Meltdown and Spectre:
Complexity and the death of security

Dr. Michael S. Kirkpatrick

May 8, 2018

Meltdown and Spectre:

Wait, my computer does what?

Dr. Michael S. Kirkpatrick

May 8, 2018

JAMES MADISON UNIVERSITY

Meltdown and Spectre:

Whoever thought that was a good idea?

Dr. Michael S. Kirkpatrick

May 8, 2018

JAMES MADISON UNIVERSITY

Meltdown and Spectre:

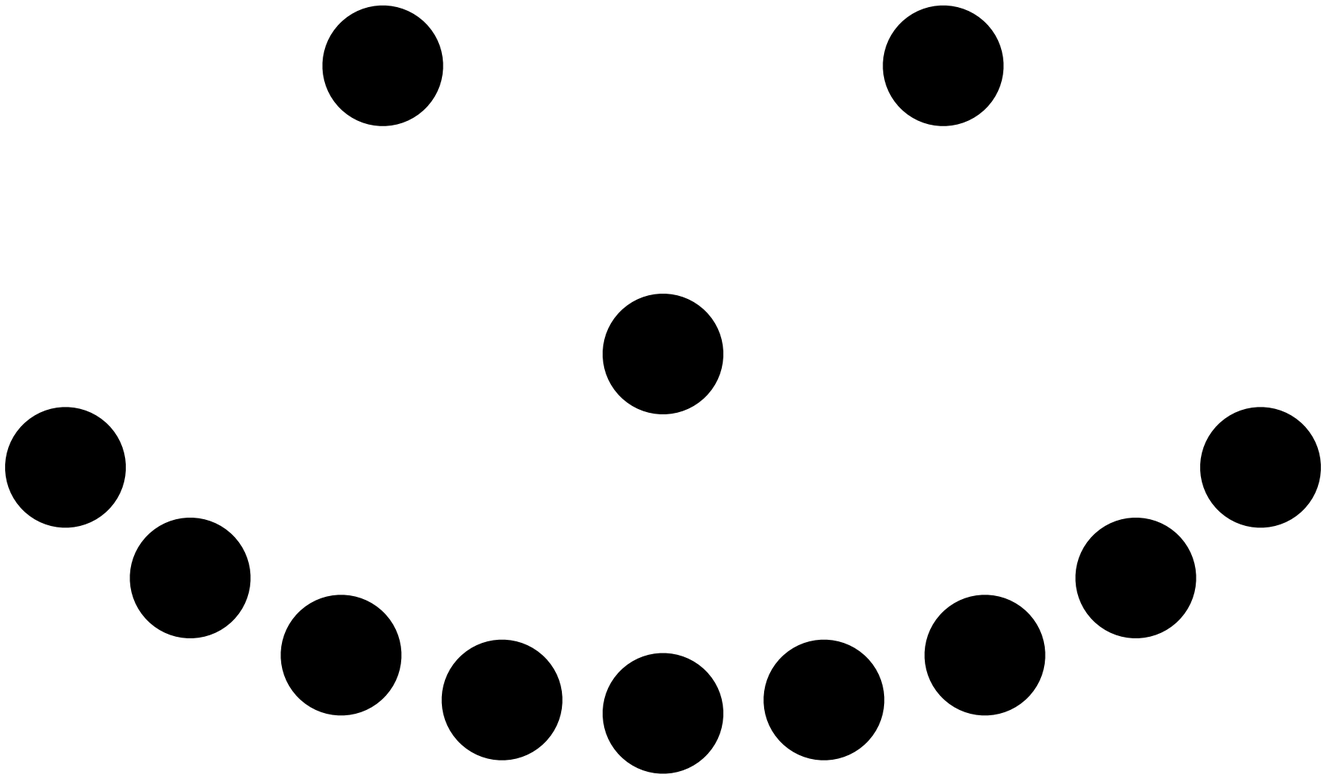
I give up. Can I just retire now?

Dr. Michael S. Kirkpatrick

May 8, 2018

JAMES MADISON UNIVERSITY

No one alive understands how computers behave.



