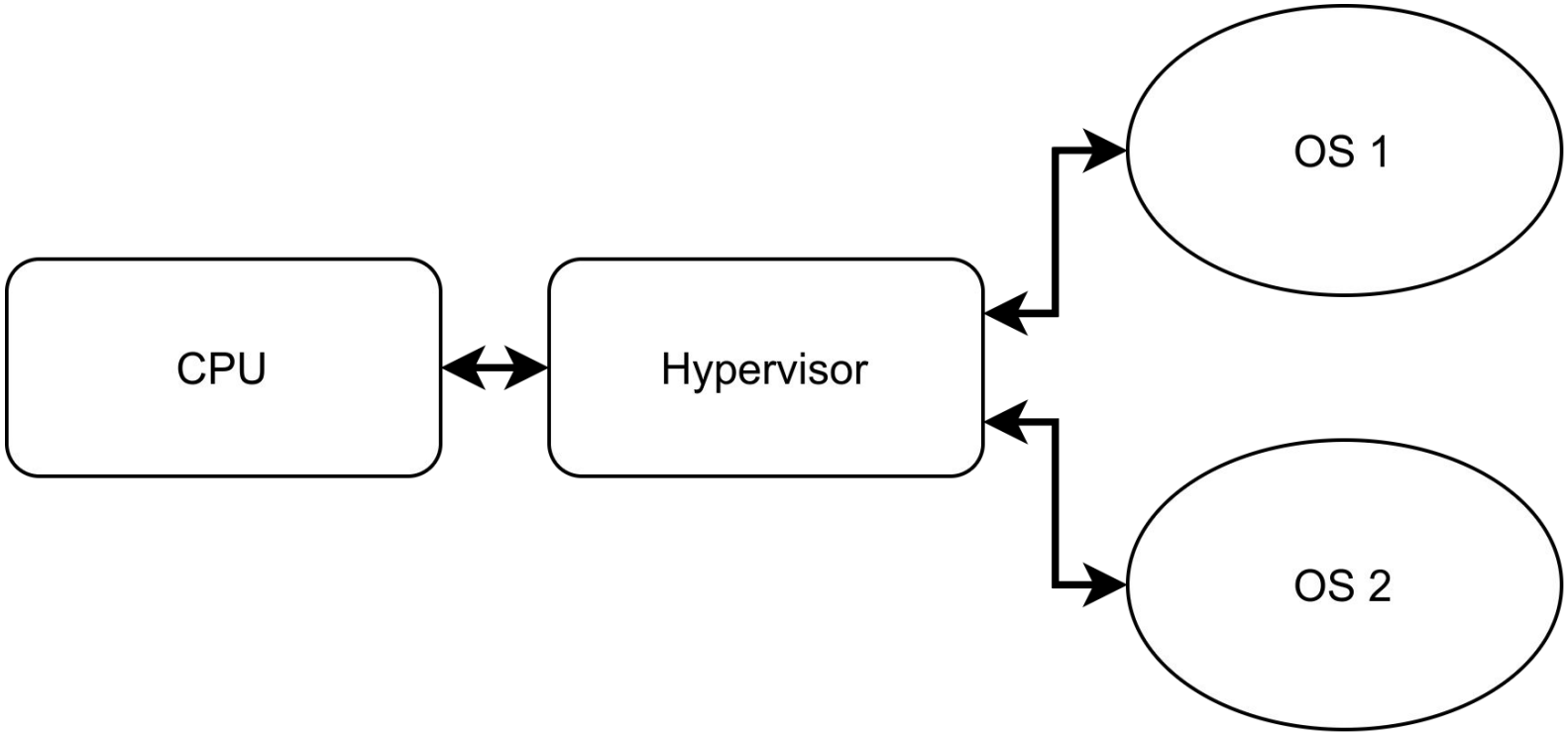
Containers

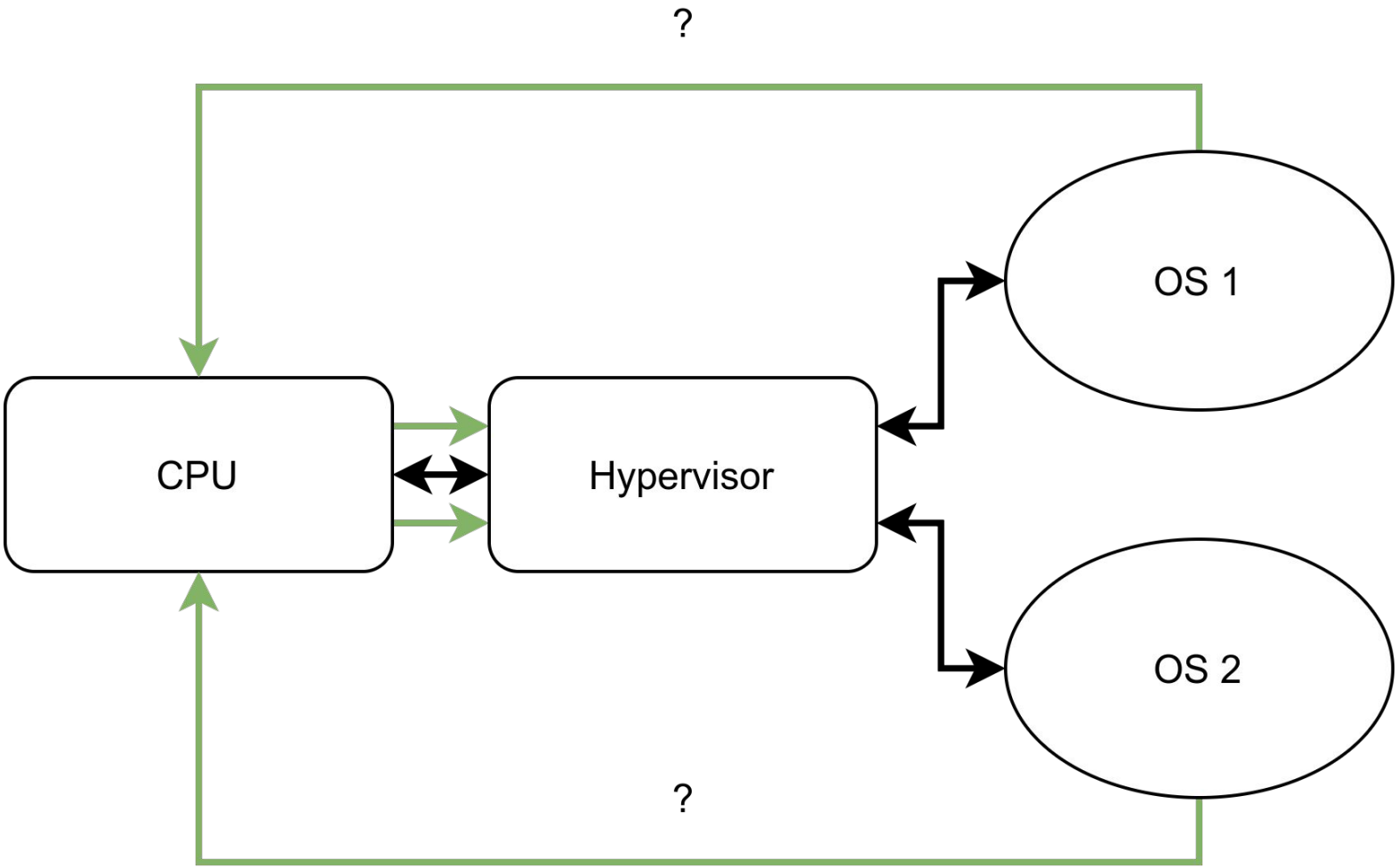
A History

The World


User-Mode
Kernel-Mode
Hardware Capabilities
(eg. memory access)
Program Code
CPU ABI
Kernel

Virtual Machines


CPU
Hypervisor
OS 1
OS 2


?
OS 1
CPU
Hypervisor
OS 2
?

