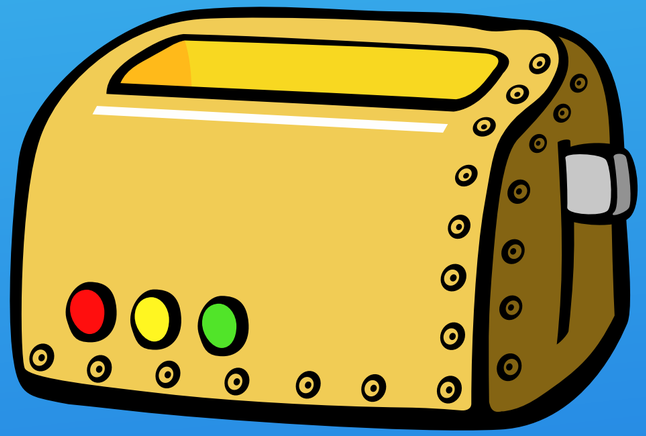
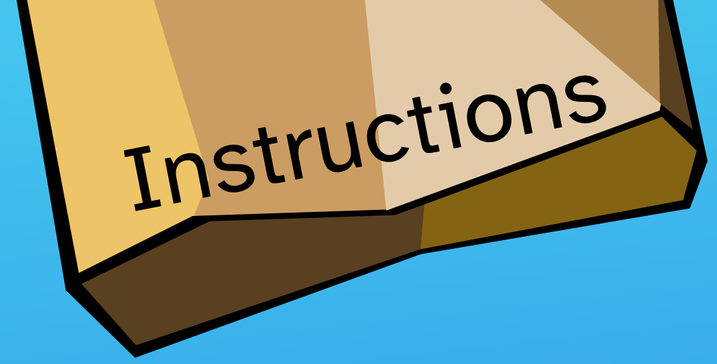
Attacker-defined Abstractions

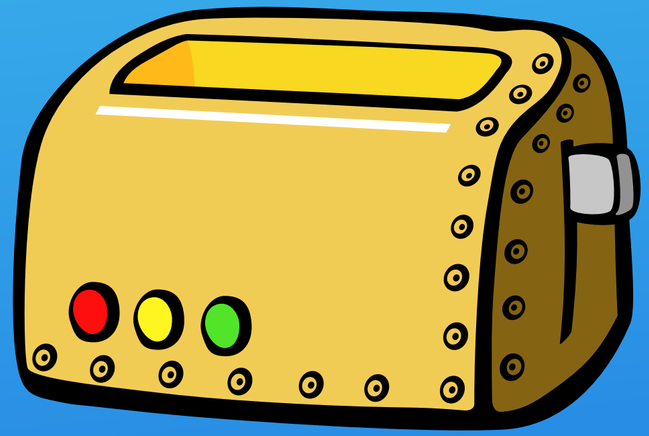
Programming Benign System Functionality For Subversive Purposes