Kernel co-location

Race conditions

Page tables

Cache mapping

Process forks

Branch prediction

Cache hierarchy

Out-of-order execution

Pipelined CPU design

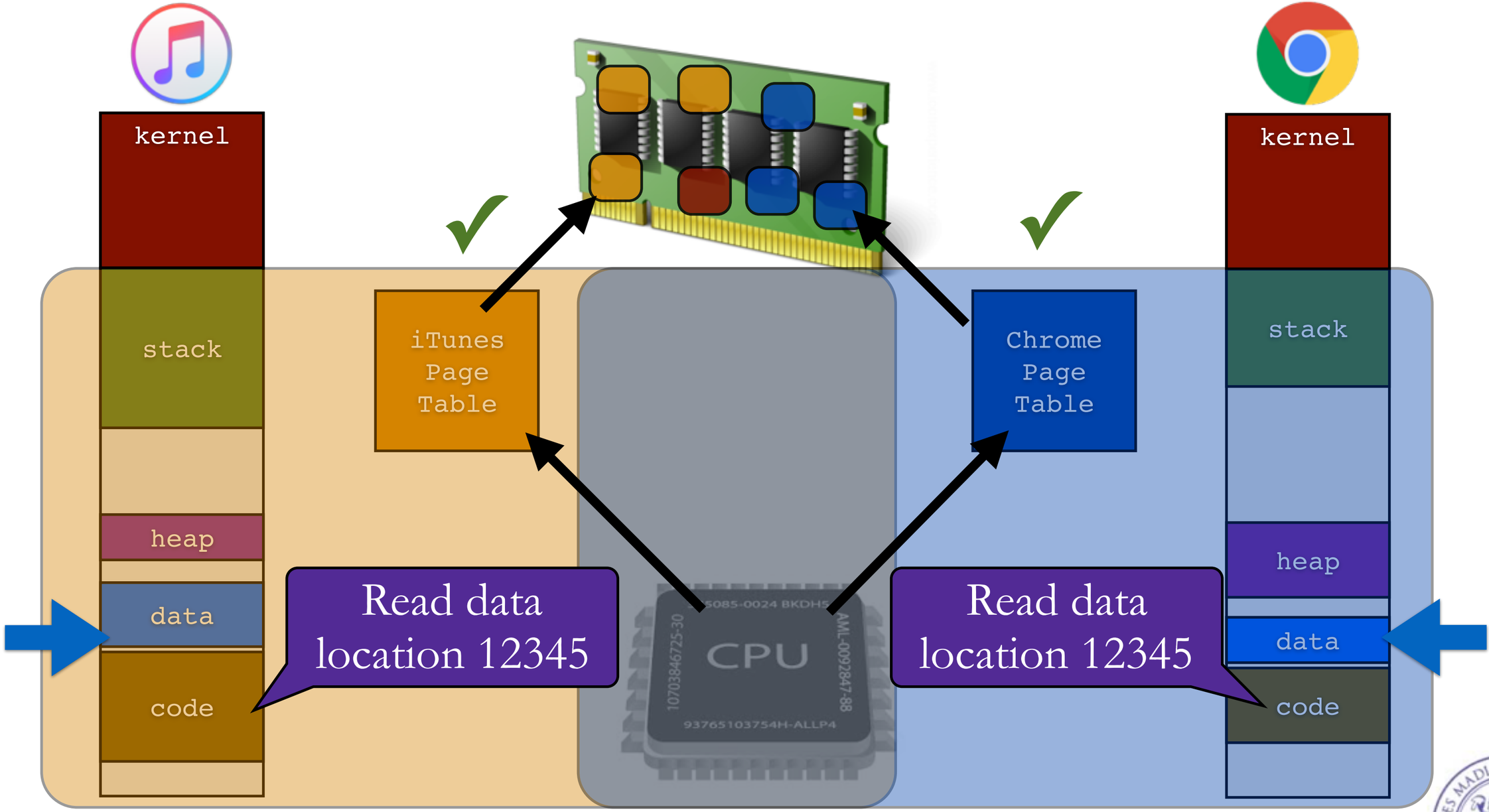
High-resolution timers

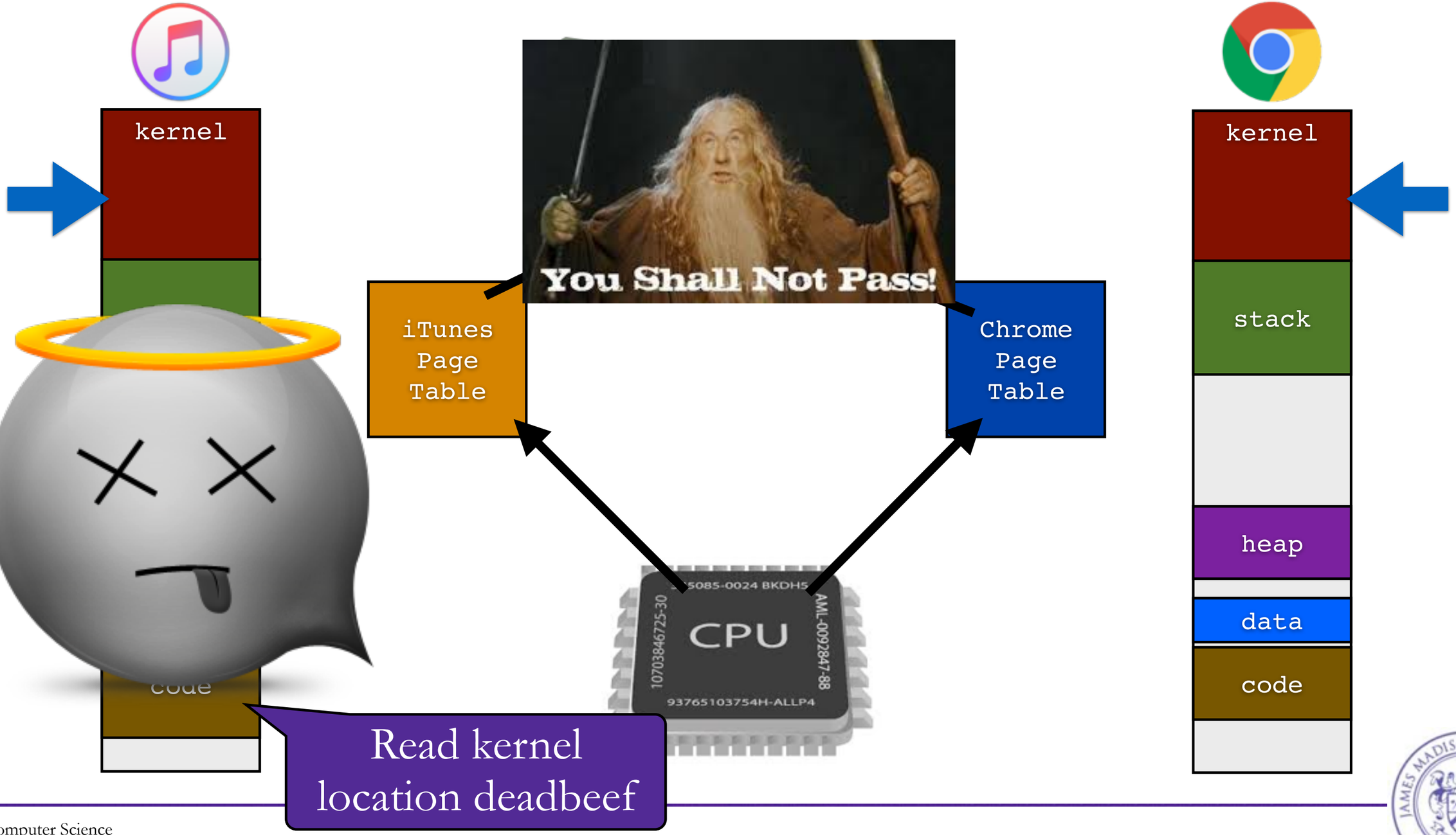
Speculative execution

Physical memory map

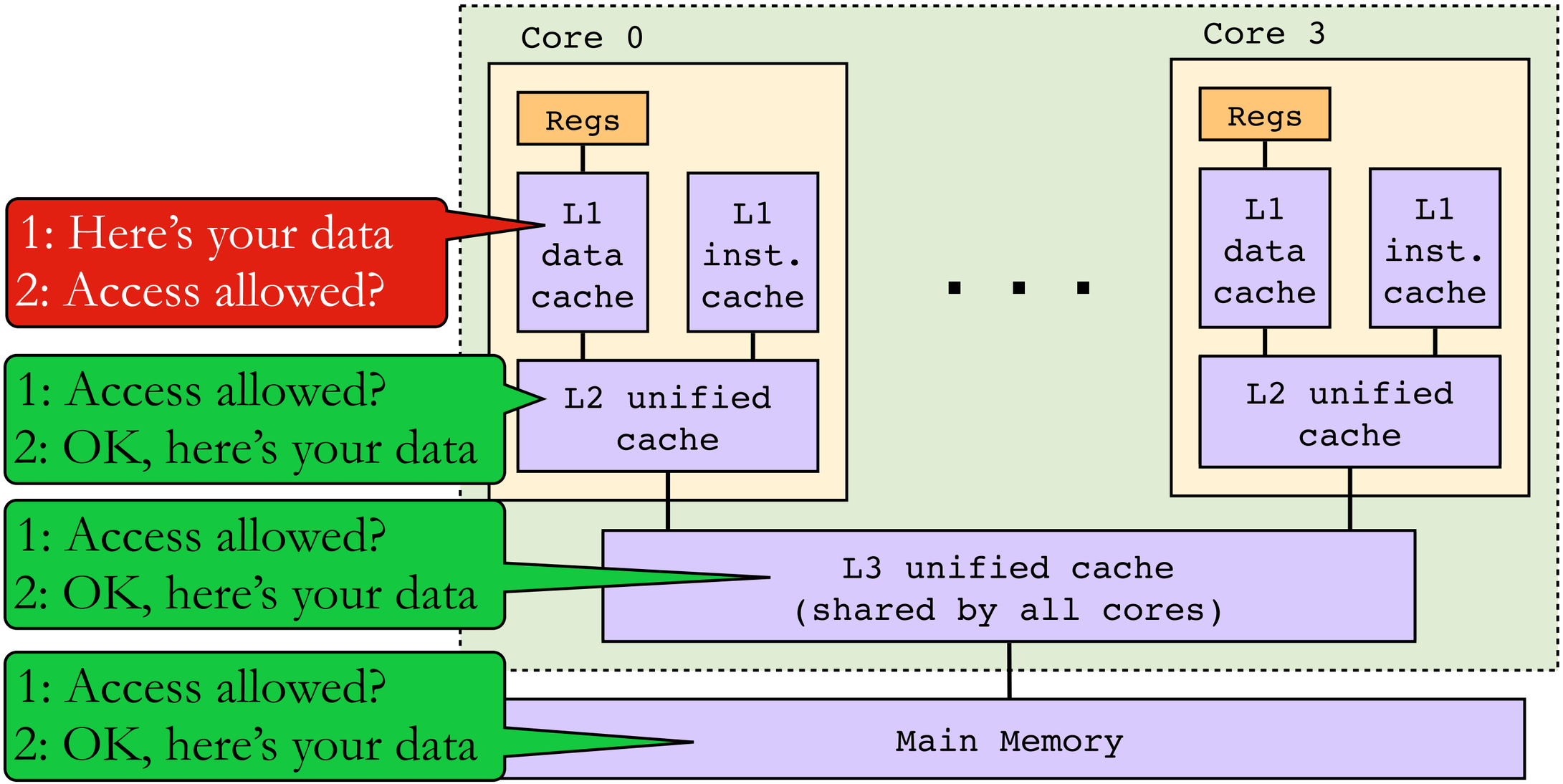
Computers are complex systems.

