MELTDOWN & SPECTRE FOR NORMAL PEOPLE

MEMORY MODEL

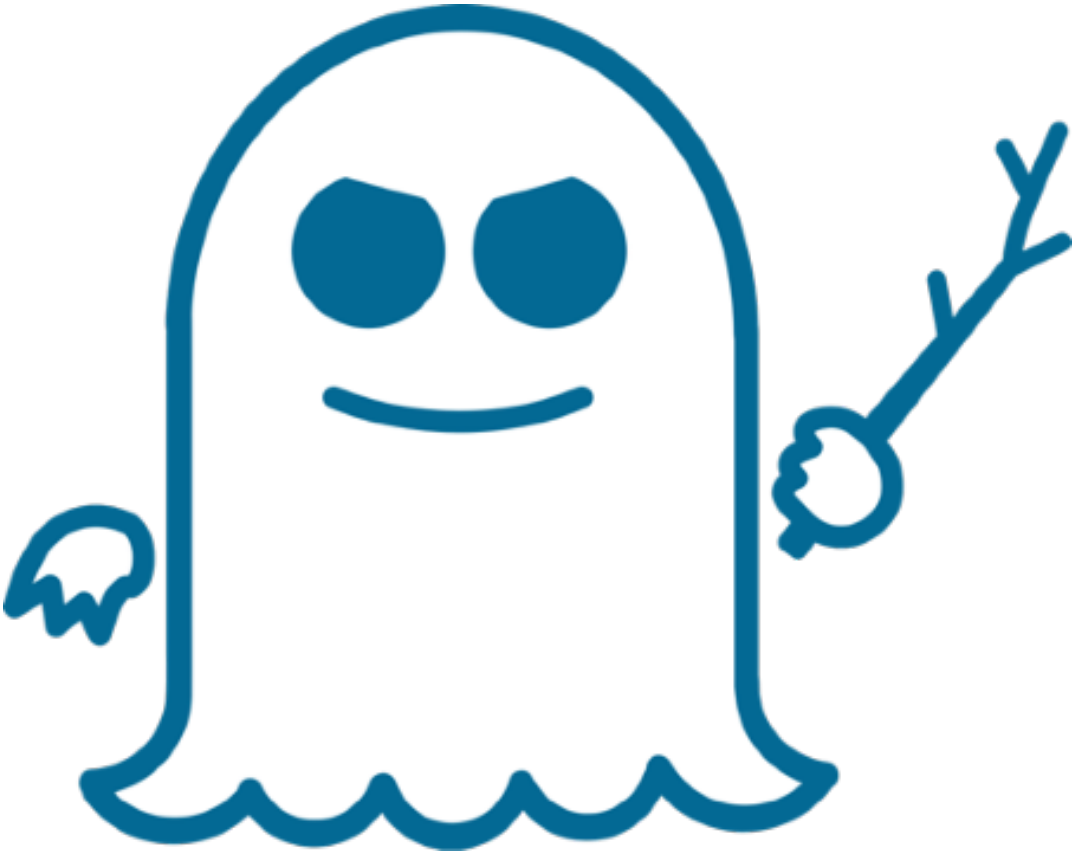

PROCESS
A

- Like a matryoshka doll the kernel *maps all physical* memory into its address space