Back to the Drawing Board…

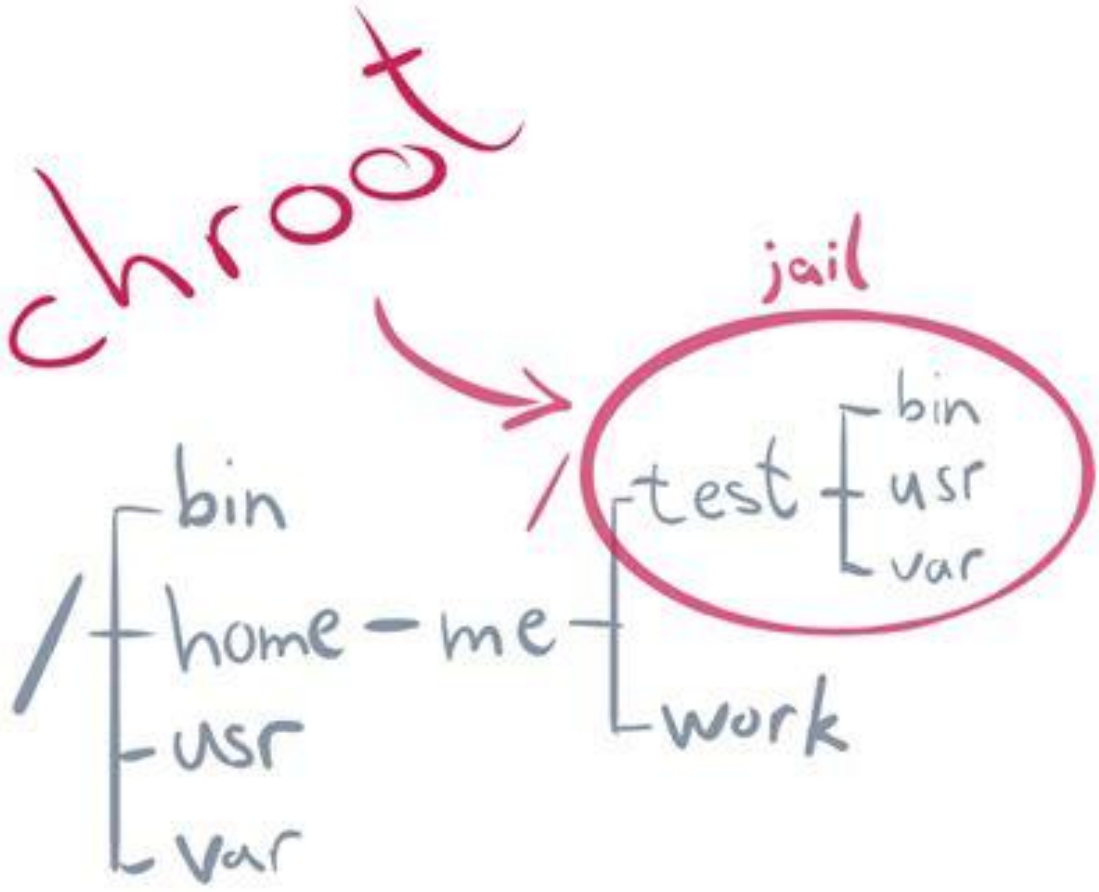
Problems with the OS