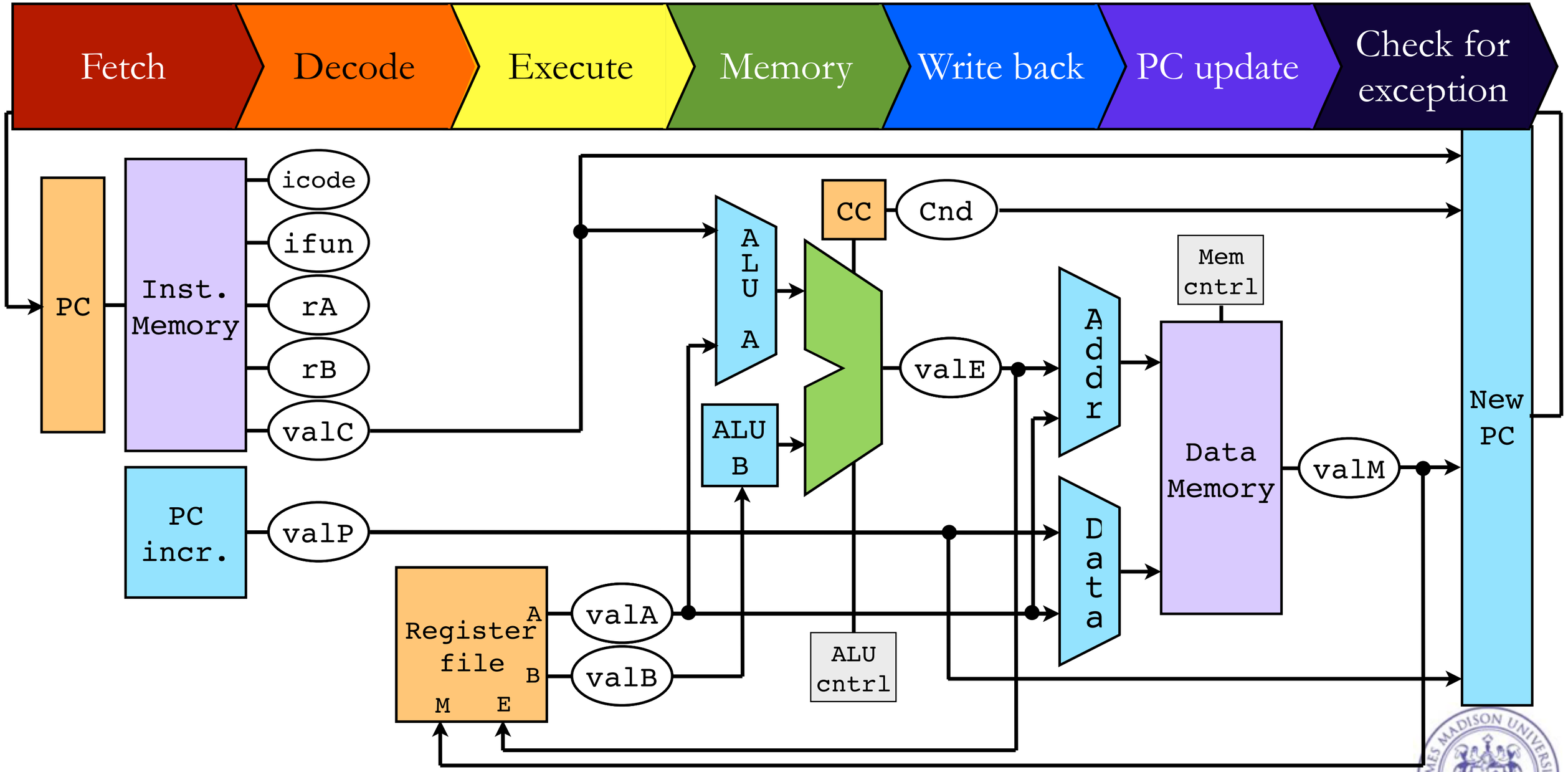

CPU
Xen


kernel
stack
heap
data
code
iTunes
Page
Table
Chrome
Page
Table
Read data
location 12345
Read data
location 12345
CPU
kernel
stack
heap
data
code

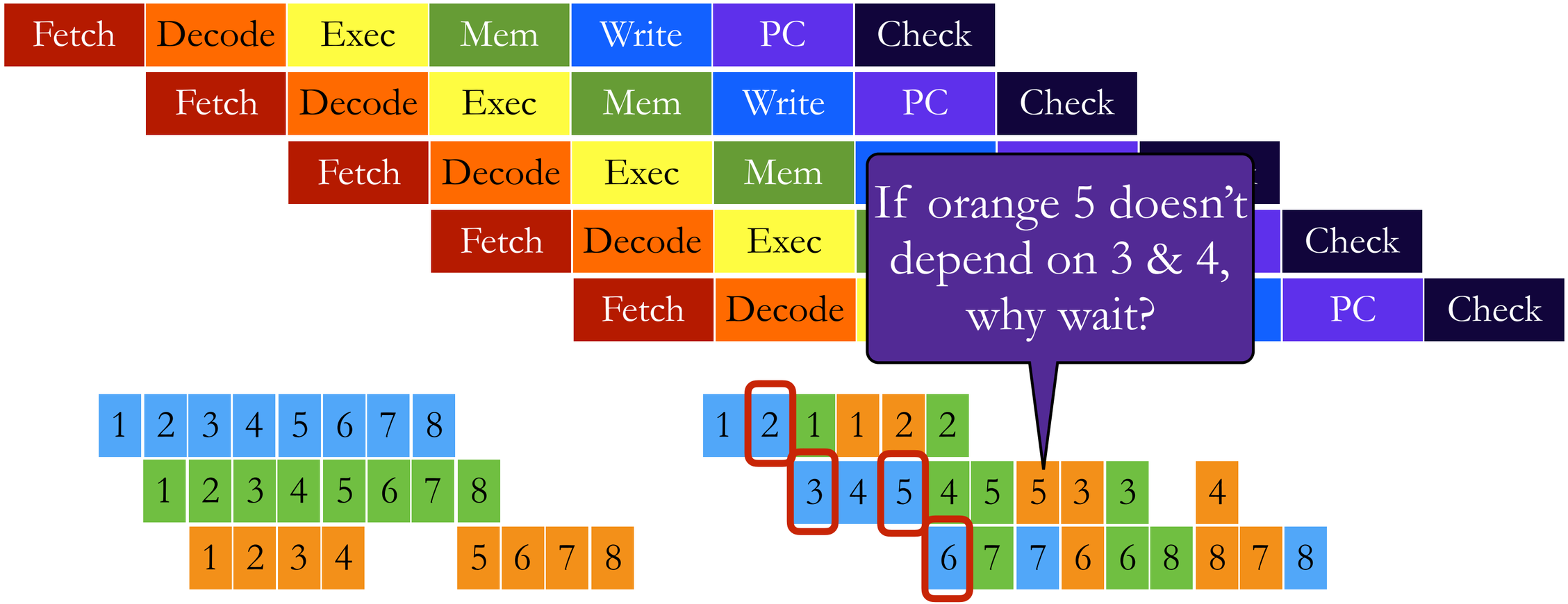

kernel
You Shall Not Pass!
iTunes Page Table
Chrome Page Table
CPU
kernel
stack
heap
data
code
Read kernel location deadbeef