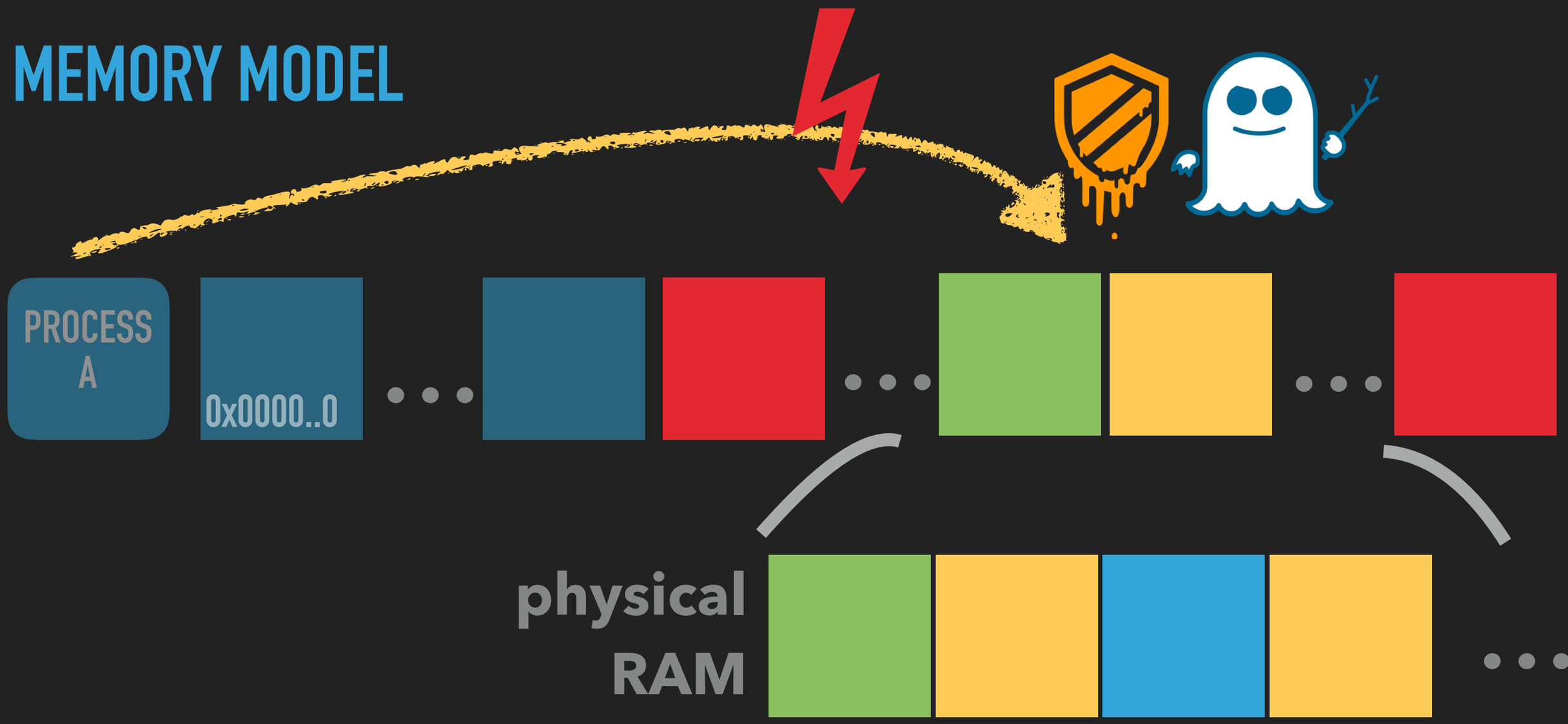
- Reading kernel memory allows reading of all (mapped) memory of all processes

physical

RAM



MEMORY MODEL



- Like a matryoshka doll the kernel *maps all physical* memory into its address space
- Reading kernel memory allows reading of all (mapped) memory of all processes

MEMORY MODEL

```
Virtual memory map with 4 level page tables:

0000000000000000 - 00007fffffffffff (=47 bits) user space, different per mm
hole caused by [47:63] sign extension
ffff800000000000 - ffff87ffffffffff (=43 bits) guard hole, reserved for hypervisor
ffff880000000000 - ffffc7ffffffffff (=64 TB) direct mapping of all phys. memory
ffffc80000000000 - ffffc8ffffffffff (=40 bits) hole
ffffc90000000000 - ffffe8ffffffffff (=45 bits) vmalloc/ioremap space
ffffe90000000000 - ffffe9ffffffffff (=40 bits) hole
ffffea0000000000 - ffffeaffffffffff (=40 bits) virtual memory map (1TB)
... unused hole ...
ffffec0000000000 - fffffbffffffffff (=44 bits) kasan shadow memory (16TB)
... unused hole ...
                 vaddr_end for KASLR
fffffe0000000000 - fffffe7fffffffff (=39 bits) cpu_entry_area mapping
fffffe8000000000 - fffffeffffffffff (=39 bits) LDT remap for PTI
ffffff0000000000 - ffffff7fffffffff (=39 bits) %esp fixup stacks
... unused hole ...
ffffffef00000000 - ffffffffffffffff (=64 GB) EFI region mapping space
... unused hole ...
ffffffff80000000 - ffffffff9fffffff (=512 MB)  kernel text mapping, from phys 0
ffffffffa0000000 - ffffffffefffffff (1520 MB) module mapping space
[fixmap start]   - fffffffff5fffff kernel-internal fixmap range
fffffffff600000 - fffffffff600fff (=4 kB) legacy vsyscall ABI
fffffffffe00000 - ffffffffffffffff (=2 MB) unused hole
```

https://www.kernel.org/doc/Documentation/x86/x86_64/mm.txt