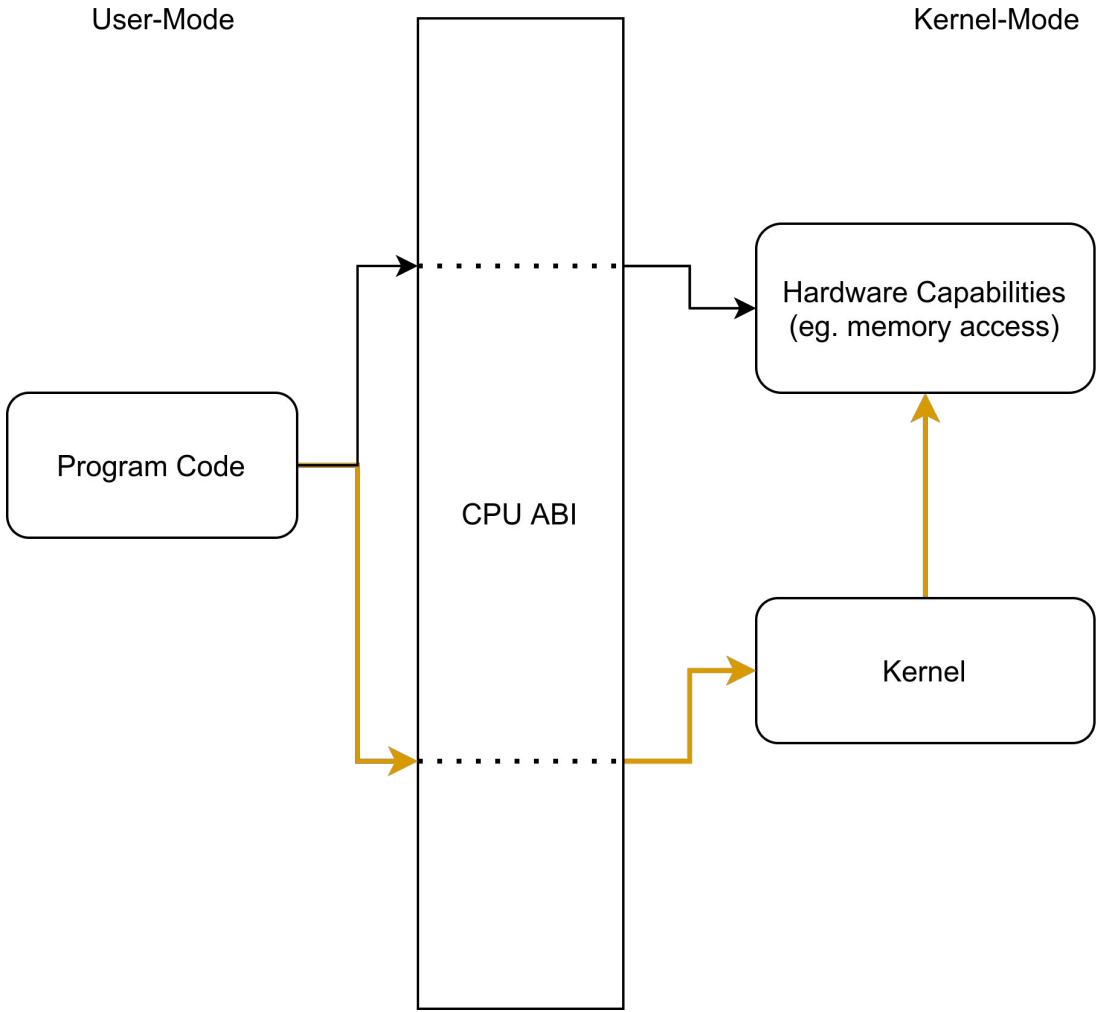
1. Security
2. Managing Resources
3. Versioning