Memory hierarchy and cache

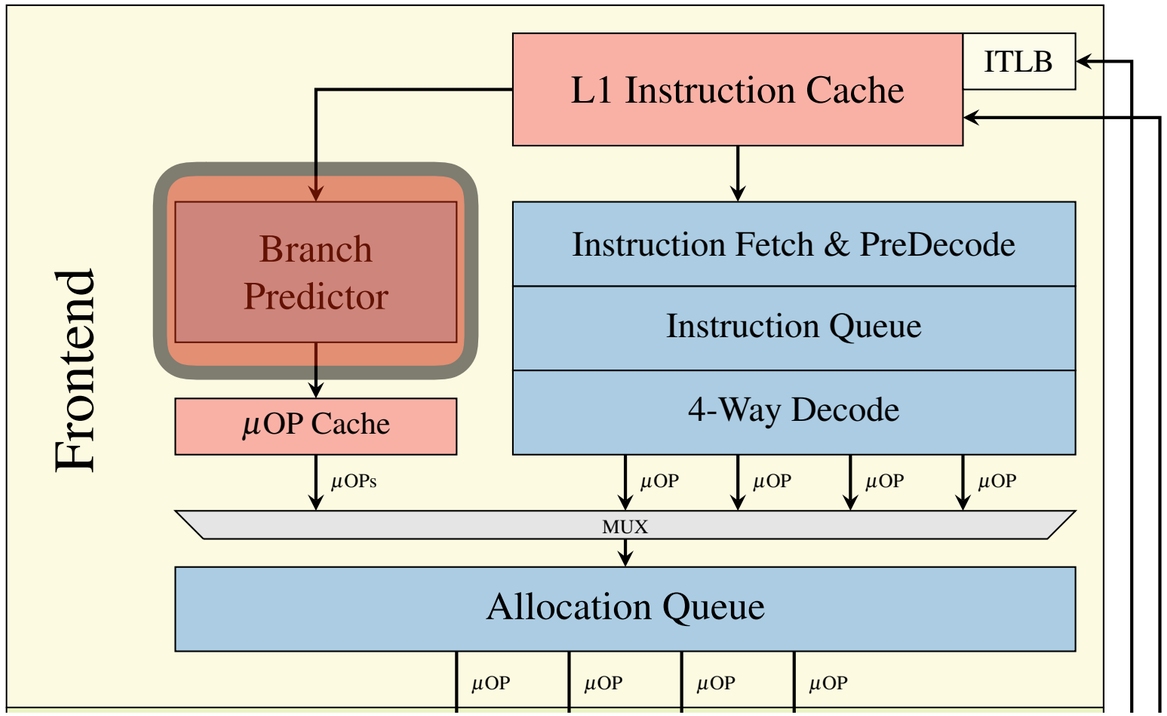


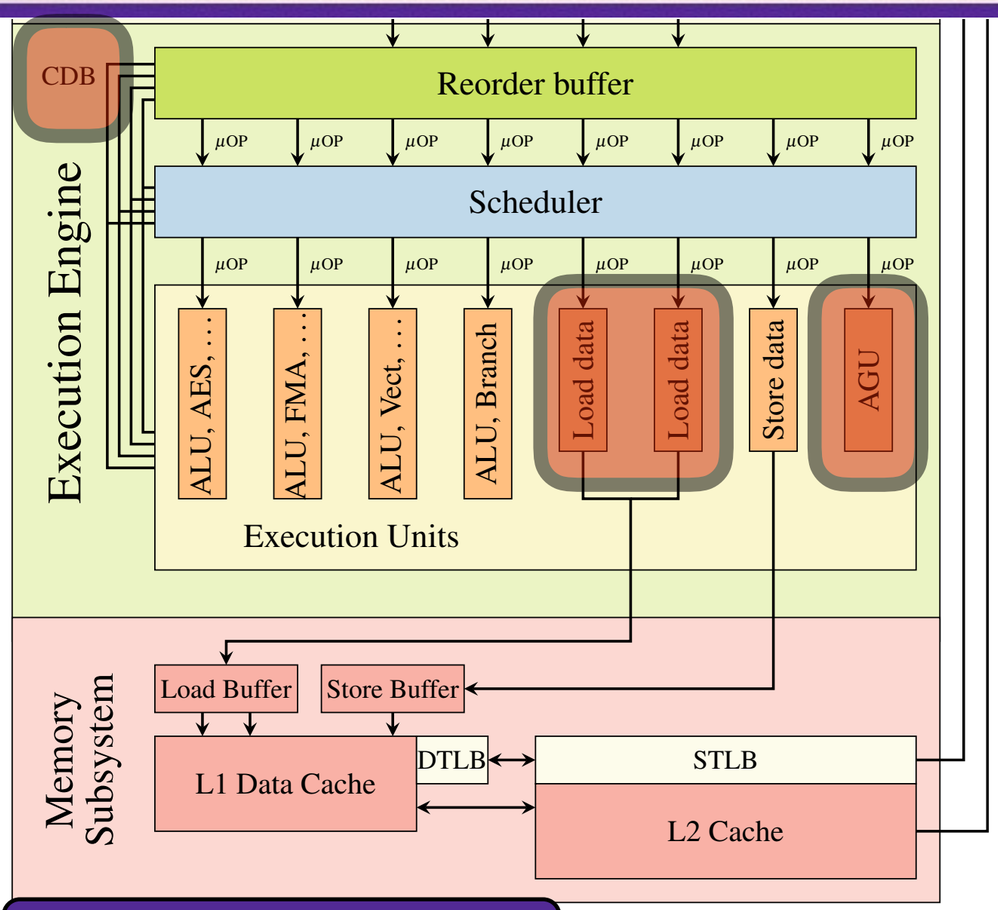

Fetch
Decode
Execute
Memory
Write back
PC update
Check for exception
PC
Inst. Memory
icode
ifun
rA
rB
valC
PC incr.
valP
ALU A
ALU B
CC
Cnd
valE
Addr
Mem cntrl
Data Memory
valM
Data
New PC
Register file
A
B
M
E
valA
valB
ALU cntrl