Erik Bosman

VUSec

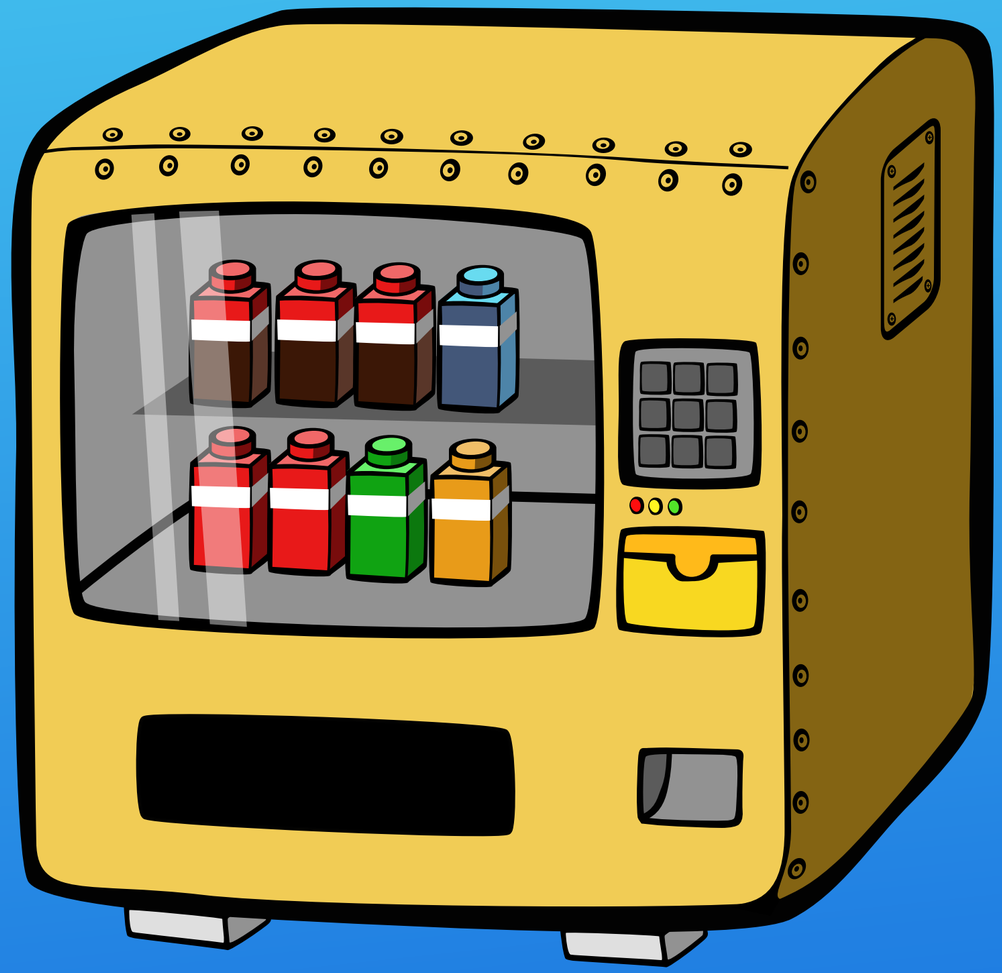



Instructions




Instructions

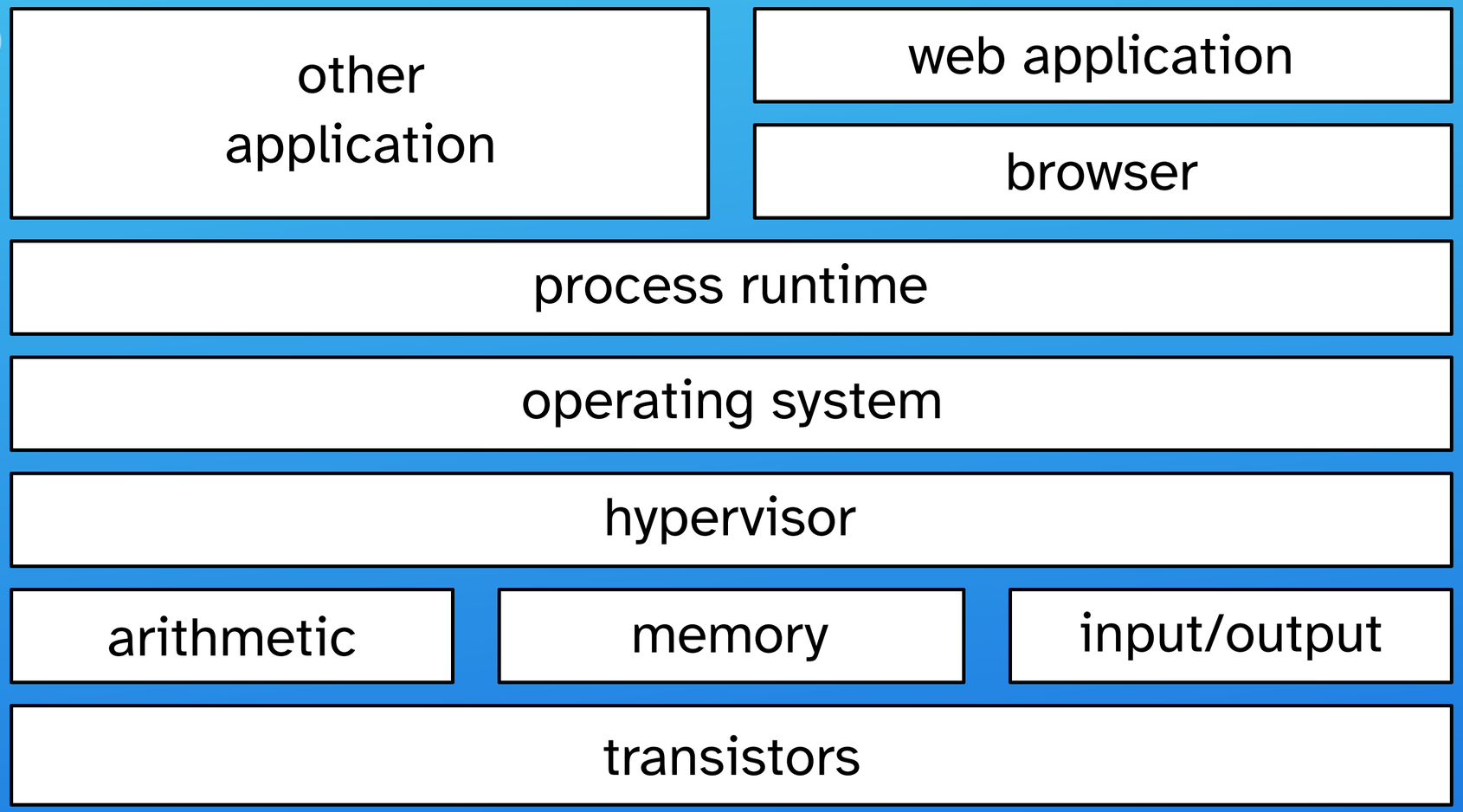

Instructions

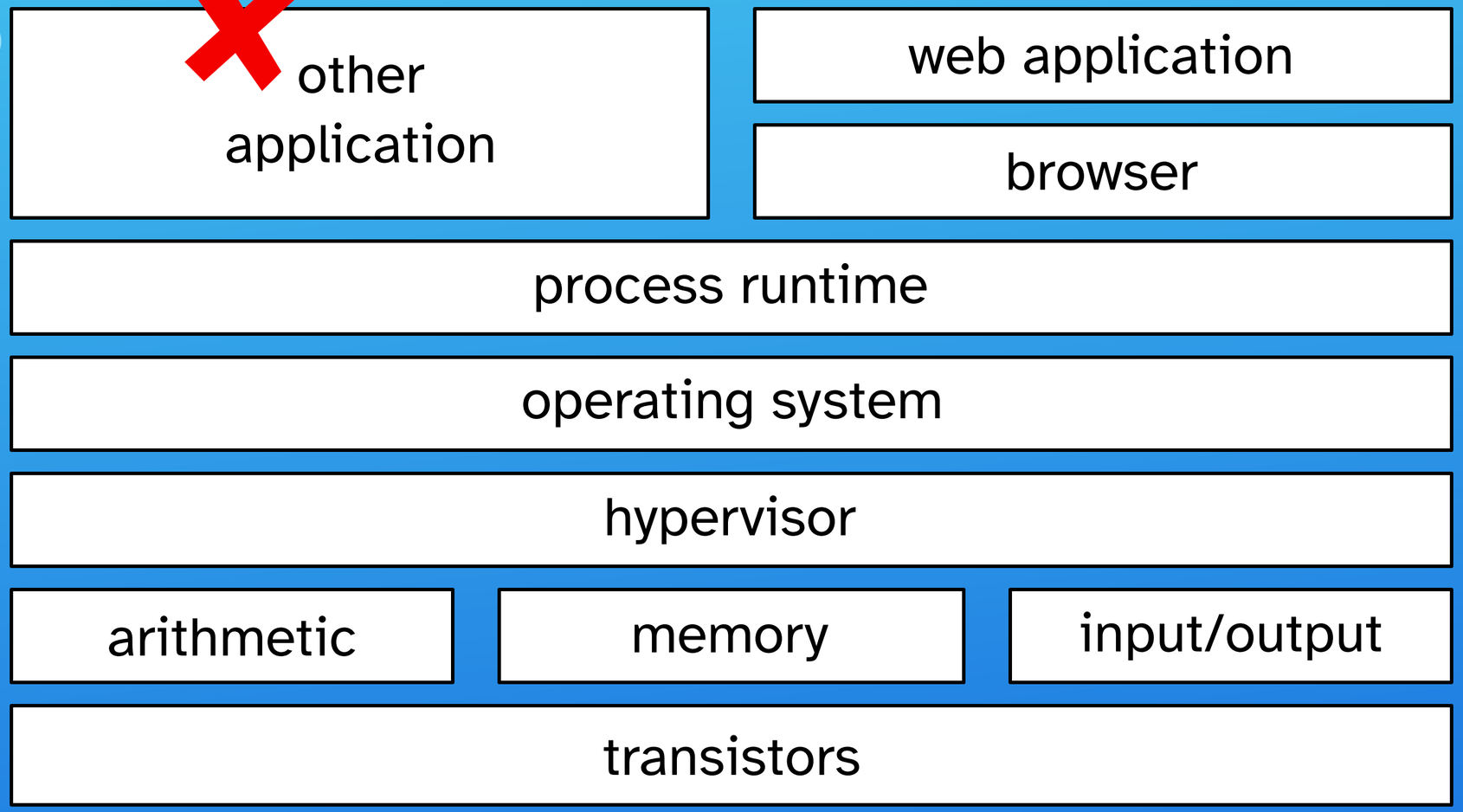


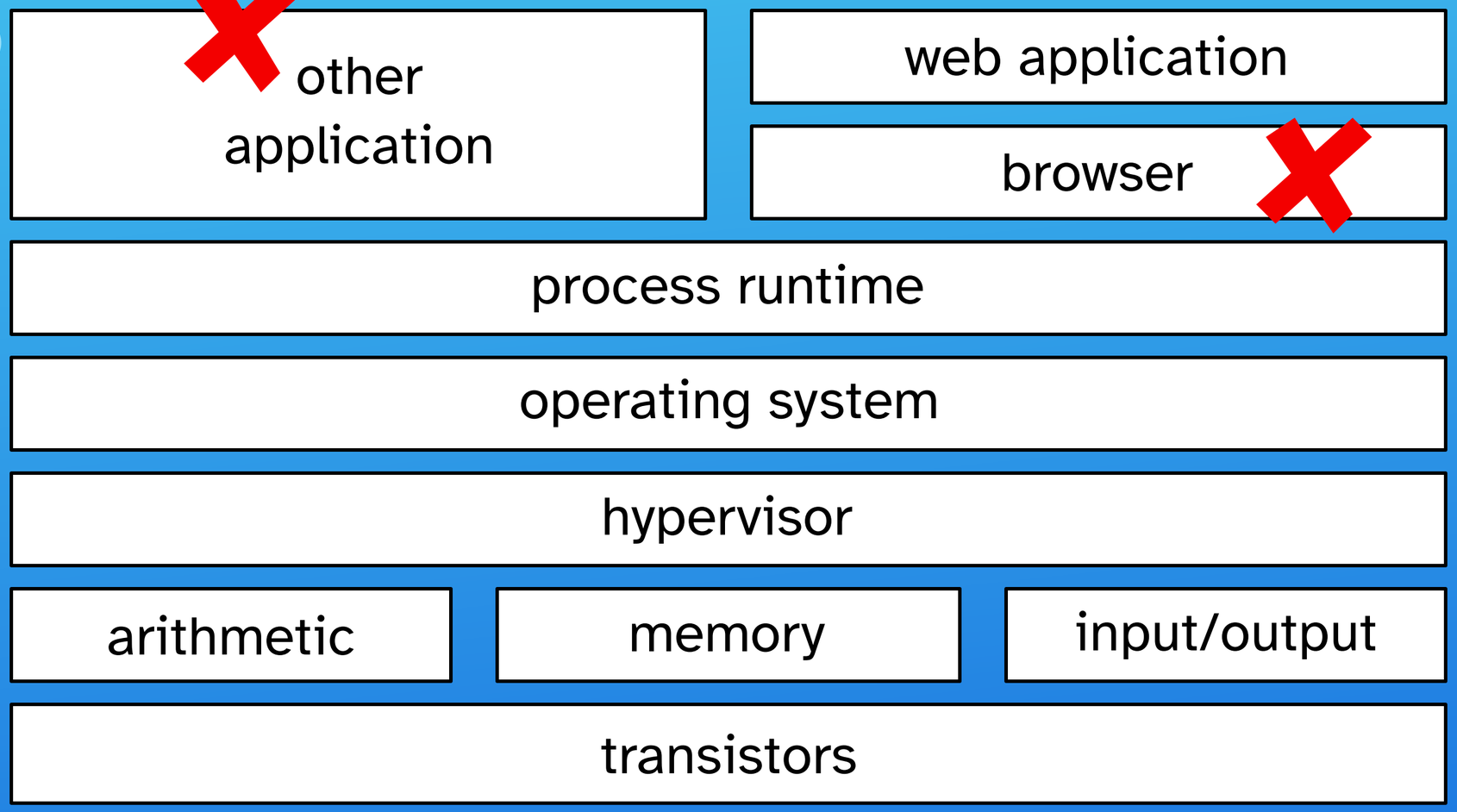

Input

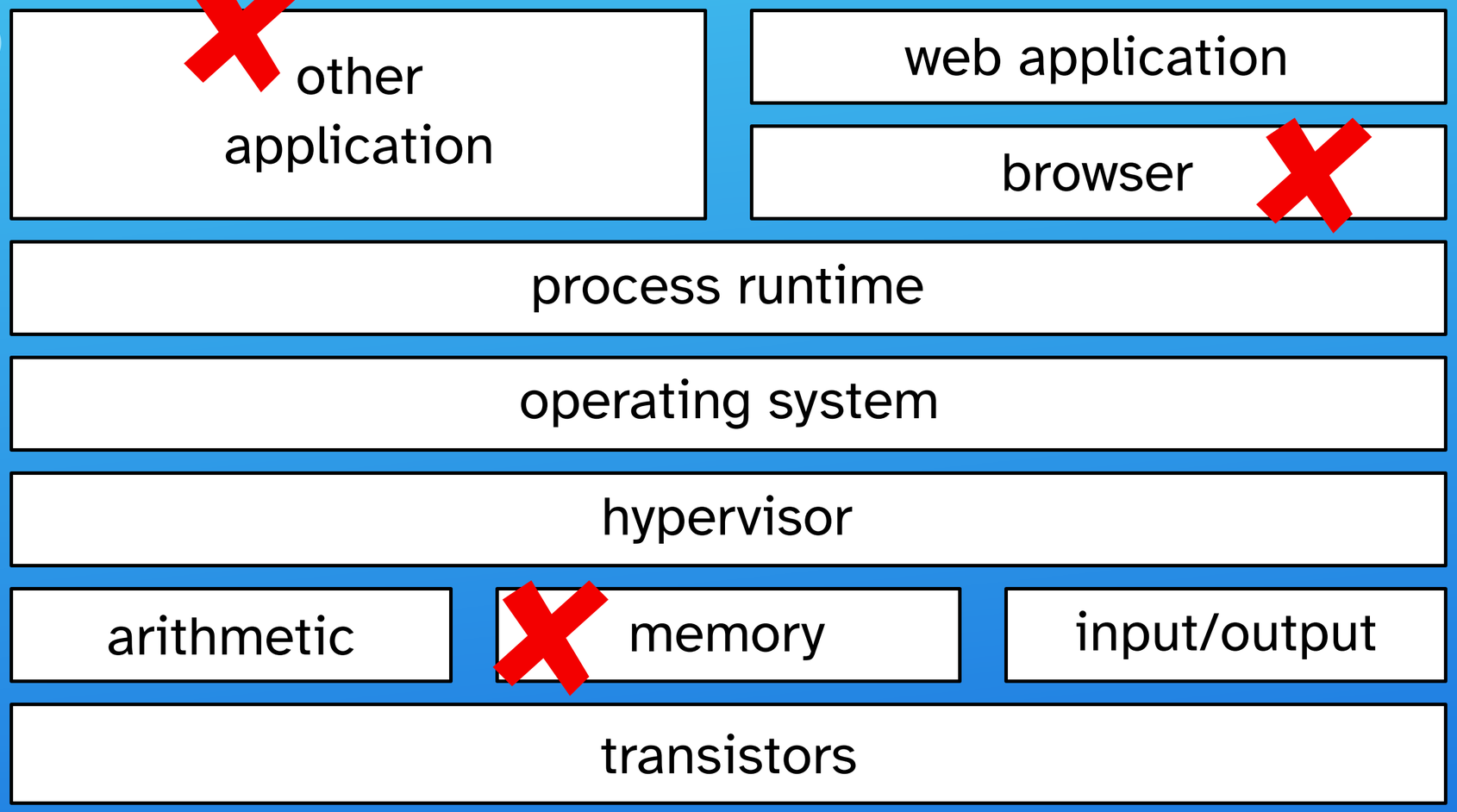

Input
Output

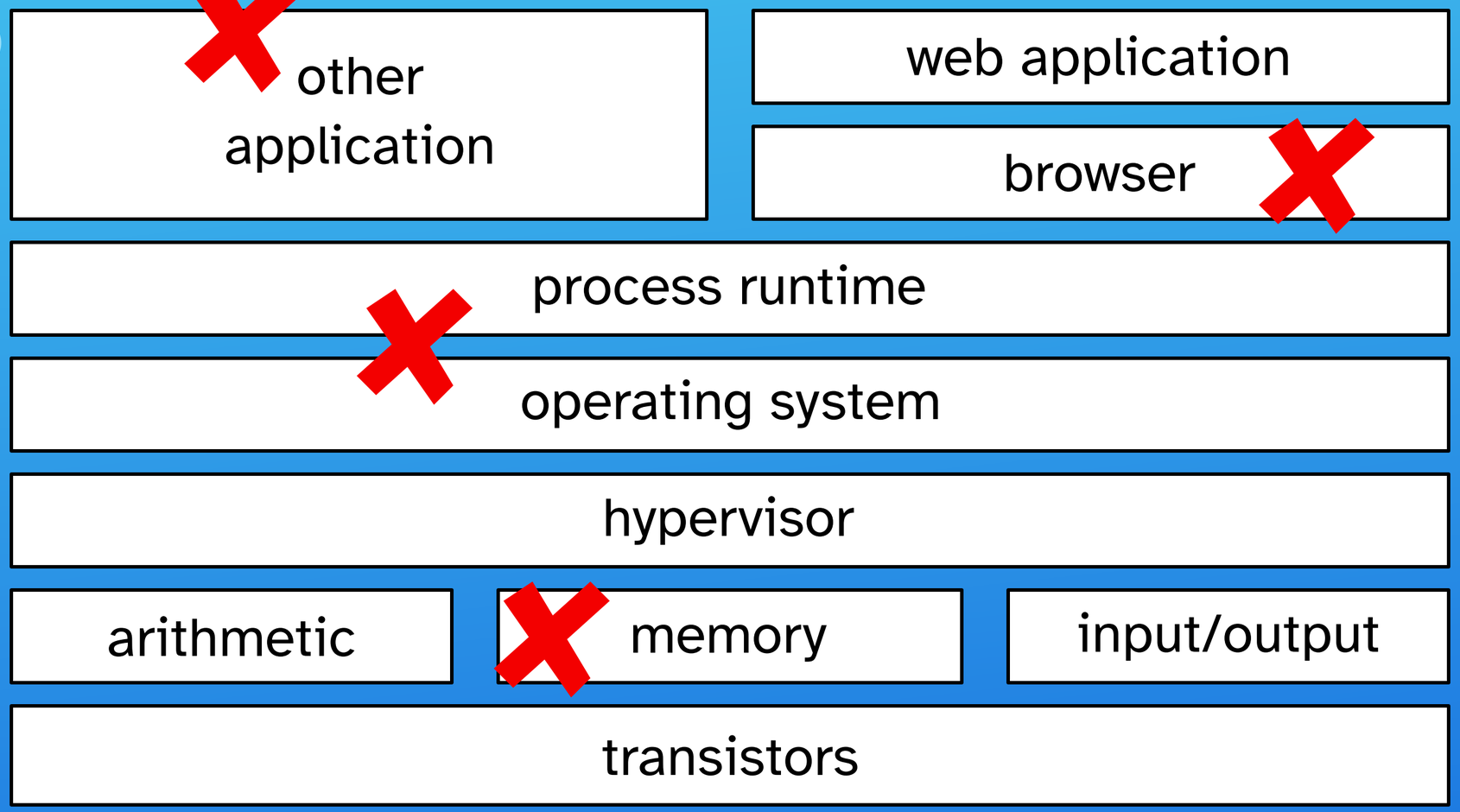

Instructions
Output


other application
web application
browser
process runtime
operating system
hypervisor
arithmetic
memory
input/output
transistors


other application
web application
browser
process runtime
operating system
hypervisor
arithmetic
memory
input/output
transistors

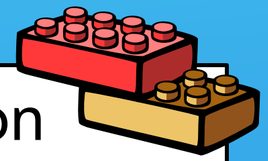

other application
web application
browser
process runtime
operating system
hypervisor
arithmetic
memory
input/output
transistors


other application
web application
browser
process runtime
operating system
hypervisor
arithmetic
memory
input/output
transistors


other application
web application
browser
process runtime
operating system
hypervisor
arithmetic
memory
input/output
transistors