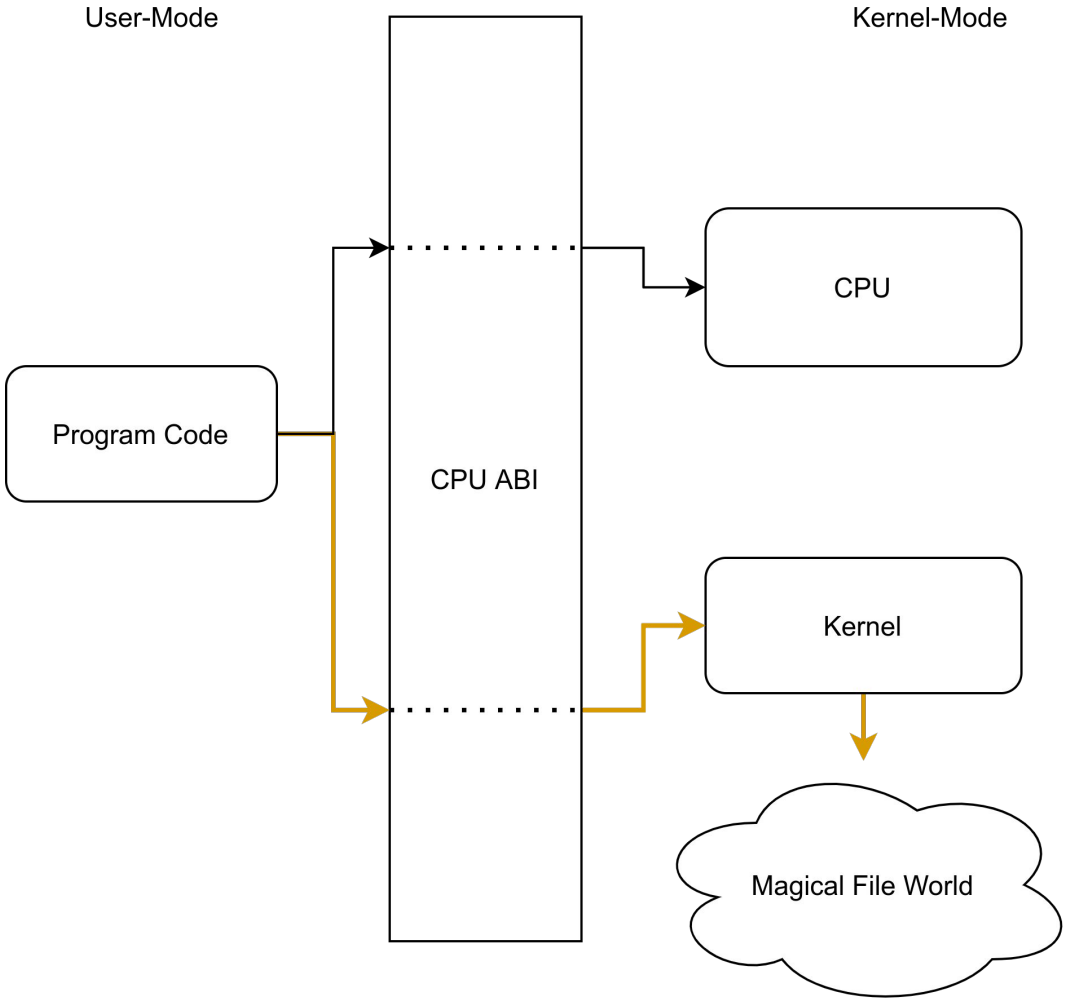
Solving Security with Capabilities

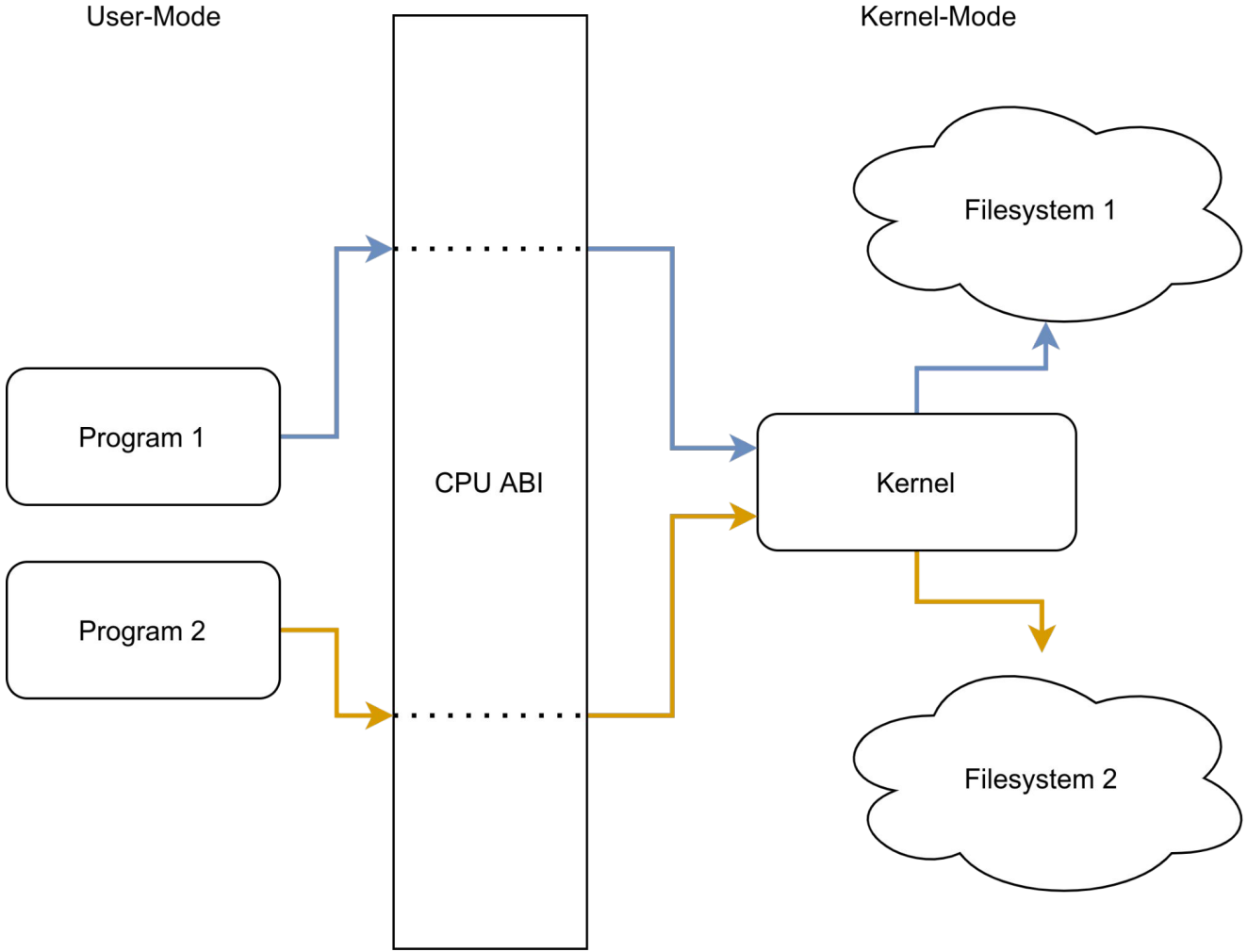
Solving Resource Management with Cgroups

Solving Versioning with Namespaces


chroot
jail
/
bin
home
me
usr
var
work
/
test
bin
usr
var


User-Mode
Kernel-Mode
Hardware Capabilities
(eg. memory access)
Program Code
CPU ABI
Kernel


User-Mode
Kernel-Mode
CPU
Program Code
CPU ABI
Kernel
Magical File World


User-Mode
Kernel-Mode
Filesystem 1
Program 1
CPU ABI
Kernel
Program 2
Filesystem 2

Containers!

1. Are allowed to touch only certain things.
2. Can be controlled easily.
3. Don’t mess up anybody else’s files.

Containers: Packaged Applications?

Historical Parallels

- C’s <include> to C++’s “using namespace std”.
- Directories
- Invention of the Process