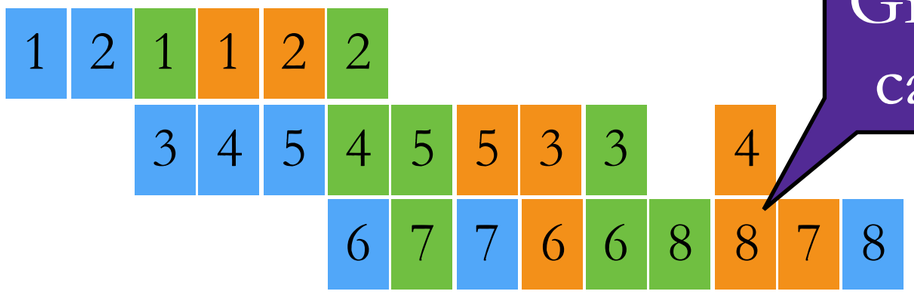
x86 Pipelining



x86 Pipelining





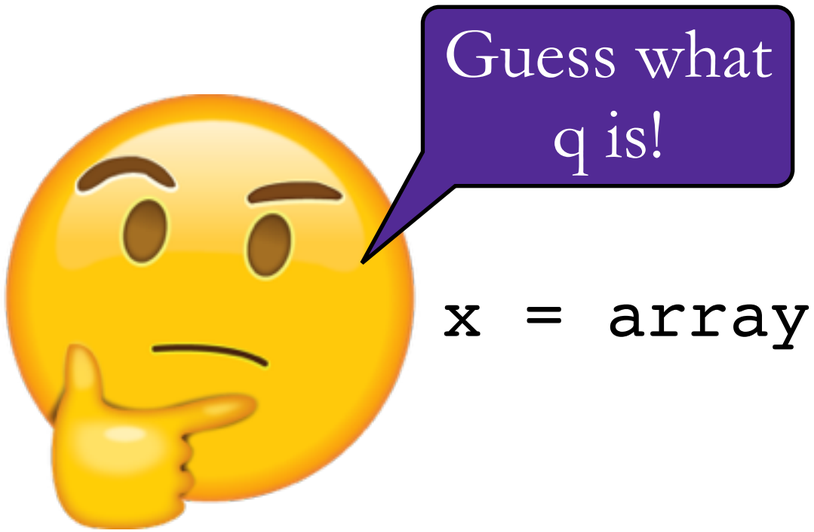


Green and orange can't "retire" yet

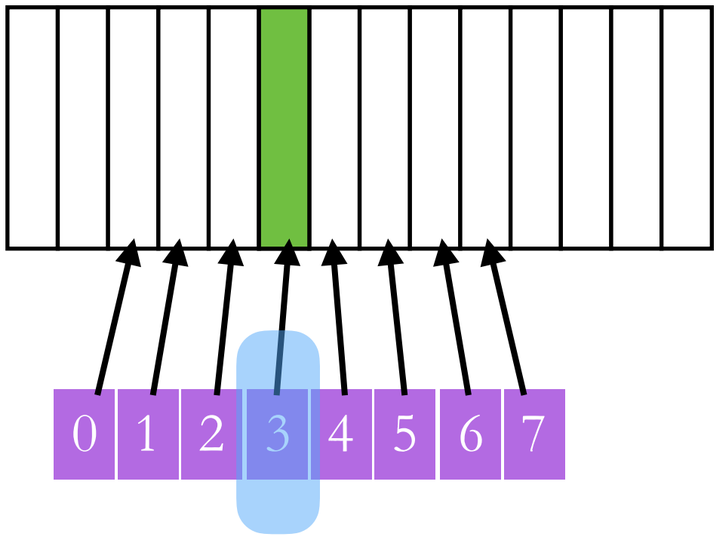
What we know so far…

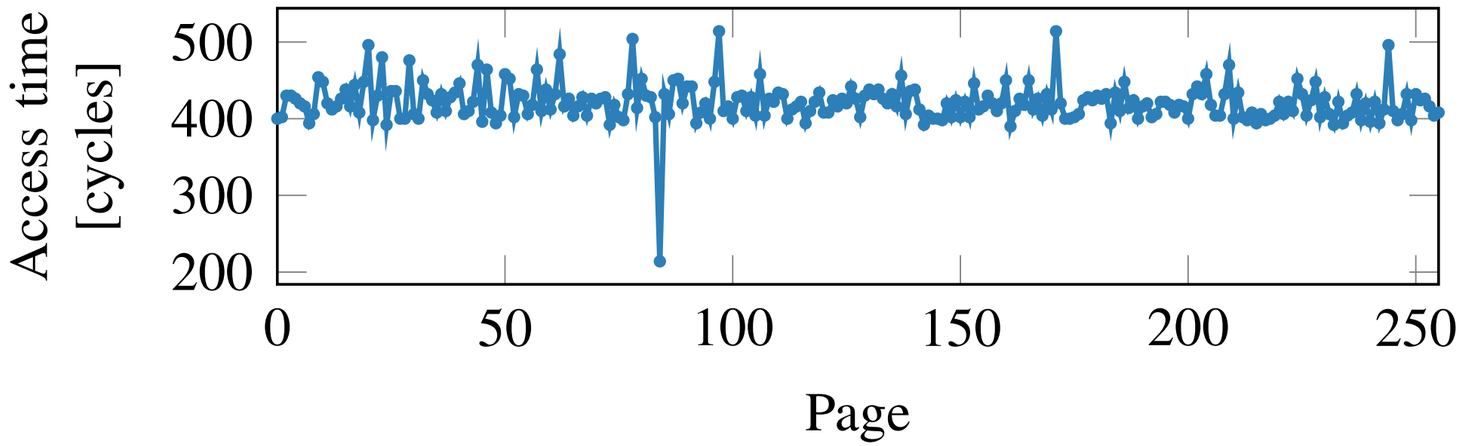
- You're not supposed to access kernel
- L1 cache timing is wrong
- x86 pipelining is complex
- Macroarchitecture != microarchitecture
  - "First" != First
- "Invisible" side effects are visible

Cache-based side channels




```
x = array[q];
```






```
for (i = 0; i < 8; i++) {
   start_timer();
   y = array[i];
   stop_timer();
}
```

Meltdown

```
1 ; rcx = kernel address
2 ; rbx = probe array
3 ret
4 mo          [rcx]
5 sh
6 jz
7 mov rbx, qword [rbx + rax]
```

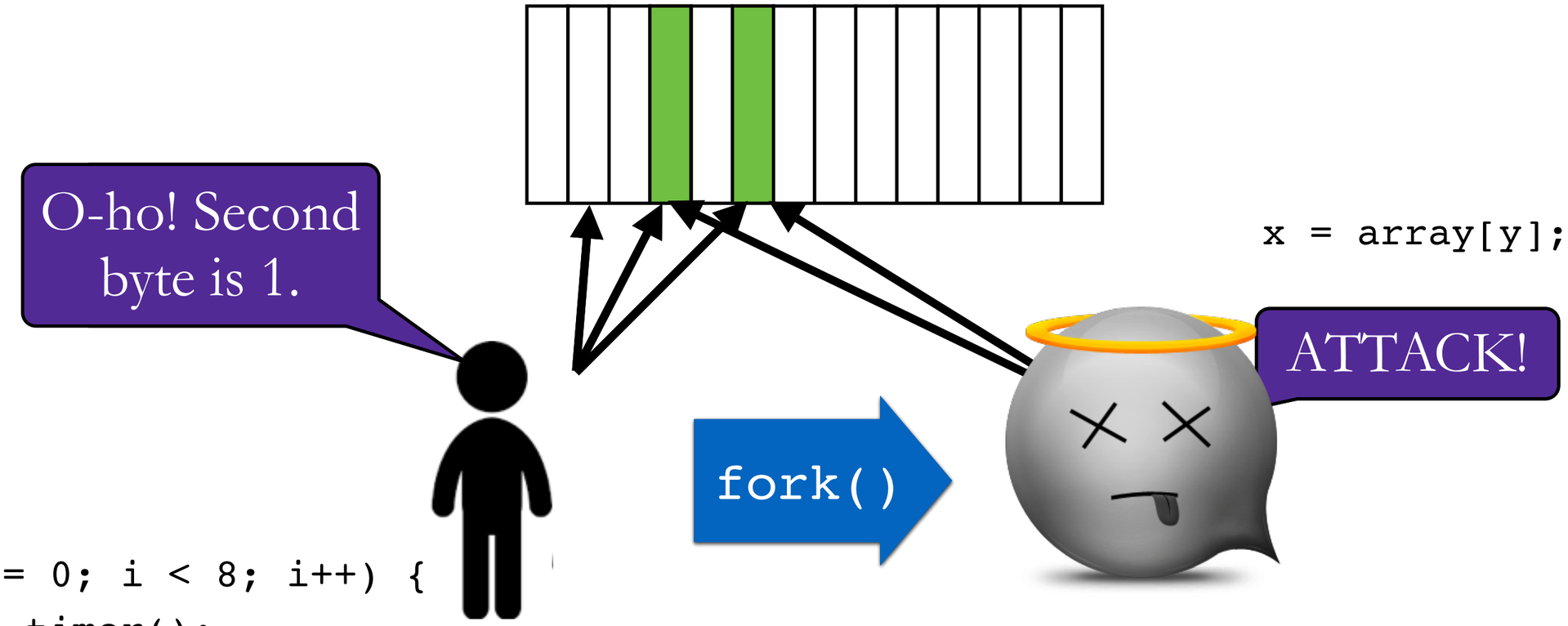
Read a byte of the kernel

Multiply byte by 4096

Use value to hit cache line

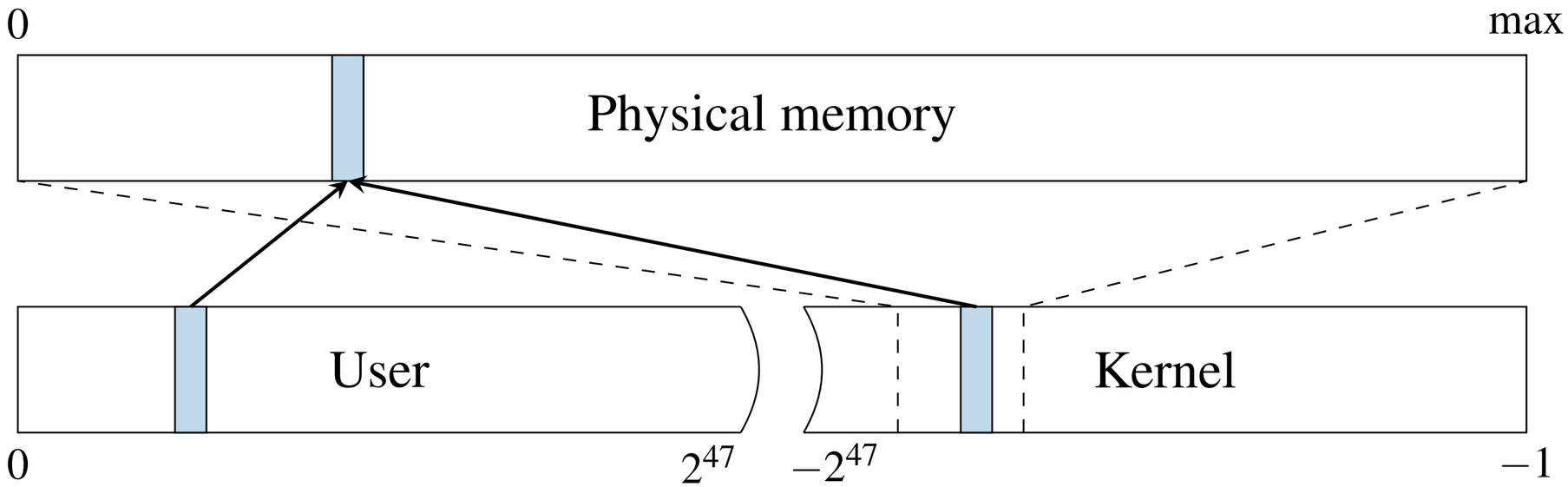
8: Maybe I should check if step 4 was valid…

Meltdown




```
for (i = 0; i < 8; i++) {
  start_timer();
  y = array[i];
  stop_timer();
}
```