other application

web application



browser

process runtime

operating system

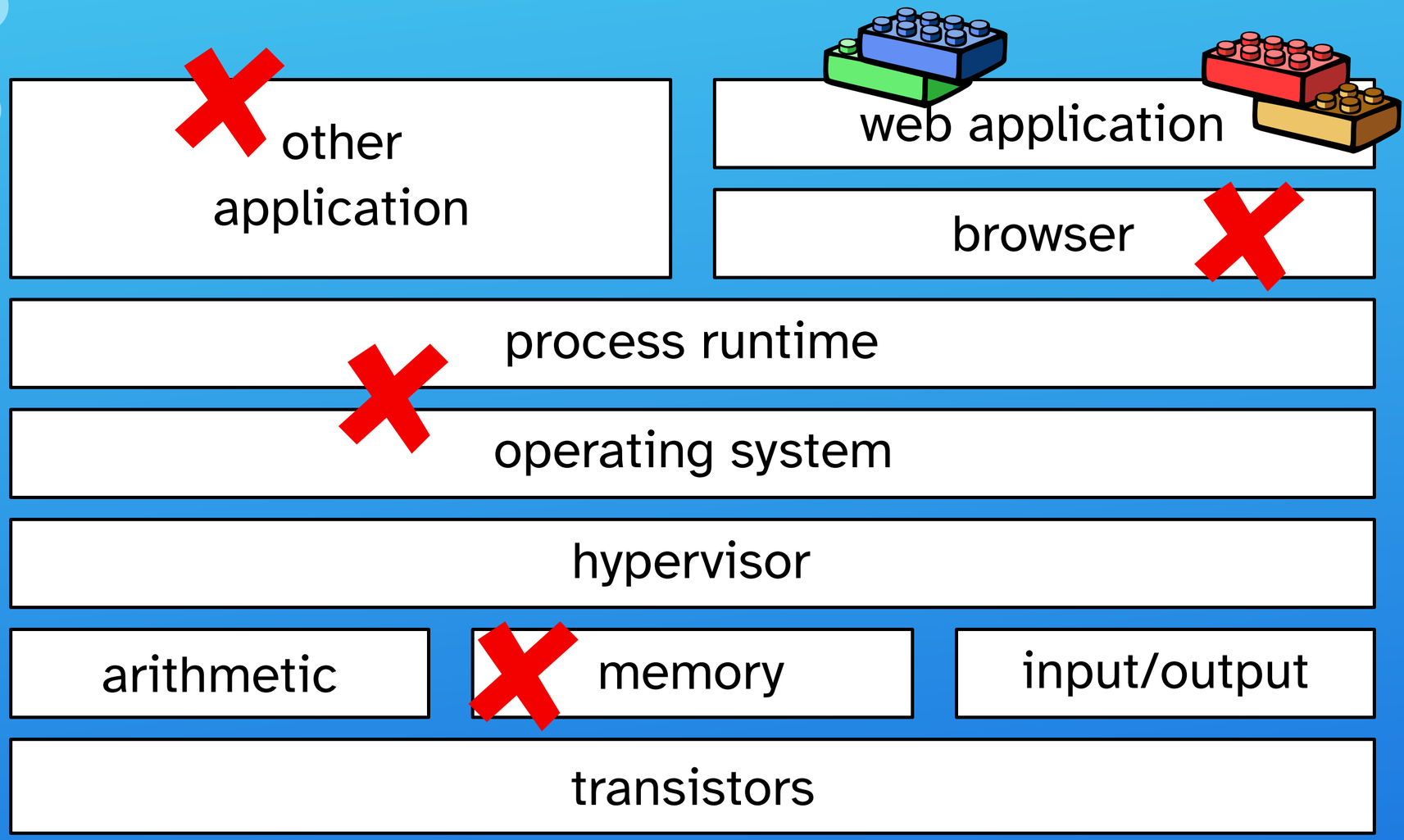
hypervisor

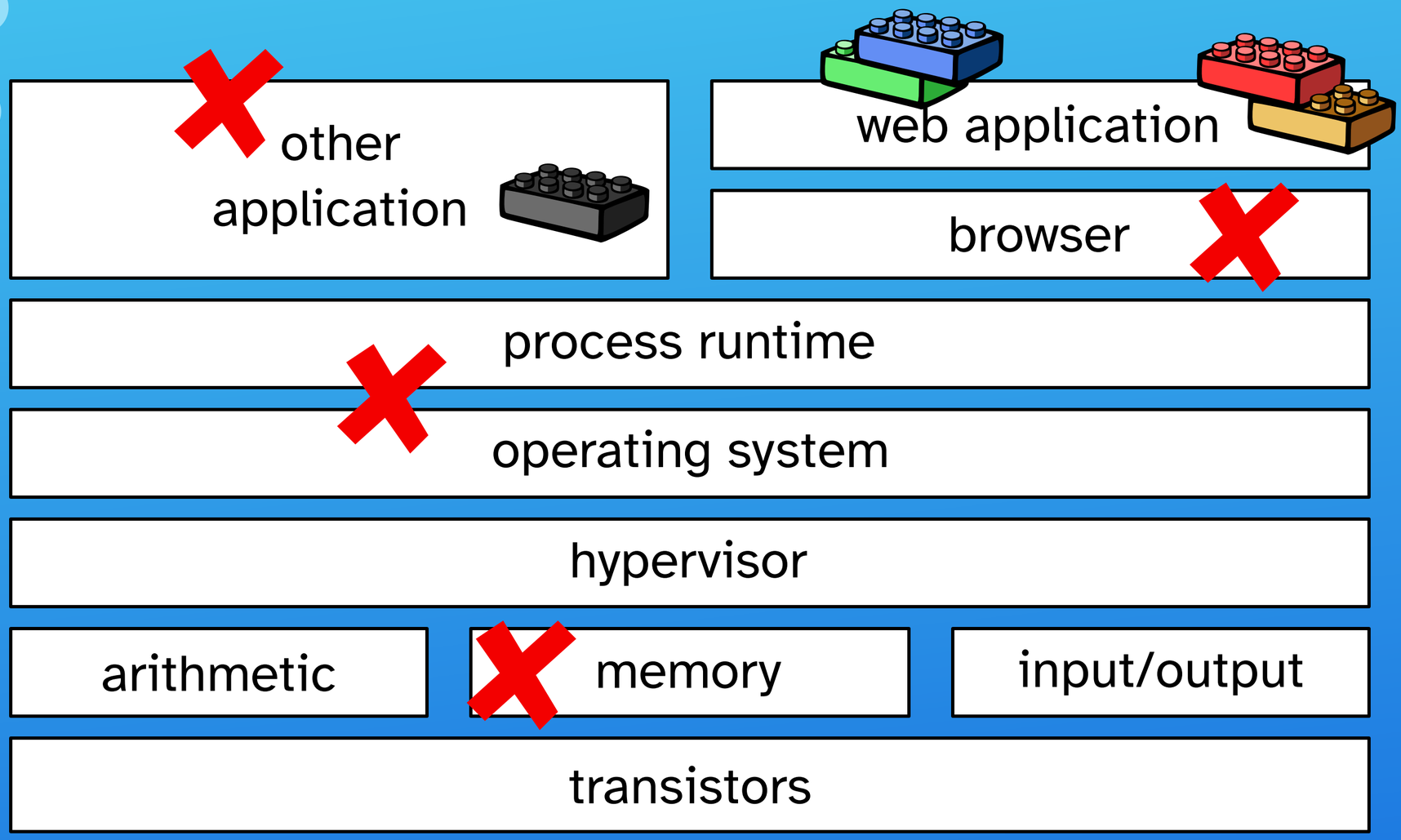
arithmetic

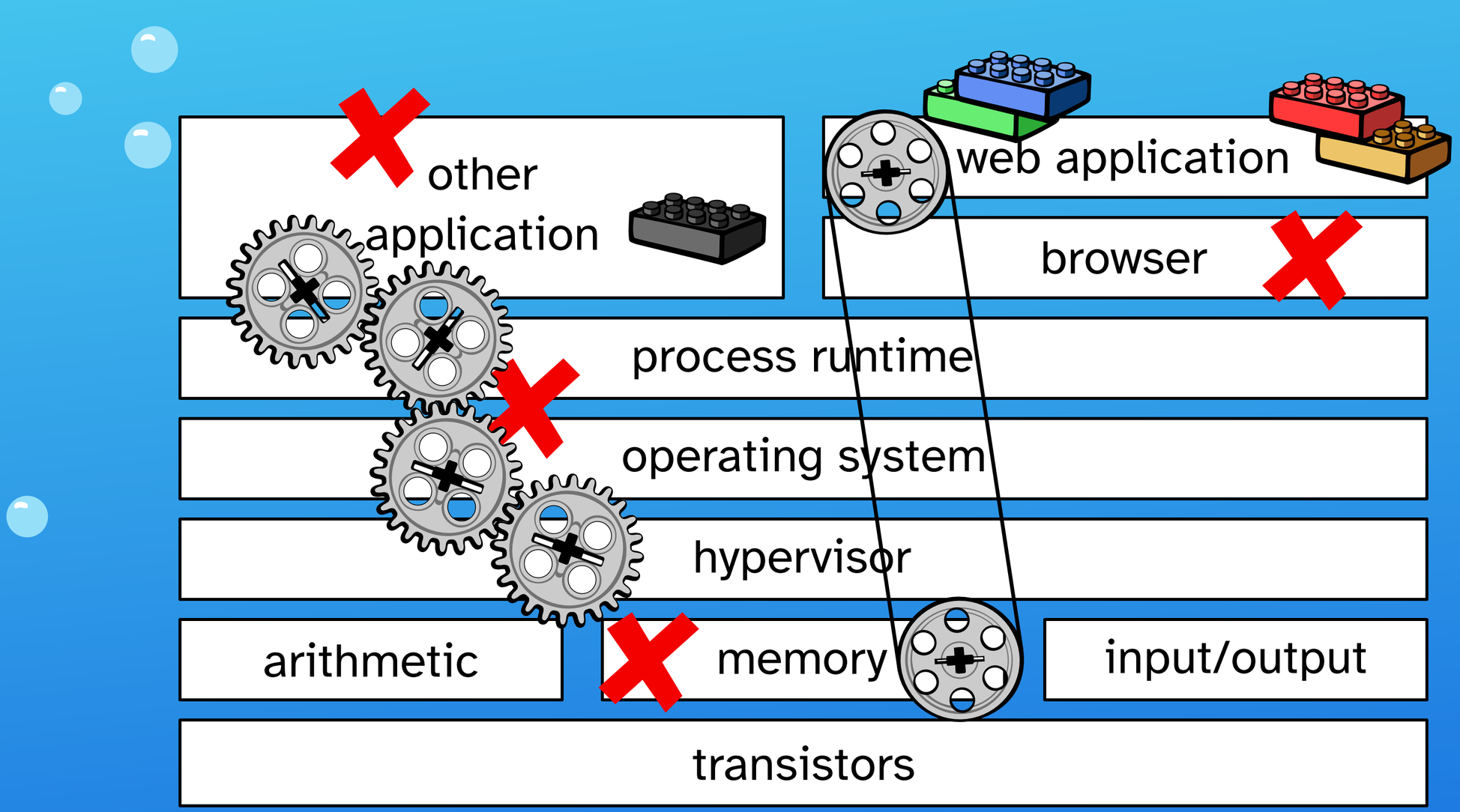
memory

input/output

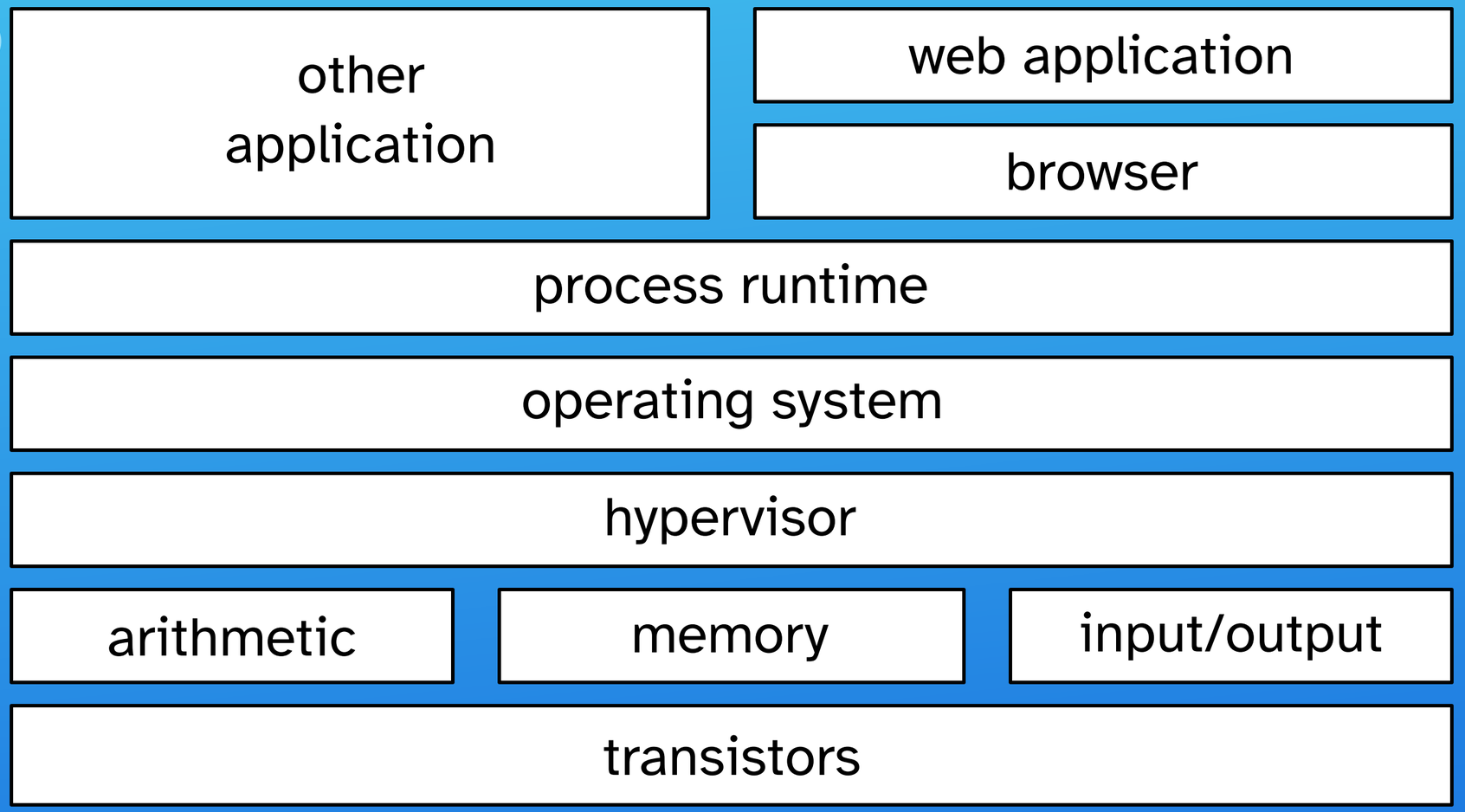
transistors


other application
web application
browser
process runtime
operating system
hypervisor
arithmetic
memory
input/output
transistors

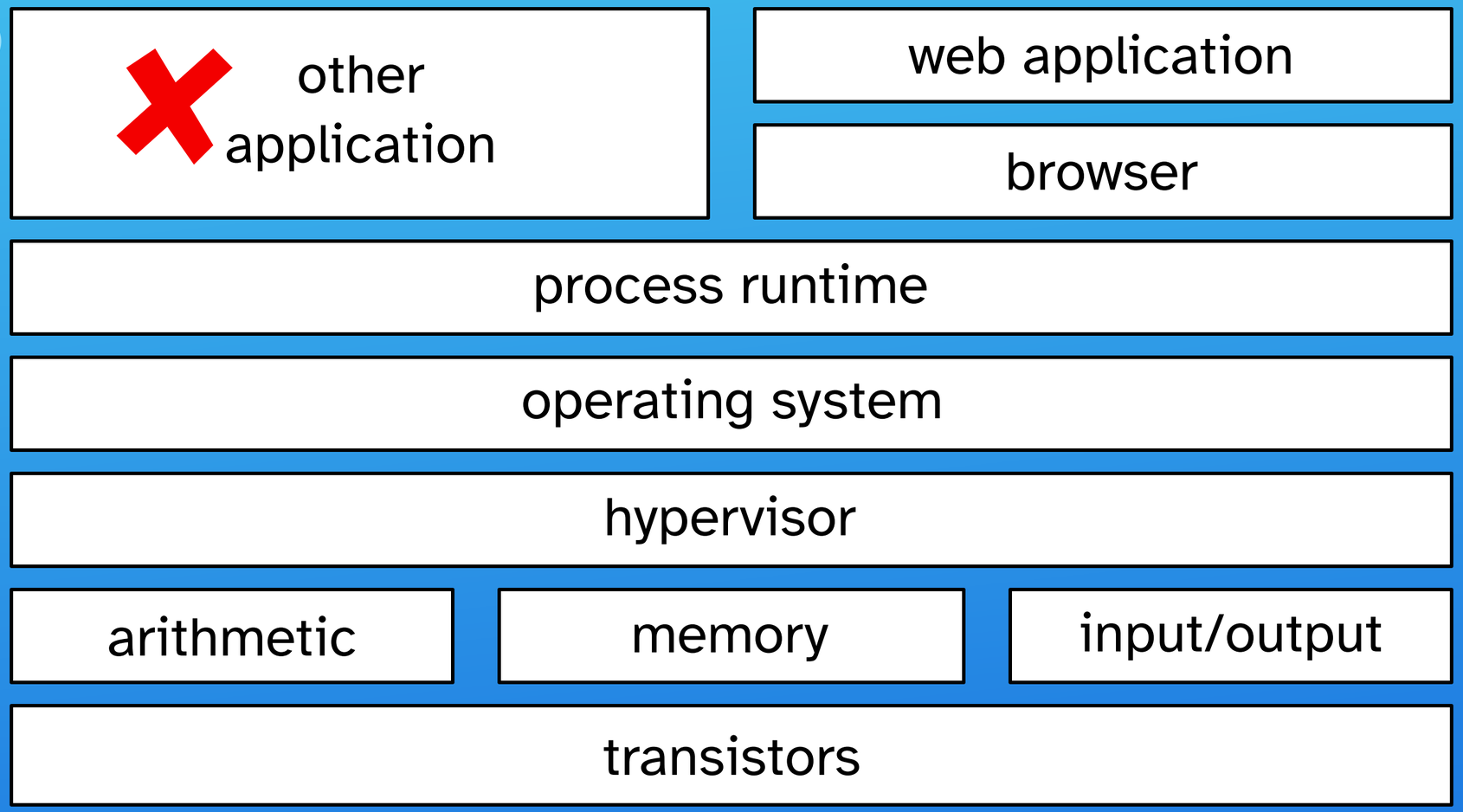

other application
web application
browser
process runtime
operating system
hypervisor
arithmetic
memory
input/output
transistors


other application
web application
browser
process runtime
operating system
hypervisor
arithmetic
memory
input/output
transistors