Meltdown



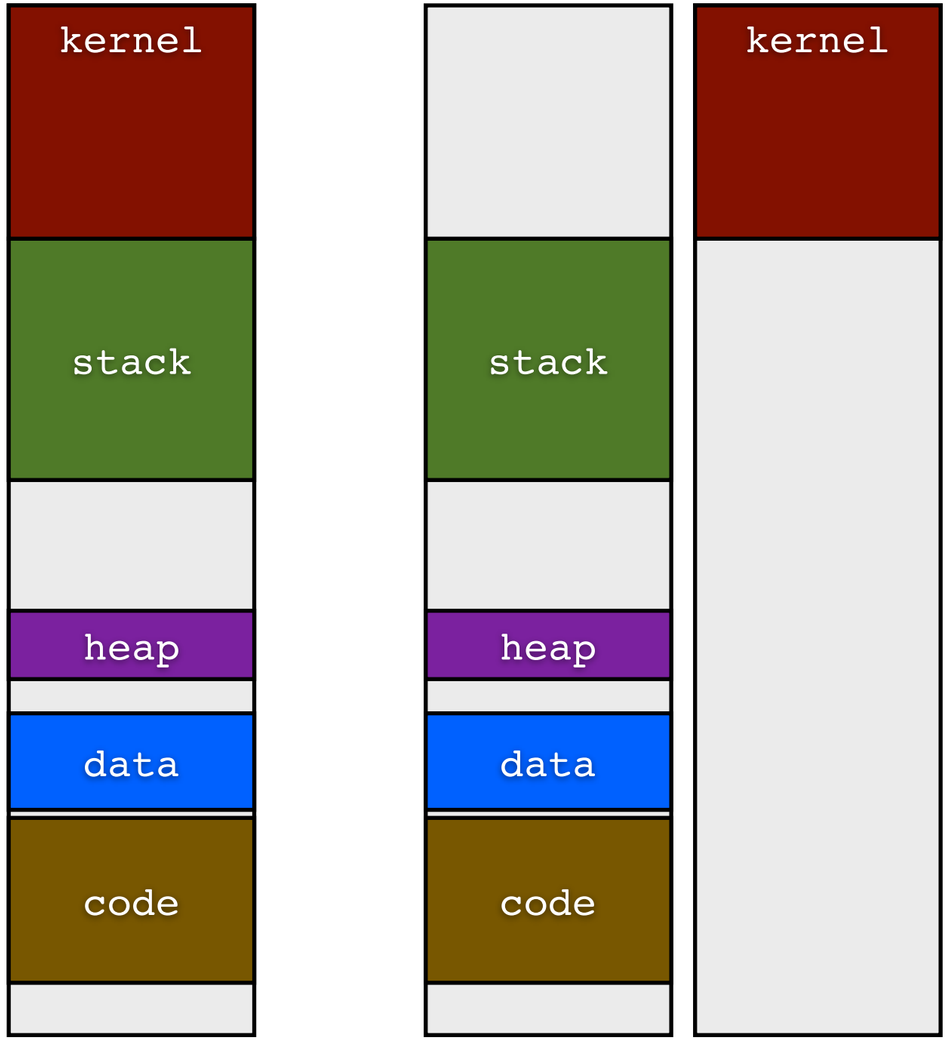
Process memory contains...

the kernel, which contains…

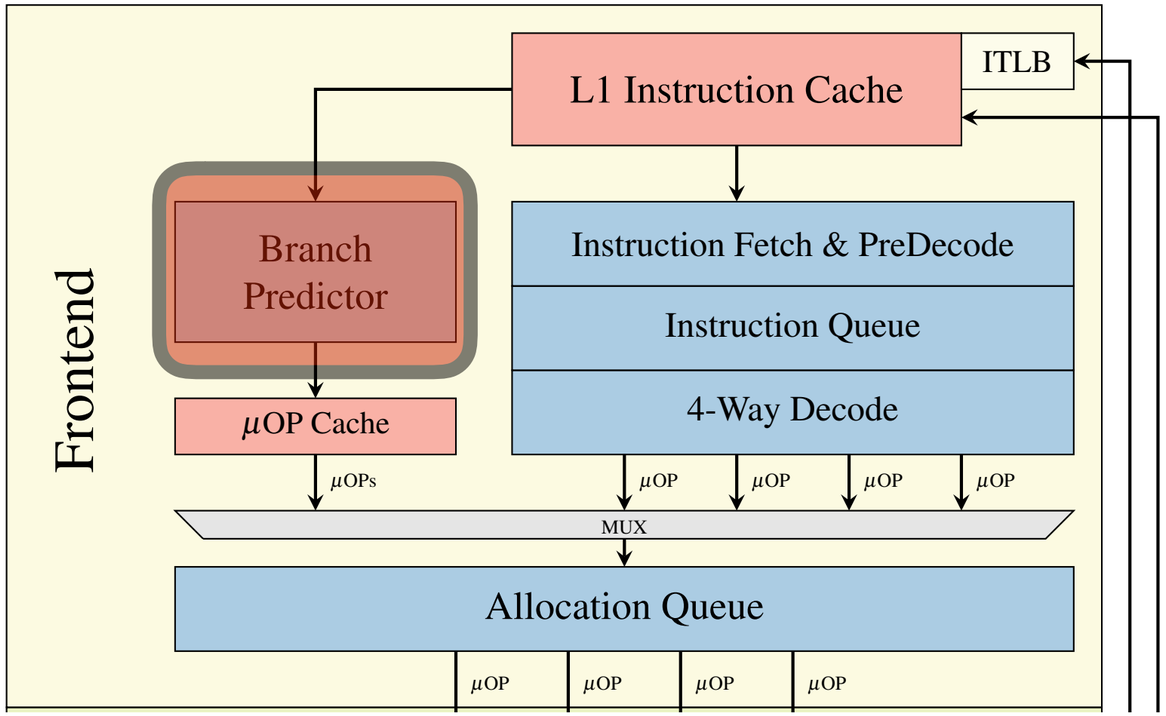
physical memory, which contains…

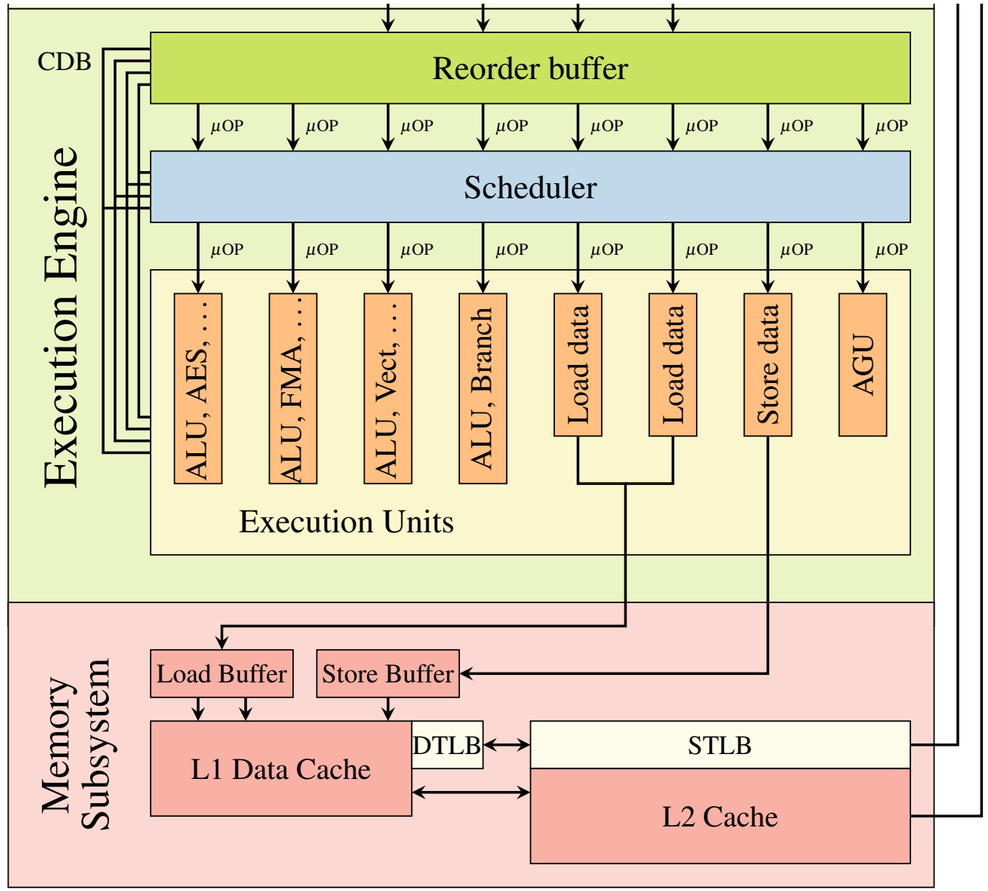
the memory contents of **every process**.