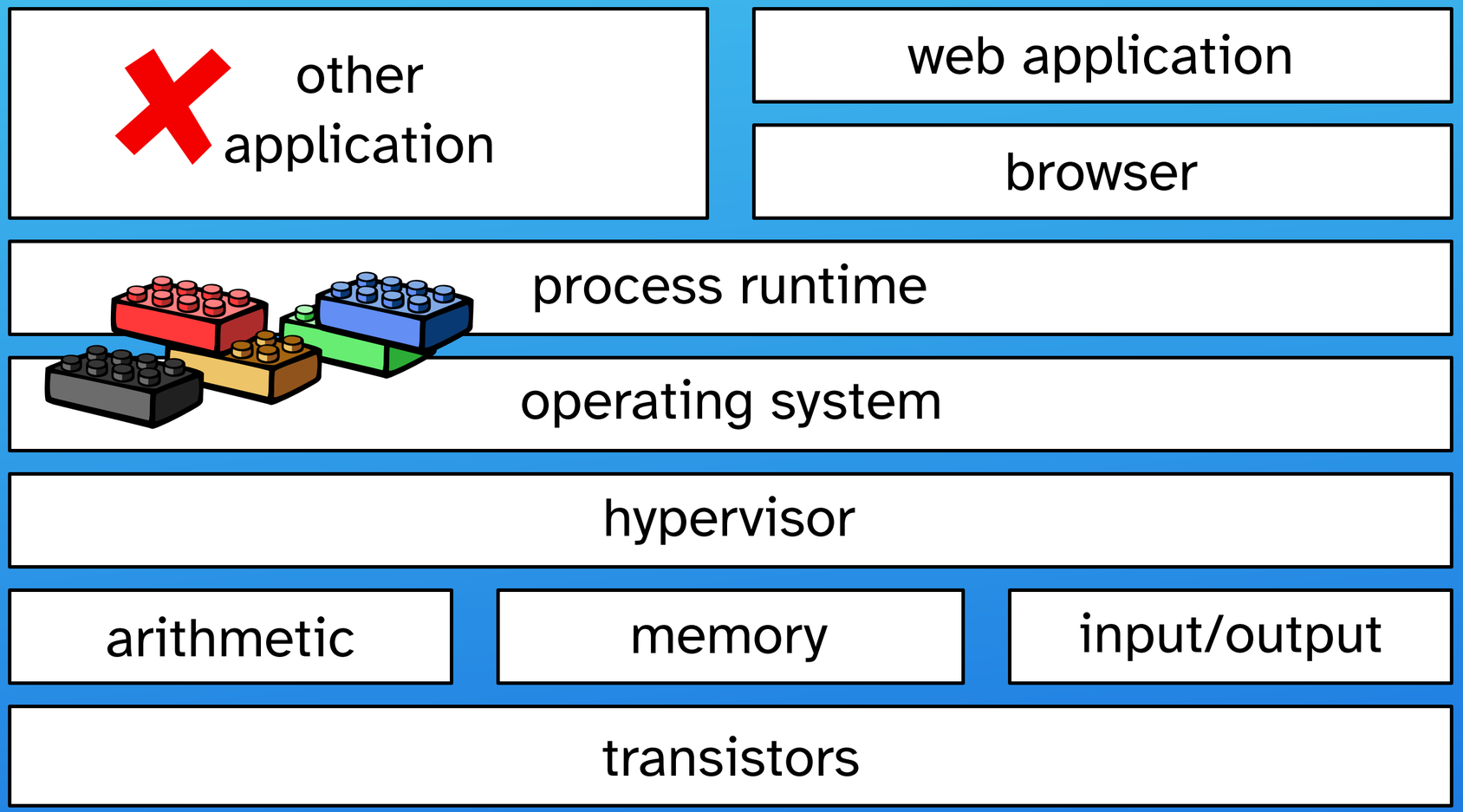
SigReturn Oriented Programming



SigReturn Oriented Programming



SigReturn Oriented Programming



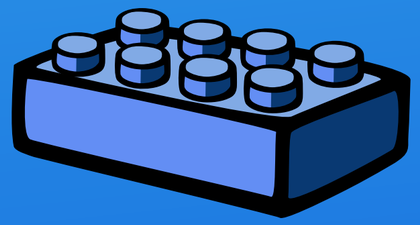
SigReturn Oriented Programming

SigReturn Oriented Programming

normal Return-Oriented Programming:

SigReturn Oriented Programming

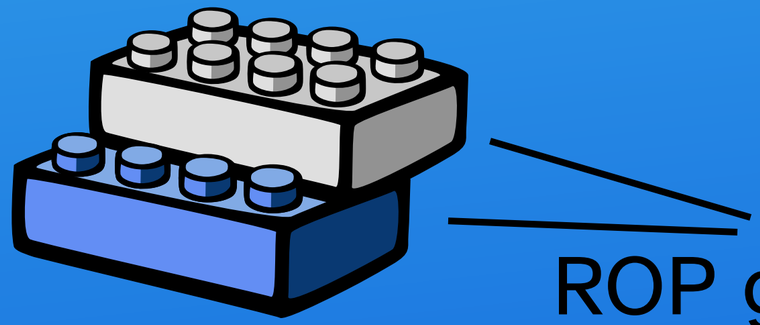
normal
Return-Oriented
Programming:



ROP gadgets

SigReturn Oriented Programming

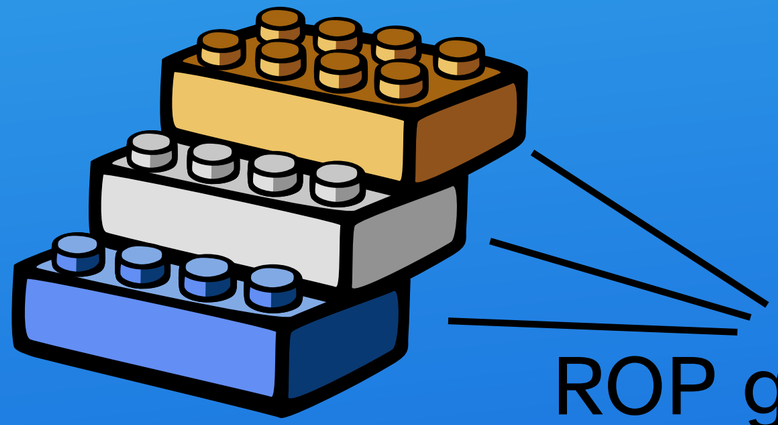
normal Return-Oriented Programming:



ROP gadgets

SigReturn Oriented Programming

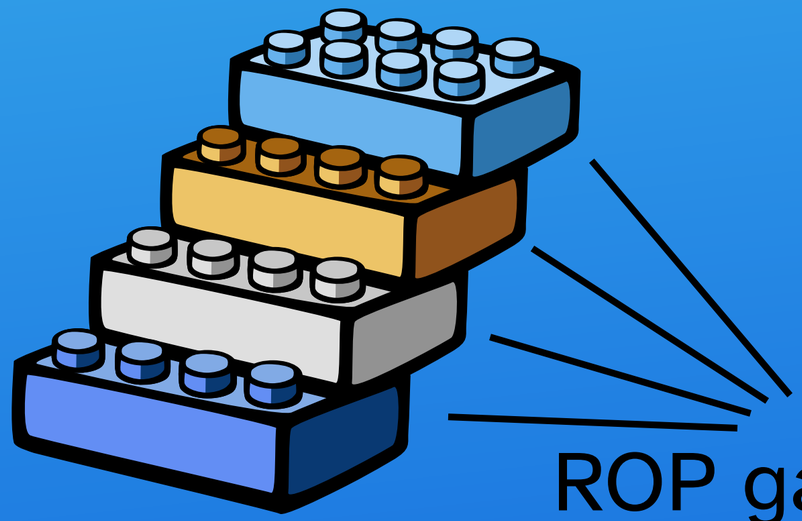
normal Return-Oriented Programming:



ROP gadgets

SigReturn Oriented Programming

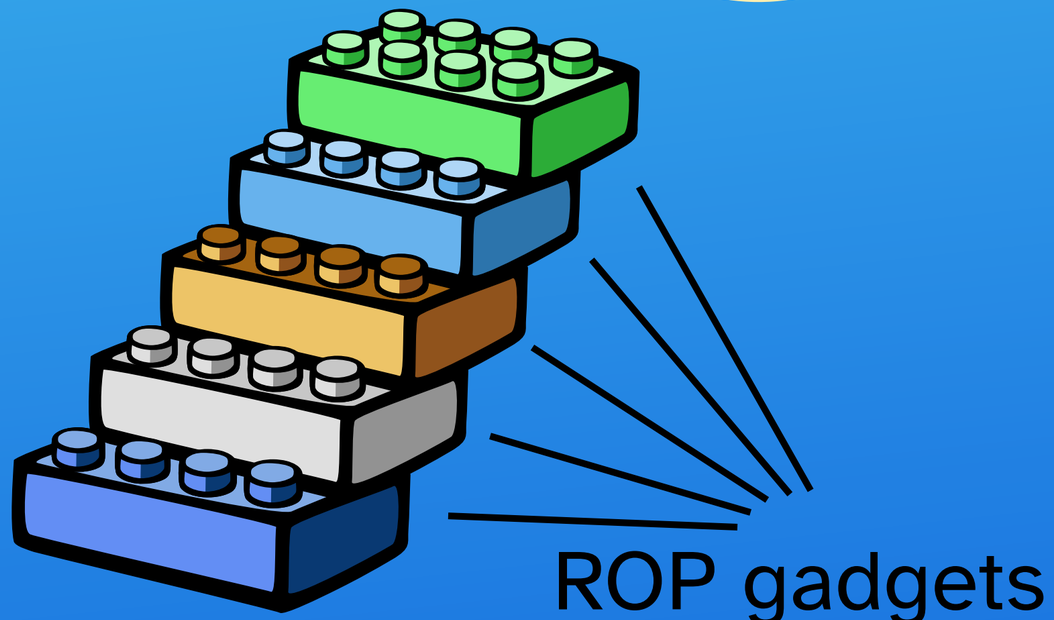
normal Return-Oriented Programming:



ROP gadgets

SigReturn Oriented Programming

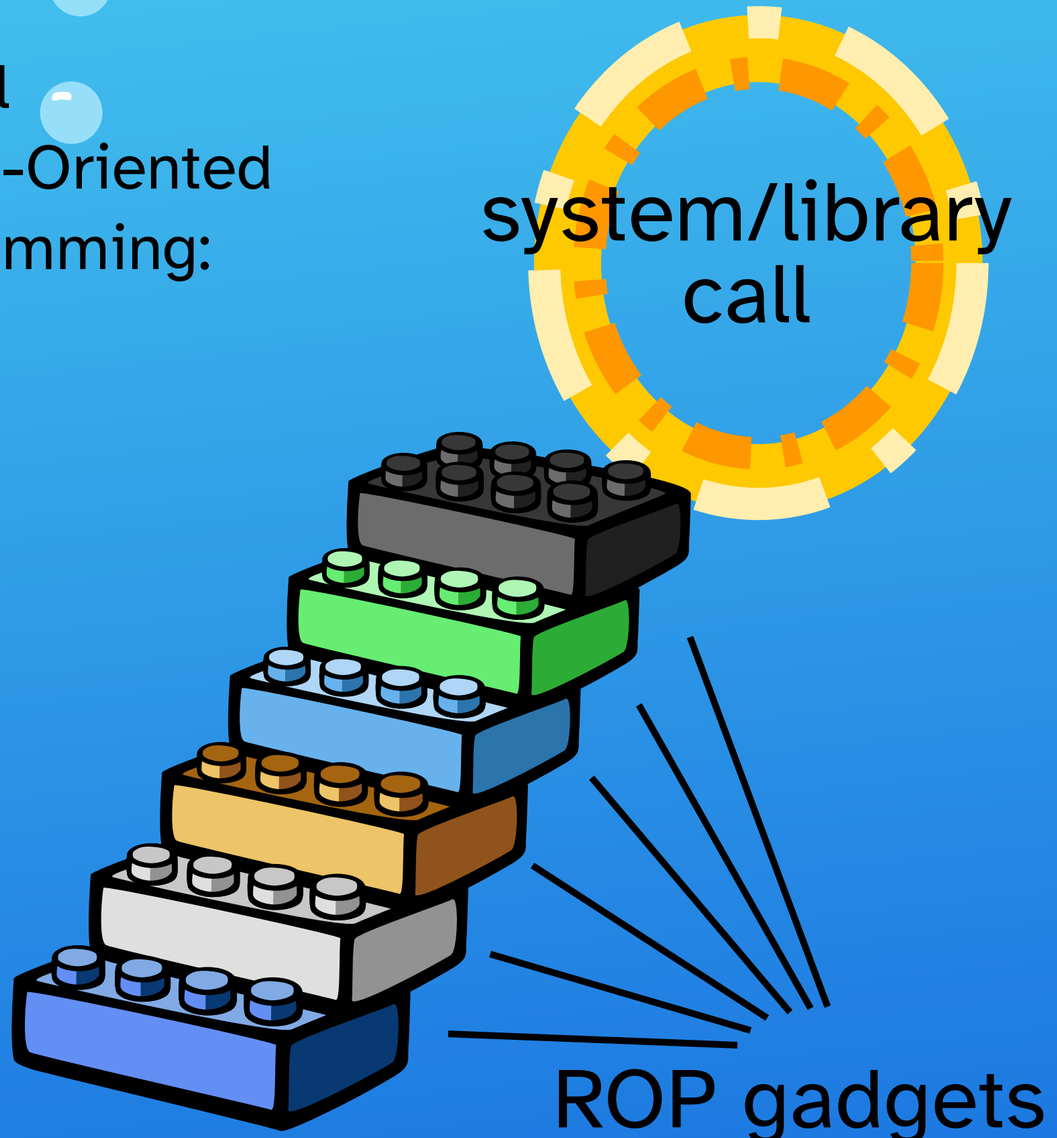
normal Return-Oriented Programming:



ROP gadgets

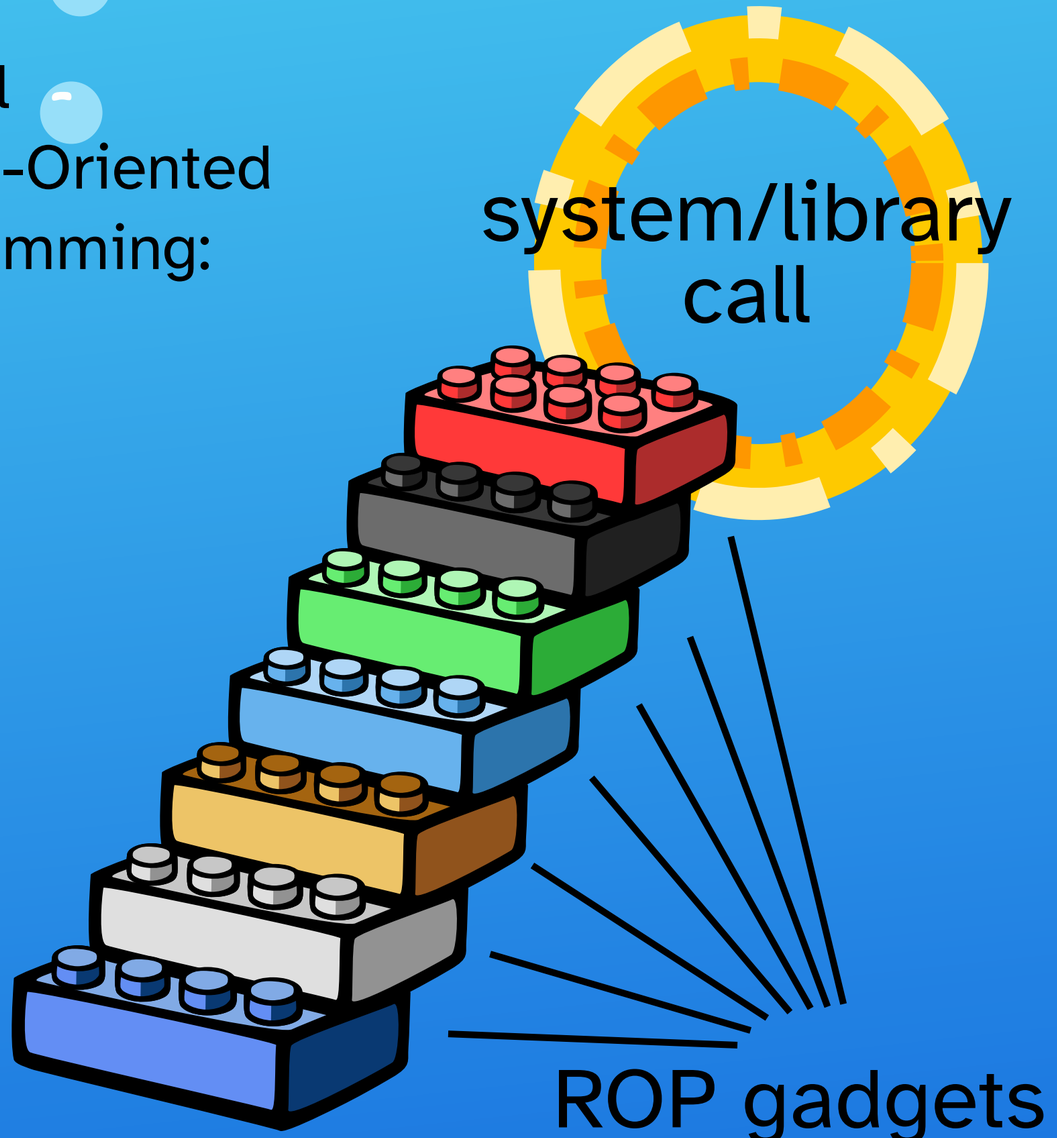
SigReturn Oriented Programming

normal Return-Oriented Programming:



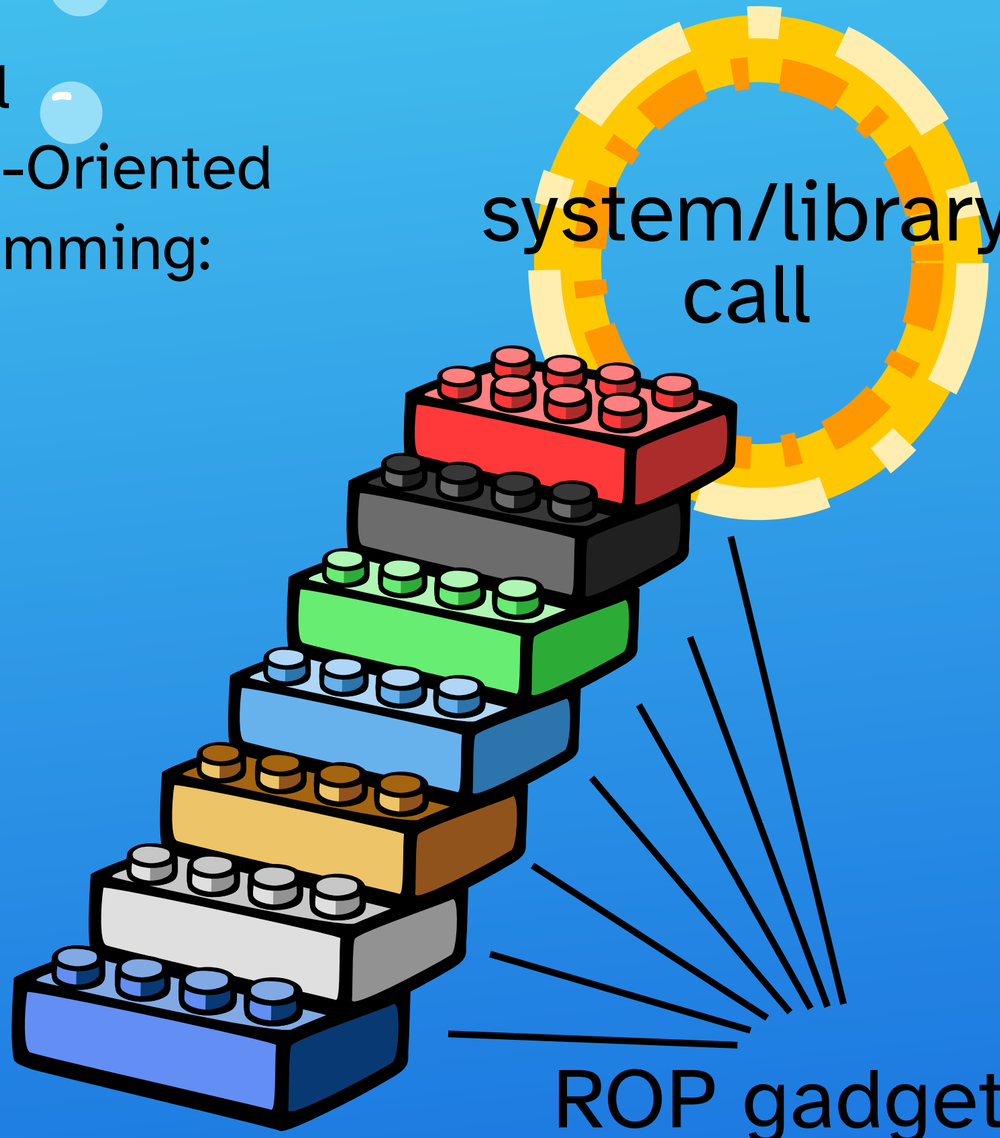
SigReturn Oriented Programming

normal Return-Oriented Programming:



SigReturn Oriented Programming

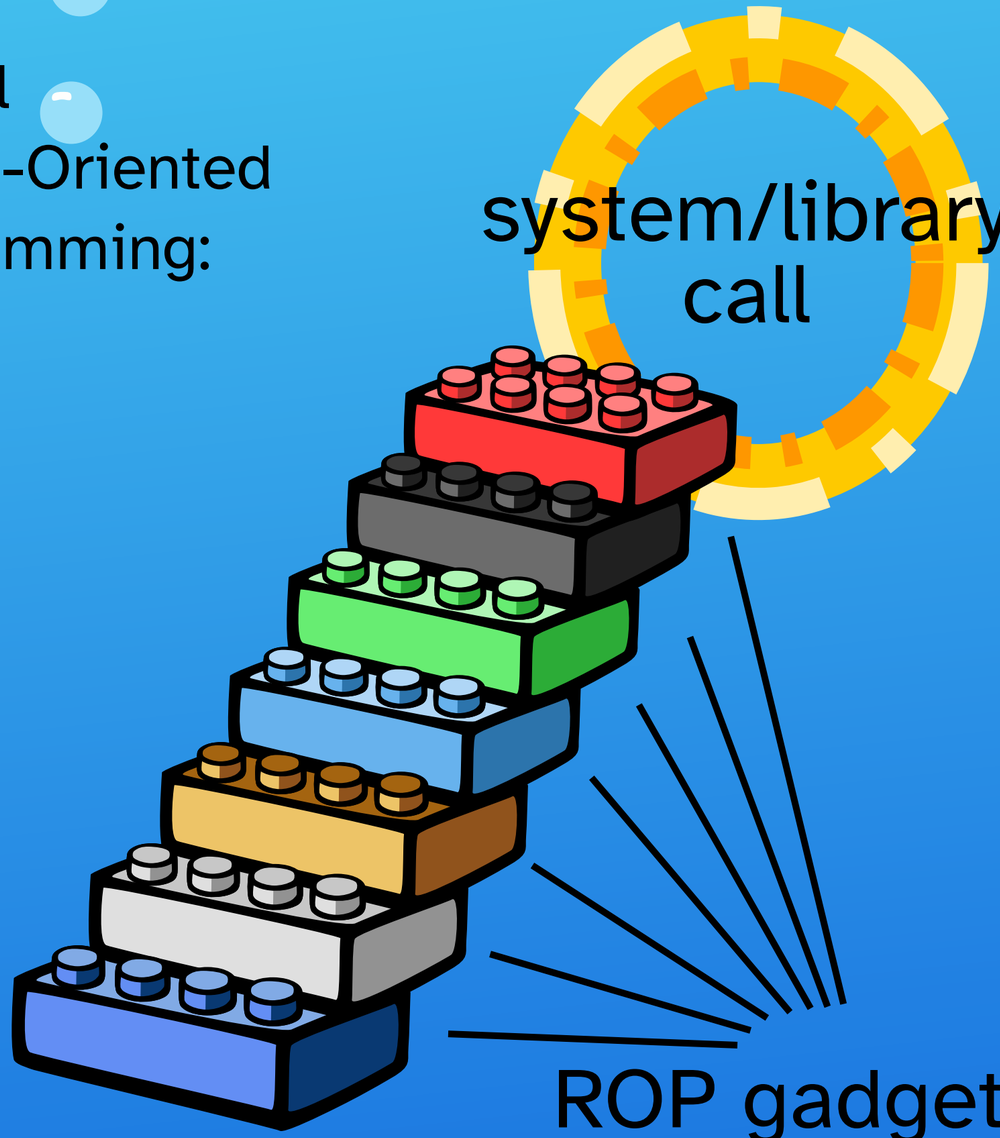
normal Return-Oriented Programming:



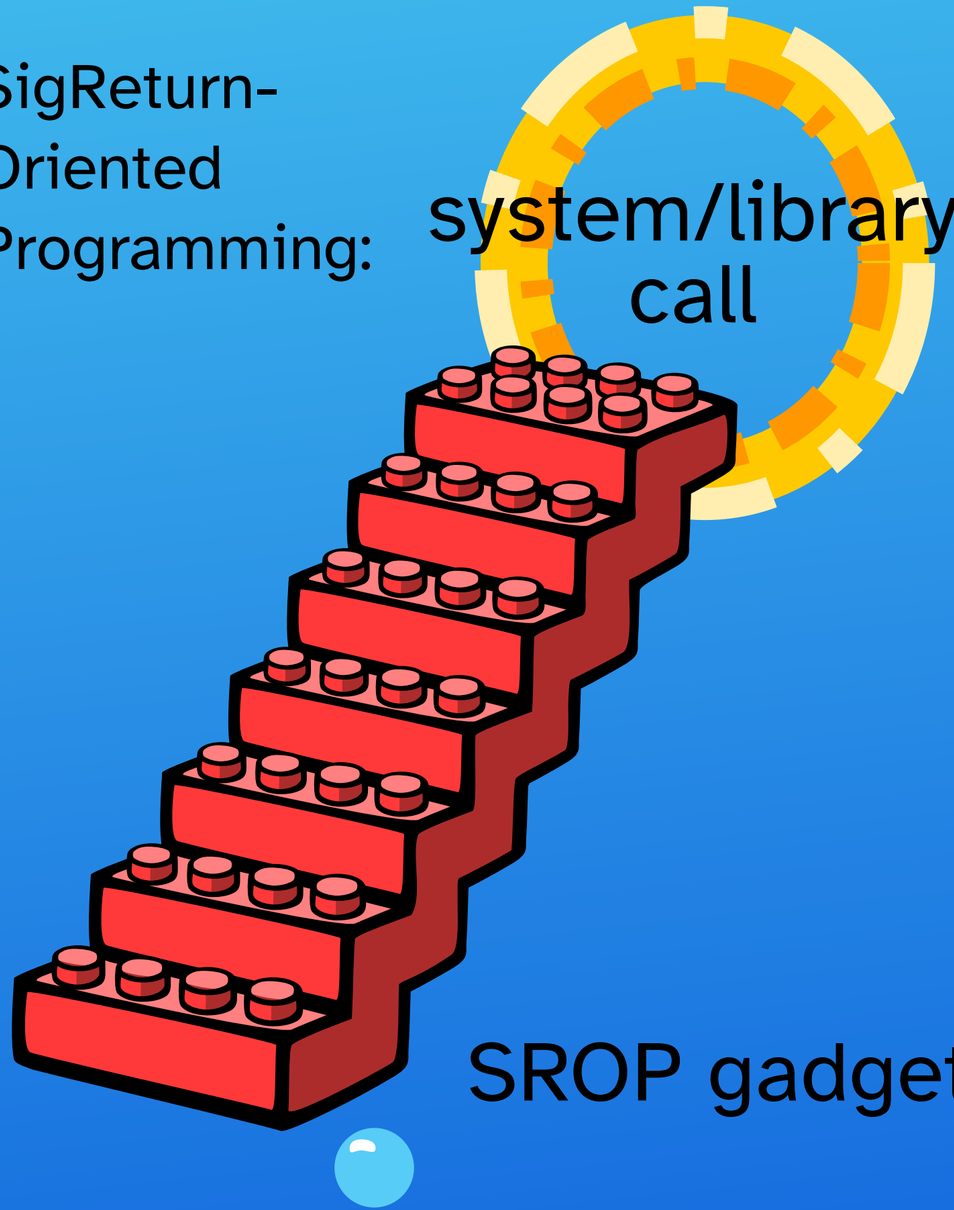
SigReturn-Oriented Programming:

SigReturn Oriented Programming

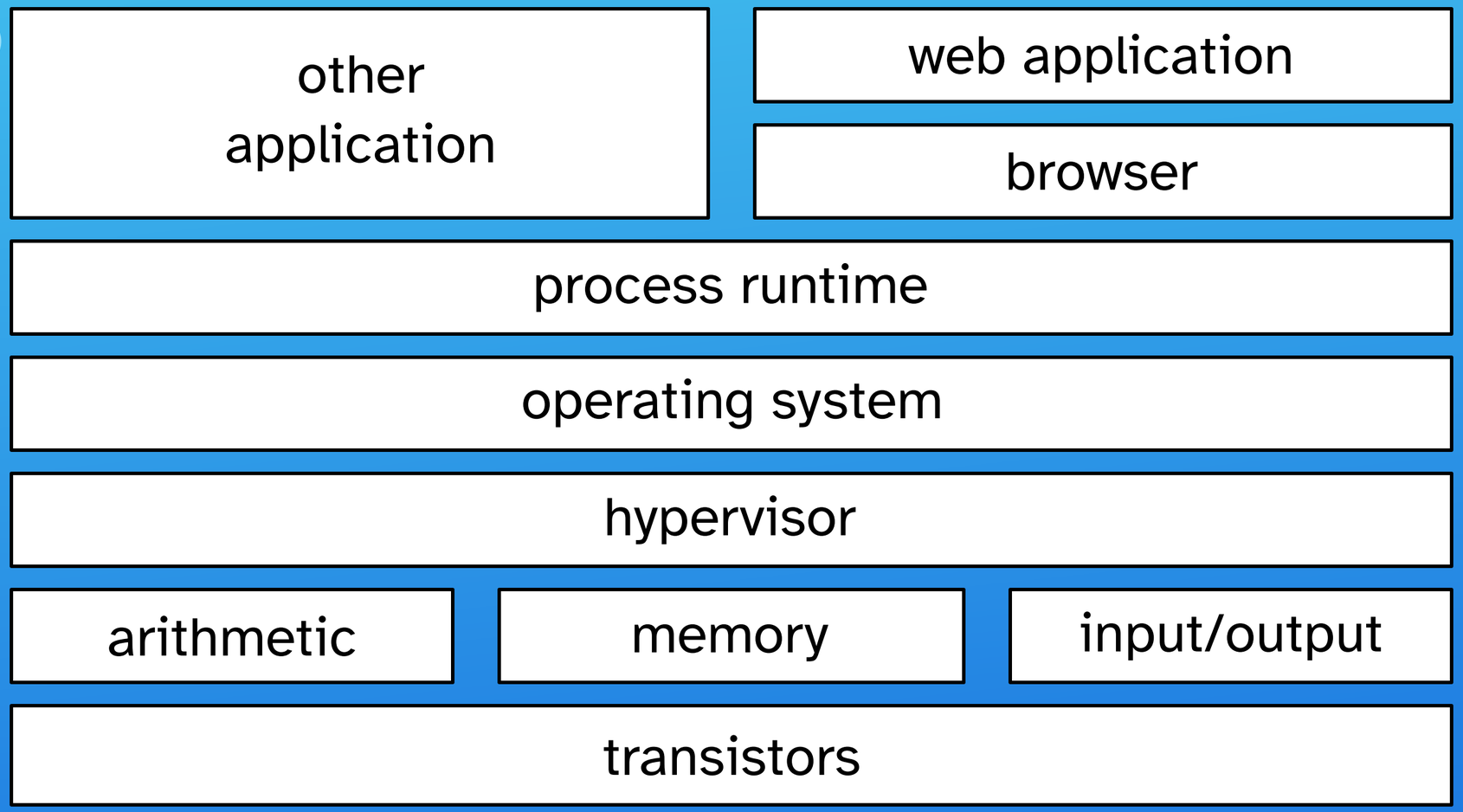
normal Return-Oriented Programming:



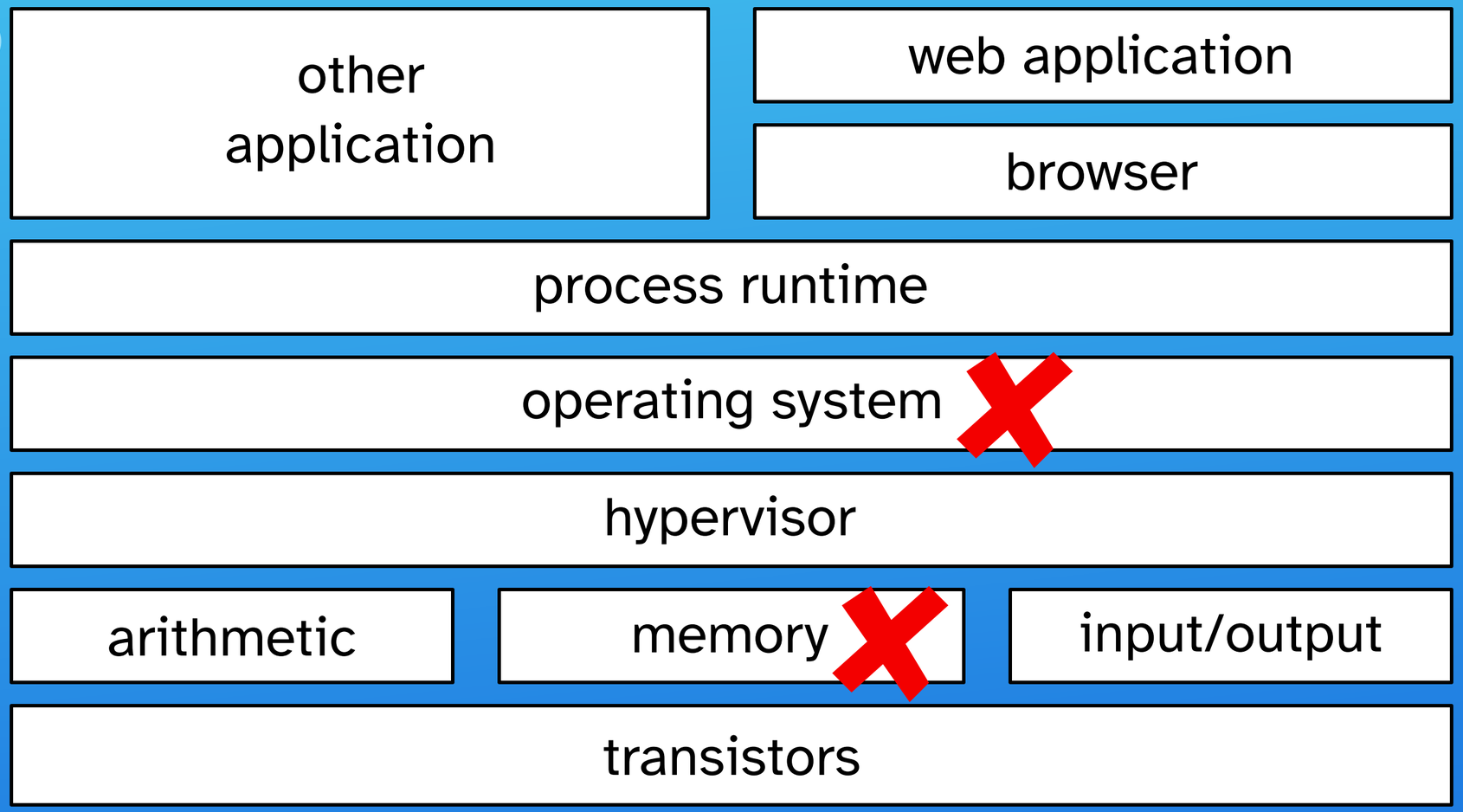
SigReturn-Oriented Programming:



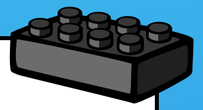
Dedup est Machina



Dedup est Machina



Dedup est Machina



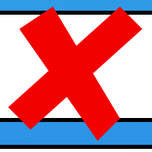
other application

web application

browser

process runtime

operating system



hypervisor

arithmetic

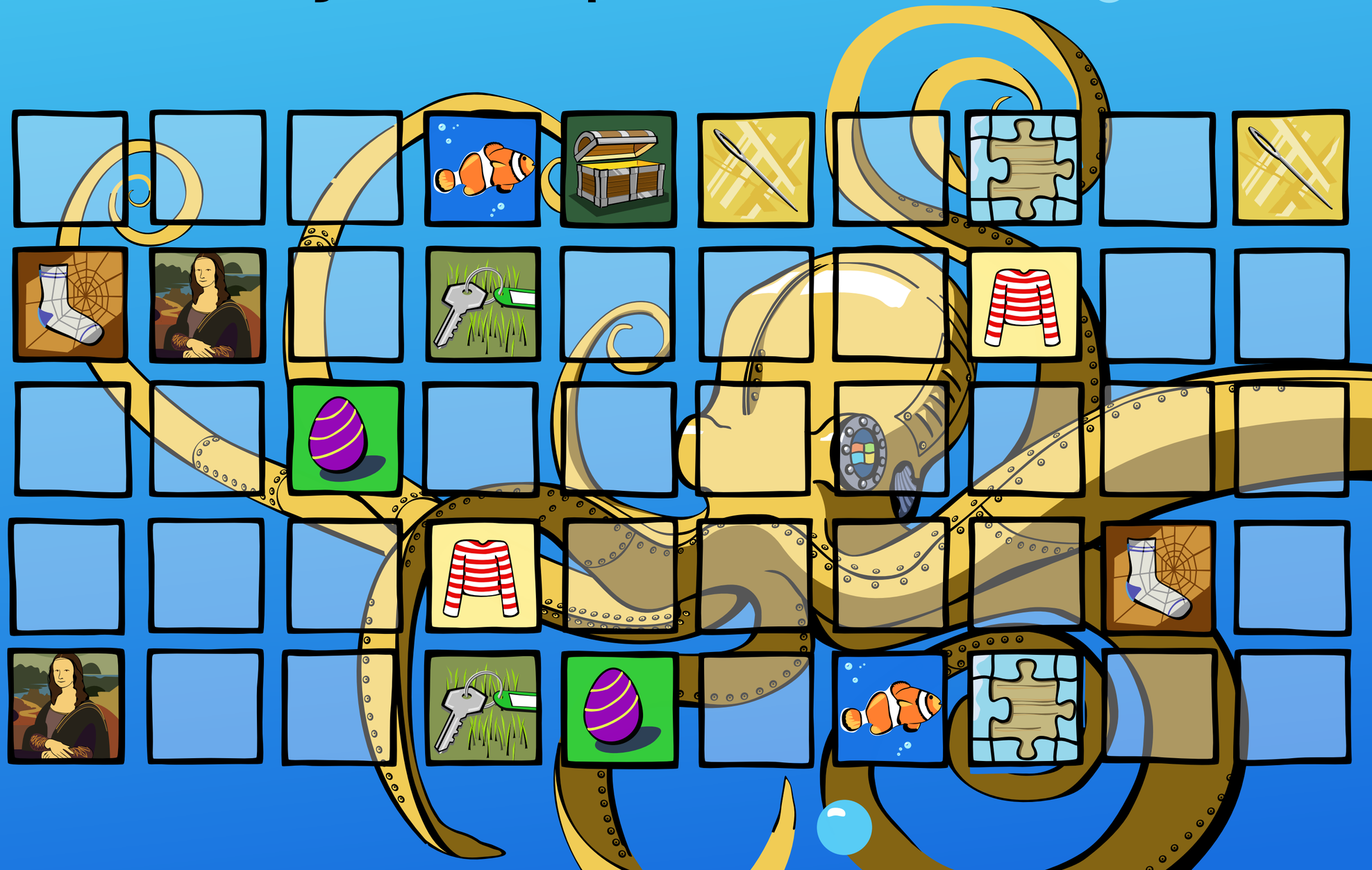
memory

input/output

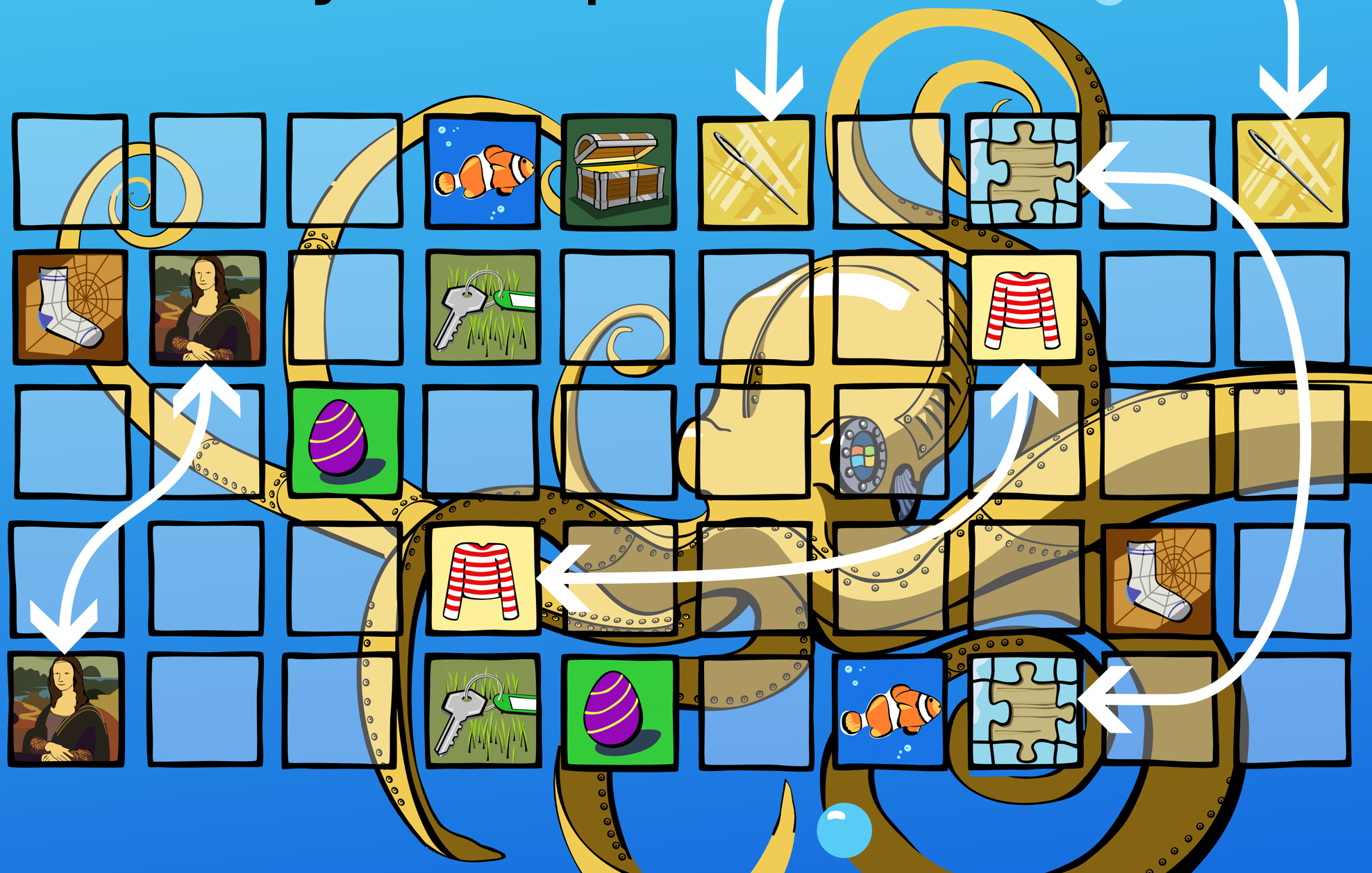
transistors

Memory Deduplication

Memory Deduplication



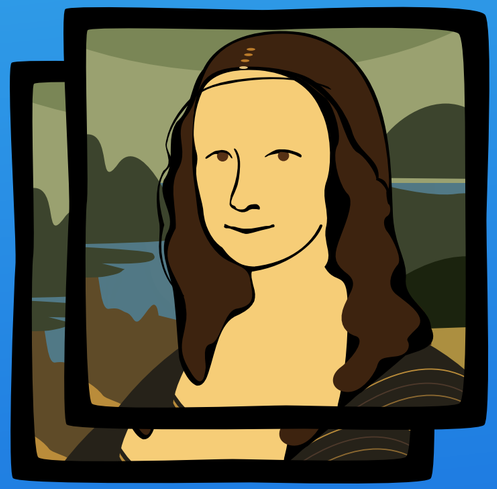
Memory Deduplication



Memory Deduplication

My memory has the only copy:

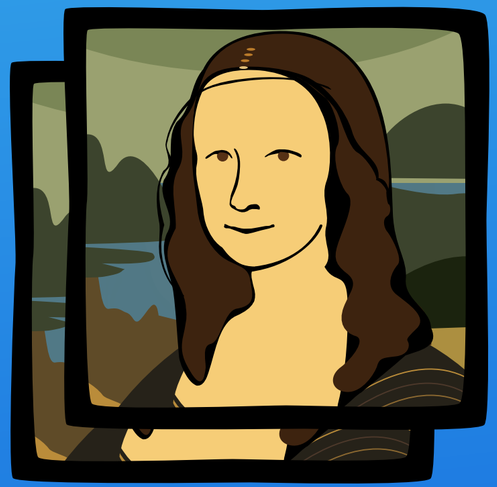
There is another copy in the system:



Memory Deduplication

My memory has the only copy:

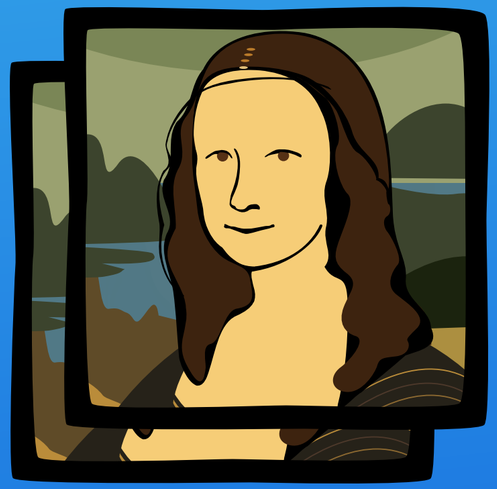
There is another copy in the system:

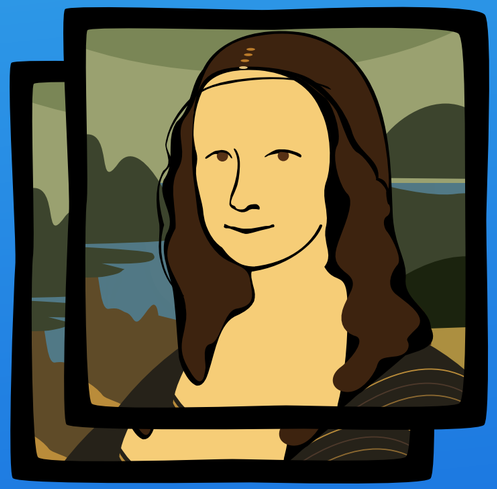


Memory Deduplication

My memory has the only copy:

There is another copy in the system:

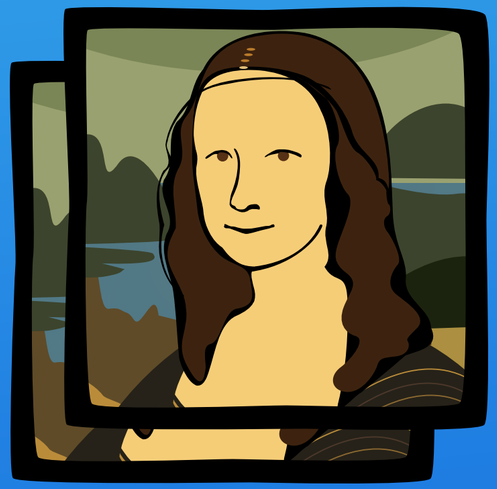


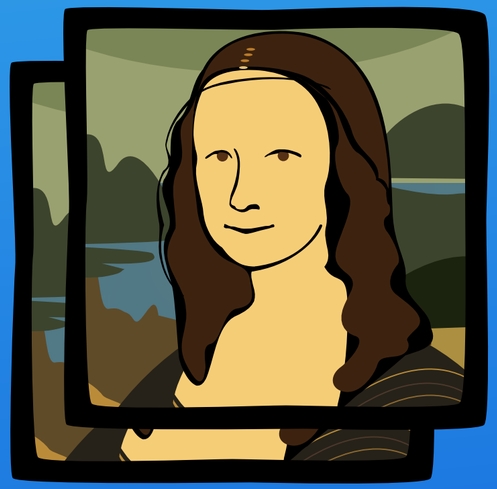


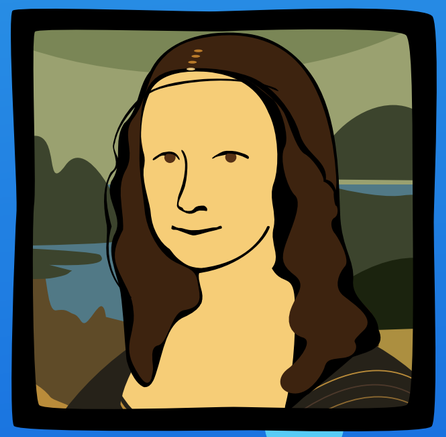
Memory Deduplication

My memory has the only copy:

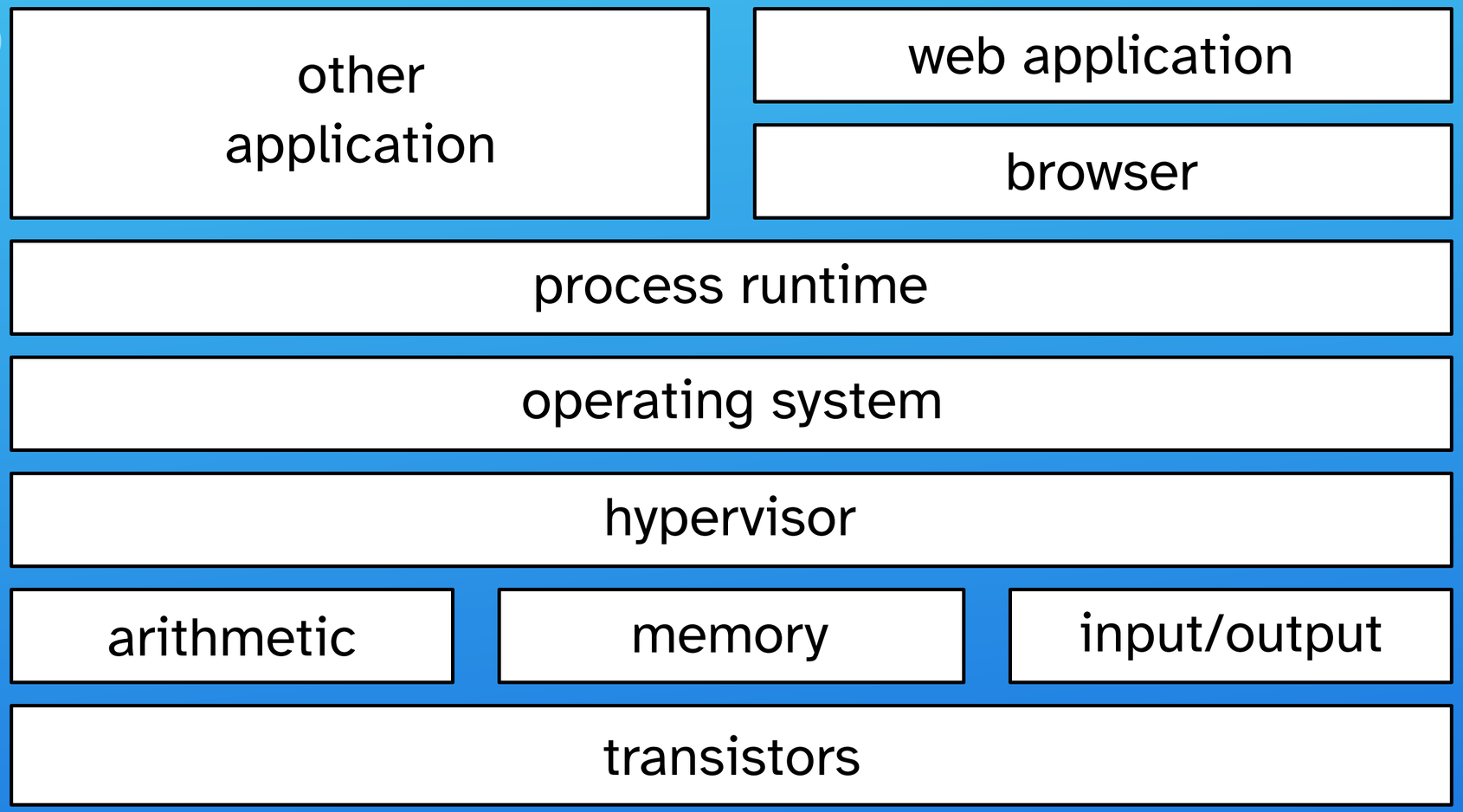
There is another copy in the system:



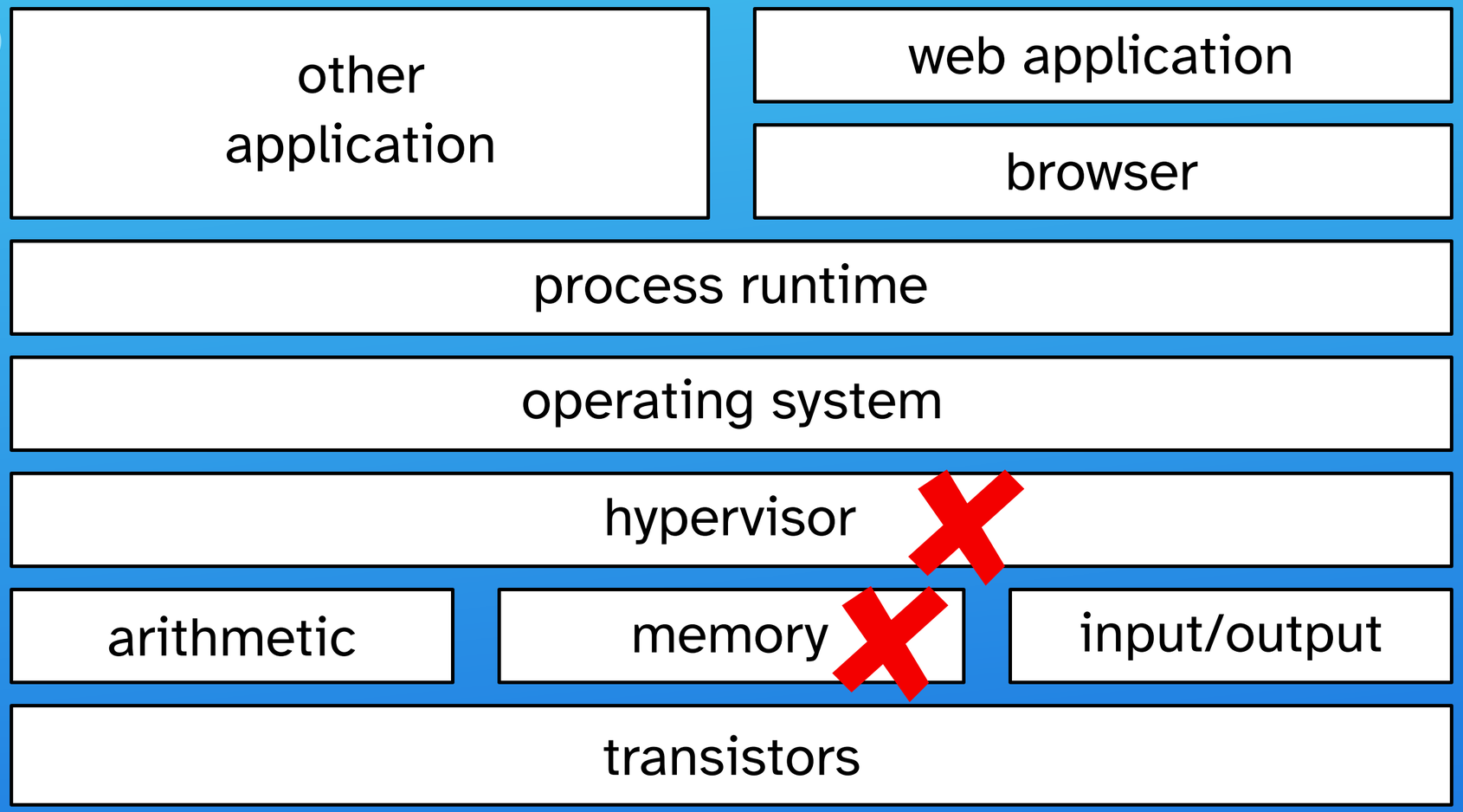




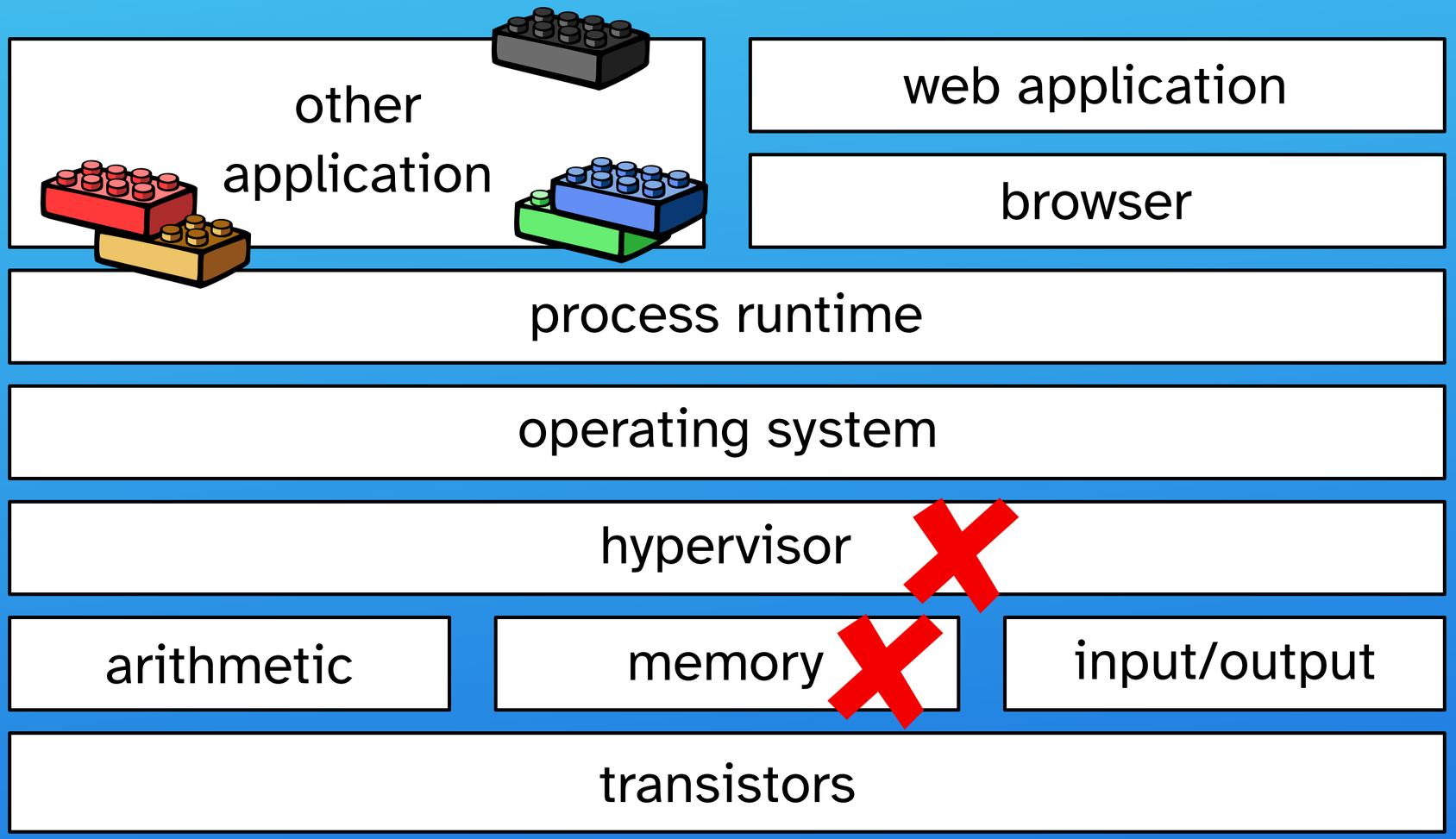
Flip Feng Shui



Flip Feng Shui



Flip Feng Shui

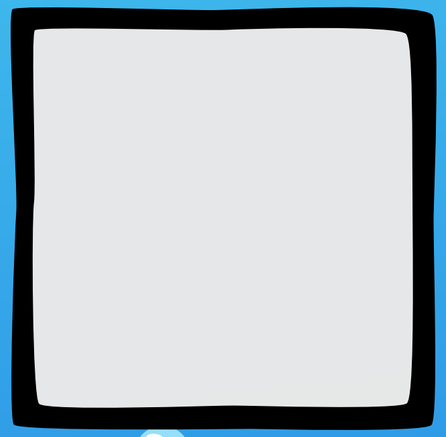


Flip Feng Shui

Target data (allowed login keys):