	Meltdown
Short-term fix	KAISER/PTI/ KVAS
Long-term fix	Split address space Replace hardware



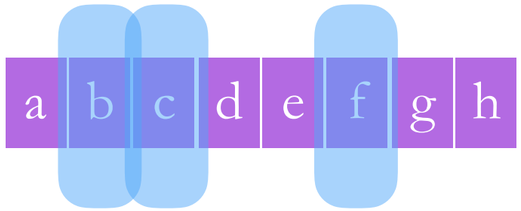
x86 Pipelining





Speculative execution

```
if (x < array_length)
  y = array[x];
```



x is 2 → y becomes c

x is 5 → y becomes f

x is 1 → y becomes b

x is 327 → y becomes

Spectre variant 1

Cache hit

Cache miss

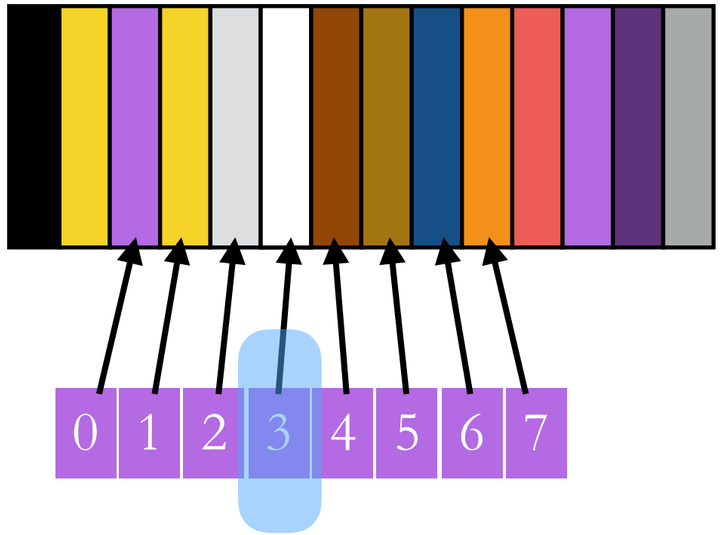
Cache hit

```
if (x < array1_size)
    y = array2[array1[x] * 256];
```

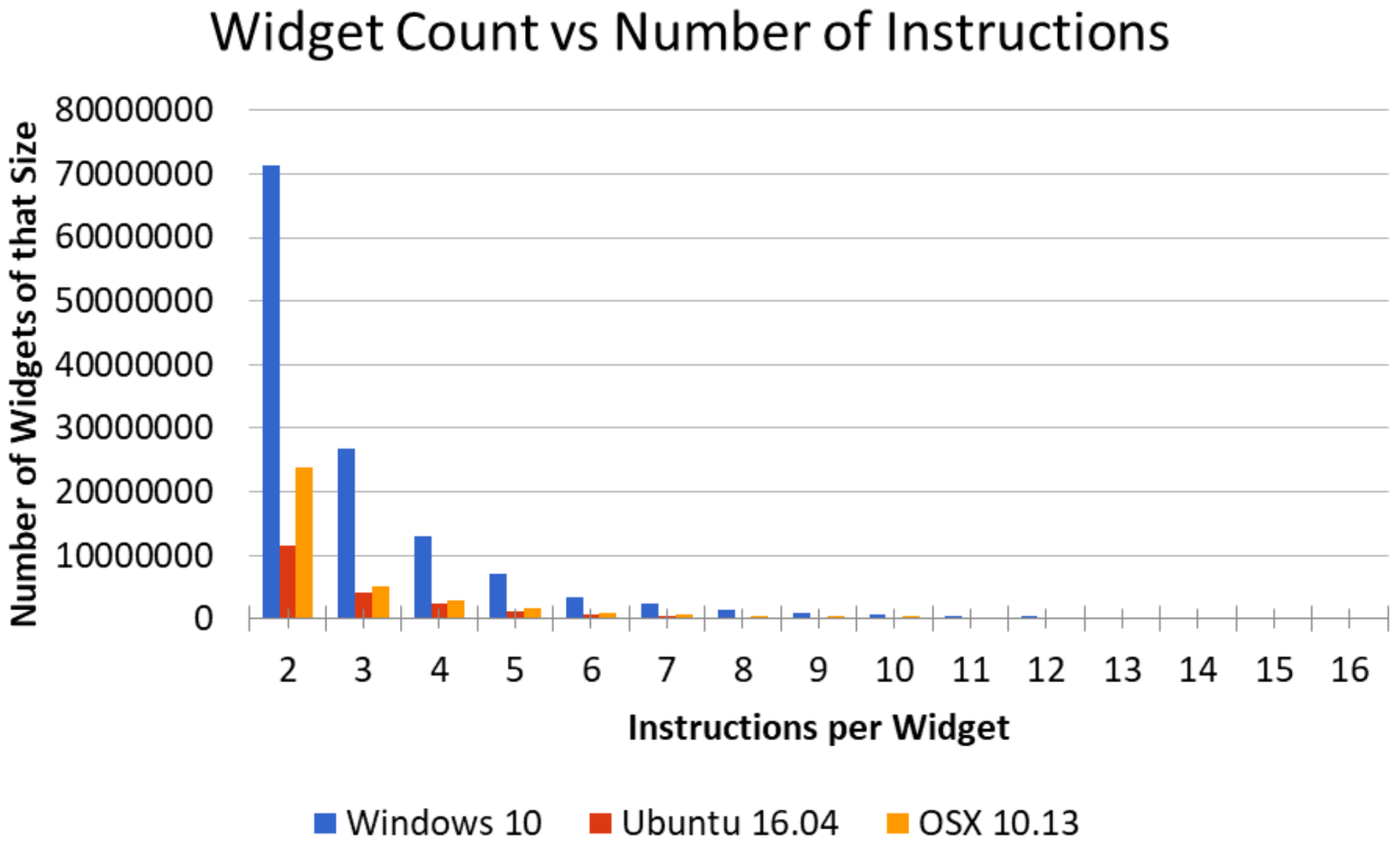
Cache miss

`x = &target - &array1`

`array1[x]` is the target



Spectre variant 2 widgets



https://34c3.cyber-itl.org/slides.pdf

	Meltdown	Spectre
Short-term fix	KAISER/PTI/ KVAS	Microcode patch OS update Recompile binaries Change compiler Browser hardening
Long-term fix	Split address space Replace hardware	????

What about applications?

CVE-2018-5093: Buffer overflow in WebAssembly during Memory/Table resizing

REPORTER	OSS-Fuzz
IMPACT	**HIGH**

Description

A heap buffer overflow vulnerability may occur in WebAssembly during Memory/Table resizing, resulting in a potentially exploitable crash.