Flip Feng Shui

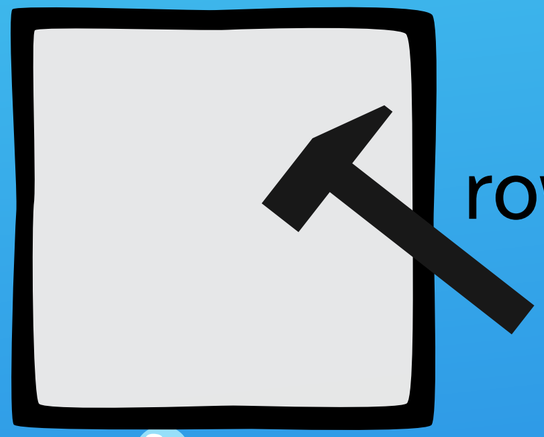
My memory:



Target data (allowed login keys):

Flip Feng Shui

My memory:

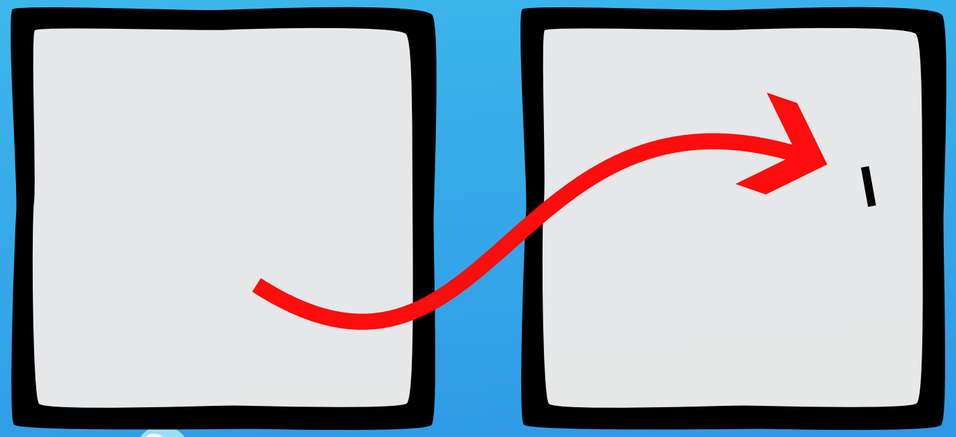


rowhammer

Target data (allowed login keys):

Flip Feng Shui

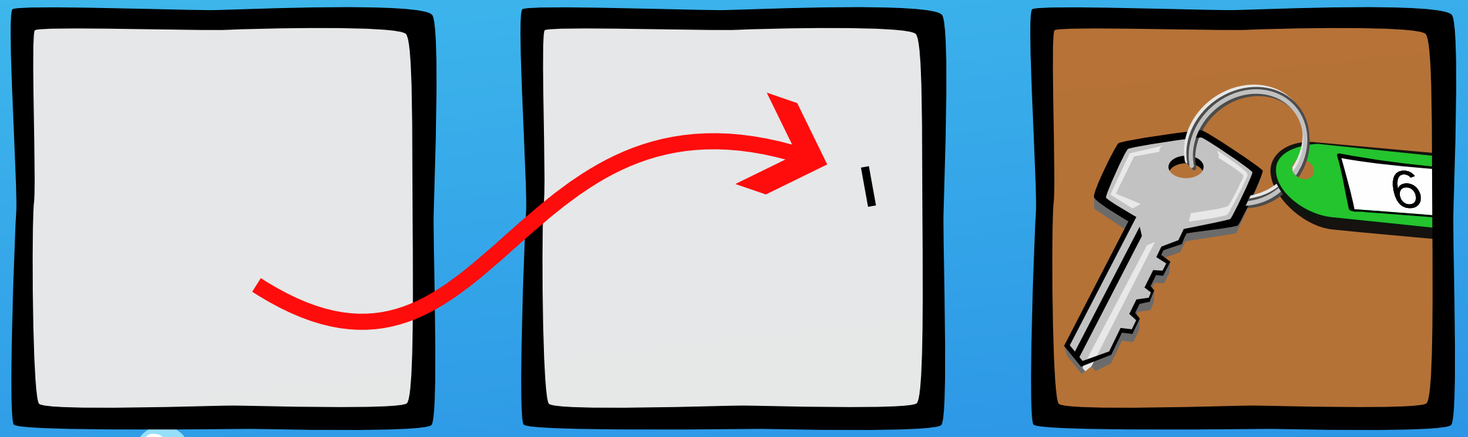
My memory:



Target data (allowed login keys):

Flip Feng Shui

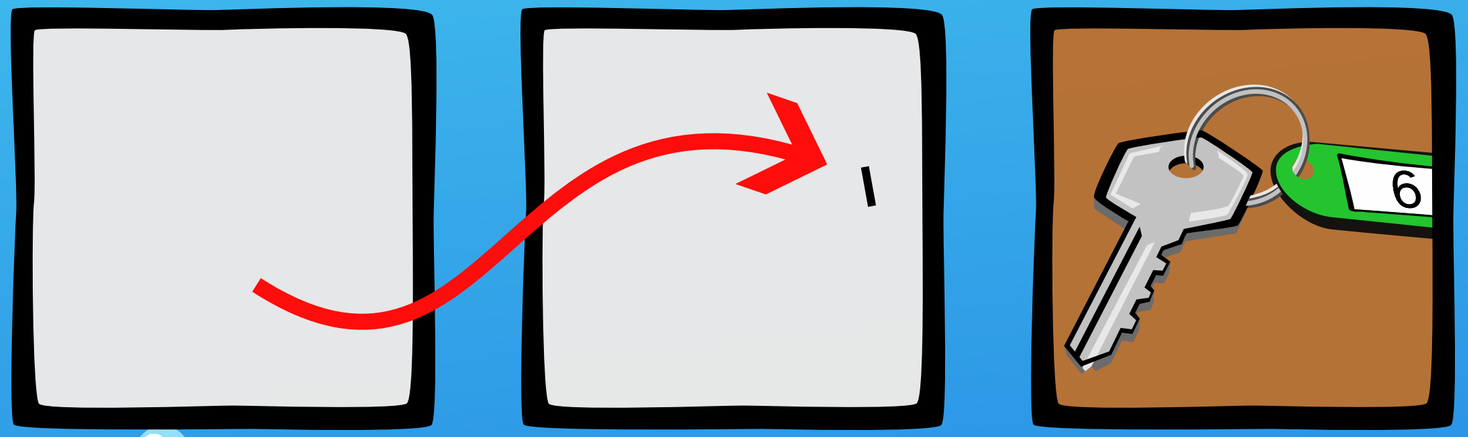
My memory:



Target data (allowed login keys):

Flip Feng Shui

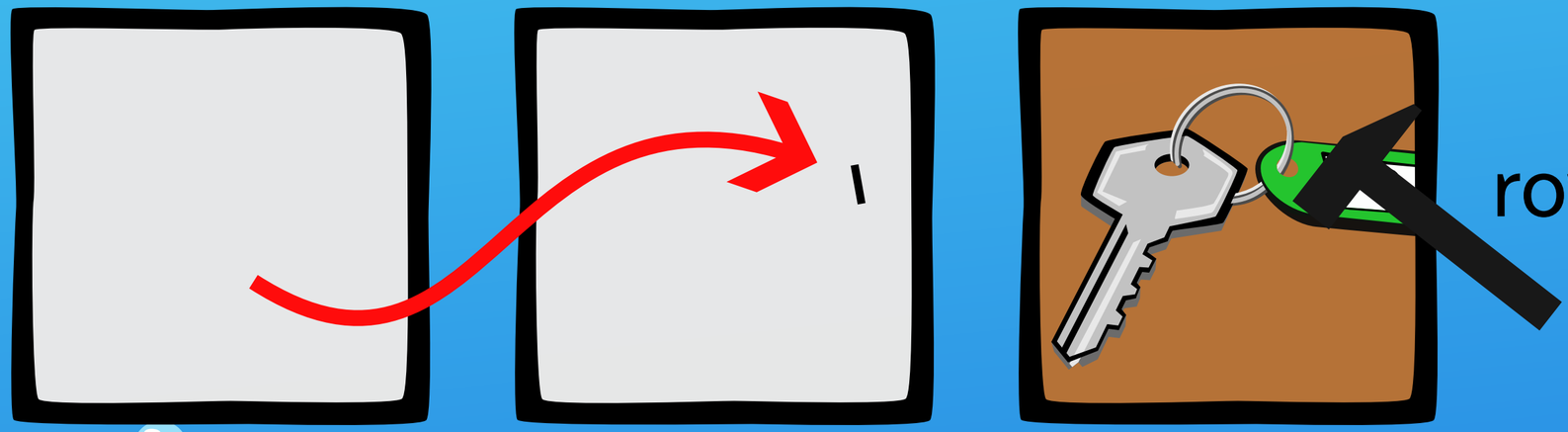
My memory:



Target data (allowed login keys):

Flip Feng Shui

My memory:

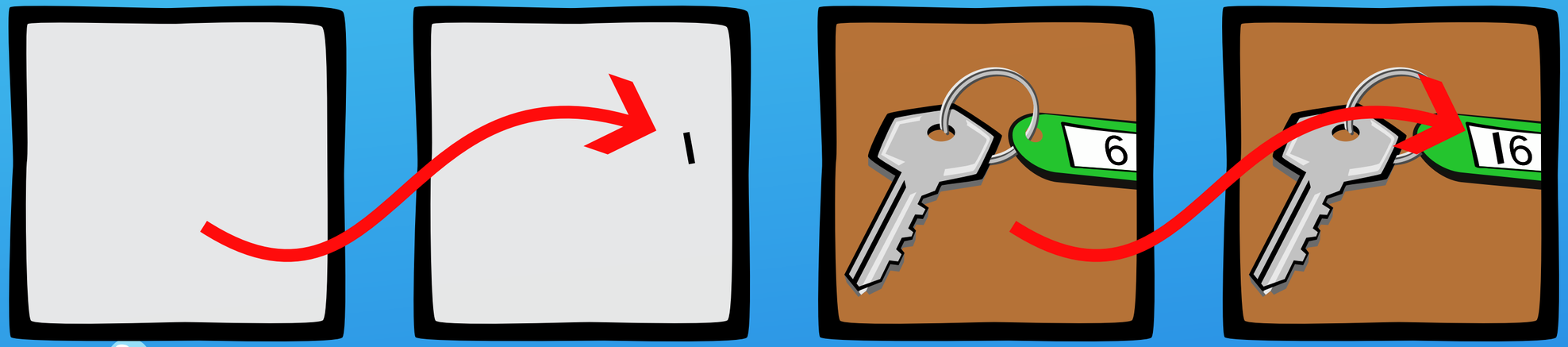


rowhammer

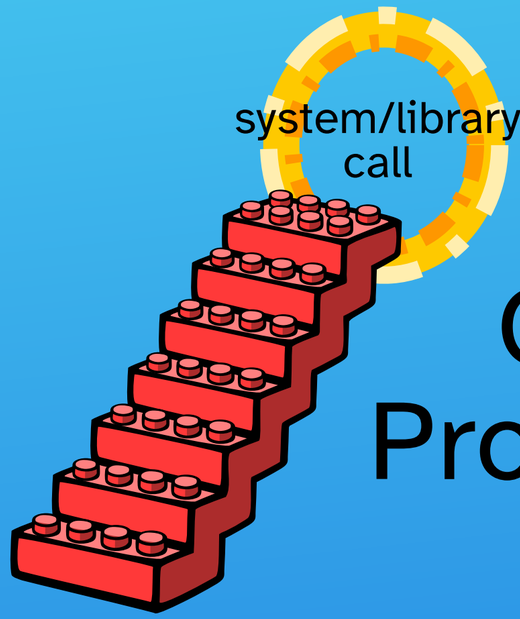
Target data (allowed login keys):

Flip Feng Shui

My memory:



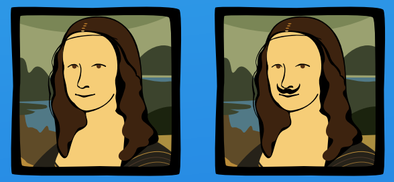
Target data (allowed login keys):



SigReturn Oriented Programming

Dedup est Machina

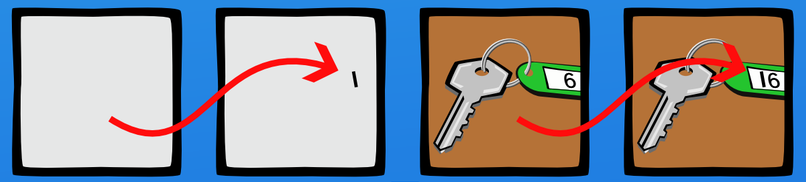
My memory has the only copy:



There is another copy in the system:

Flip Feng Shui

My memory:



Target data (allowed login keys):