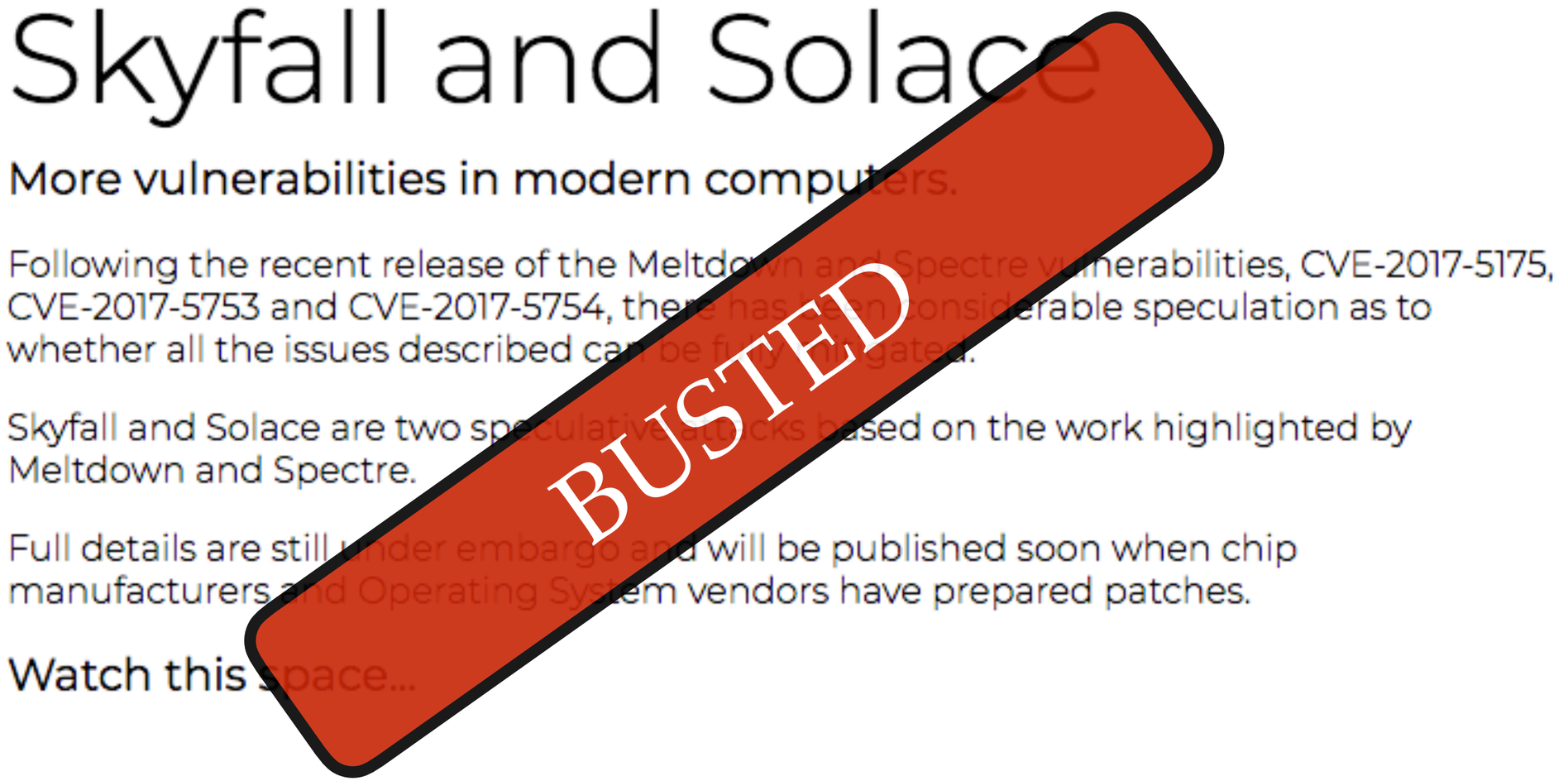
References

- Bug 1415291

CVE-2018-5094: Buffer overflow in WebAssembly with garbage collection on uninitialized memory

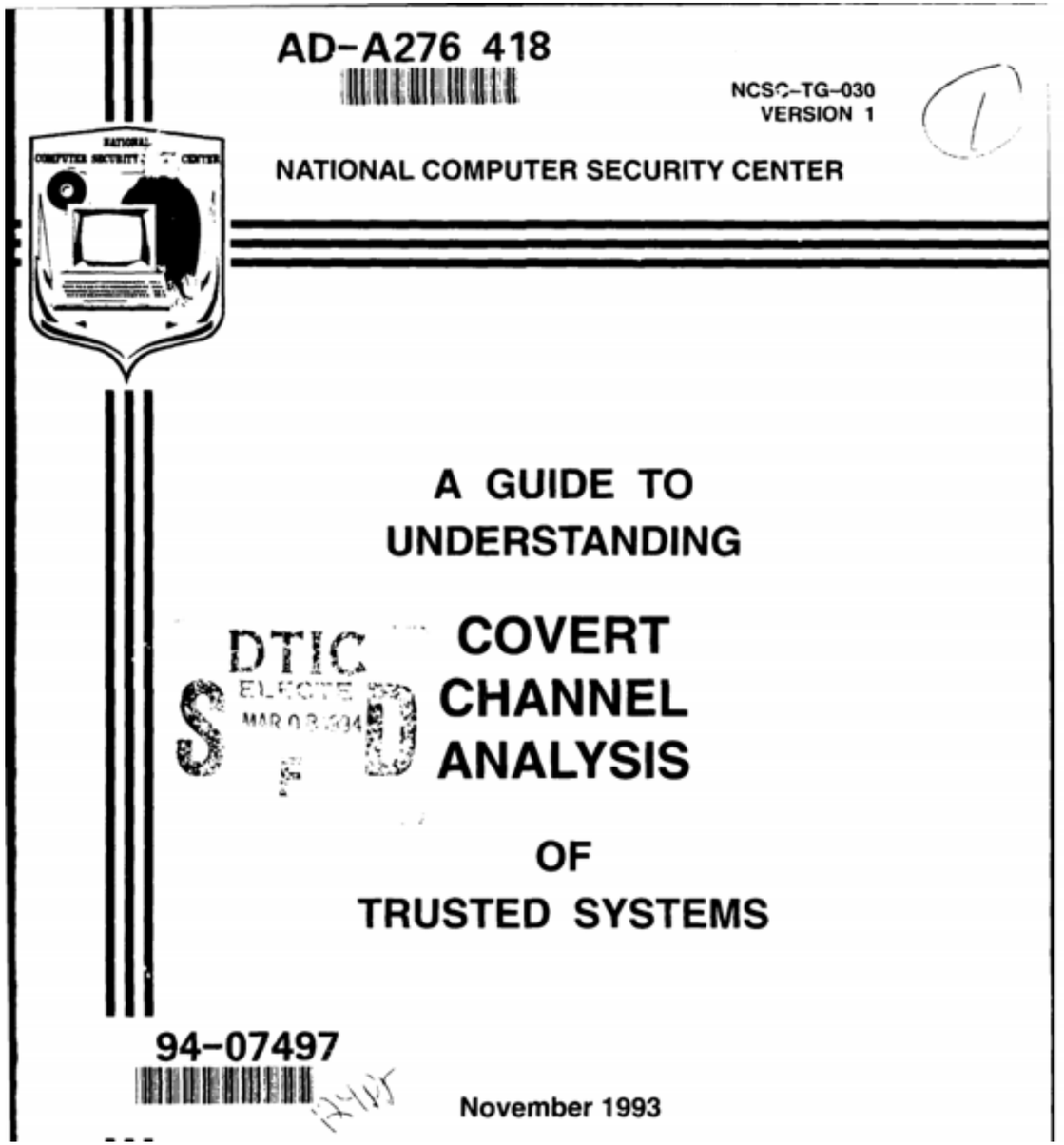
REPORTER	OSS-Fuzz
IMPACT	**HIGH**

And so it begins…



And so it begins…

A return to the past…




THE MELTDOWN AND SPECTRE EXPLOITS USE "SPECULATIVE EXECUTION?" WHAT'S THAT?
YOU KNOW THE TROLLEY PROBLEM? WELL, FOR A WHILE NOW, CPUs HAVE BASICALLY BEEN SENDING TROLLEYS DOWN BOTH PATHS, QUANTUM-STYLE, WHILE AWAITING YOUR CHOICE. THEN THE UNNEEDED "PHANTOM" TROLLEY DISAPPEARS.
THE PHANTOM TROLLEY ISN'T SUPPOSED TO TOUCH ANYONE. BUT IT TURNS OUT YOU CAN STILL USE IT TO DO STUFF.
AND IT CAN DRIVE THROUGH WALLS.
THAT SOUNDS BAD.
HONESTLY, I'VE BEEN ASSUMING WE WERE DOOMED EVER SINCE I LEARNED ABOUT ROWHAMMER.
WHAT'S THAT?
IF YOU TOGGLE A ROW OF MEMORY CELLS ON AND OFF REALLY FAST, YOU CAN USE ELECTRICAL INTERFERENCE TO FLIP NEARBY BITS AND—
DO WE JUST SUCK AT...COMPUTERS?
YUP. ESPECIALLY SHARED ONES.
SO YOU'RE SAYING THE CLOUD IS FULL OF PHANTOM TROLLEYS ARMED WITH HAMMERS.
...YES. THAT IS EXACTLY RIGHT.
OKAY. I'LL, UH... INSTALL UPDATES?
GOOD IDEA.

Thank you and good luck!