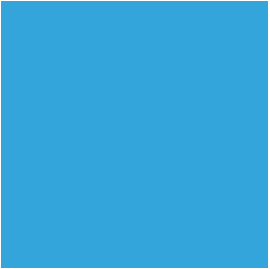




MEMORY MODEL

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

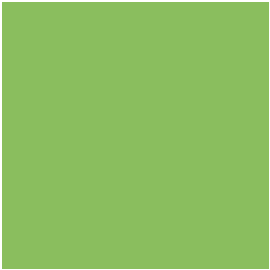




















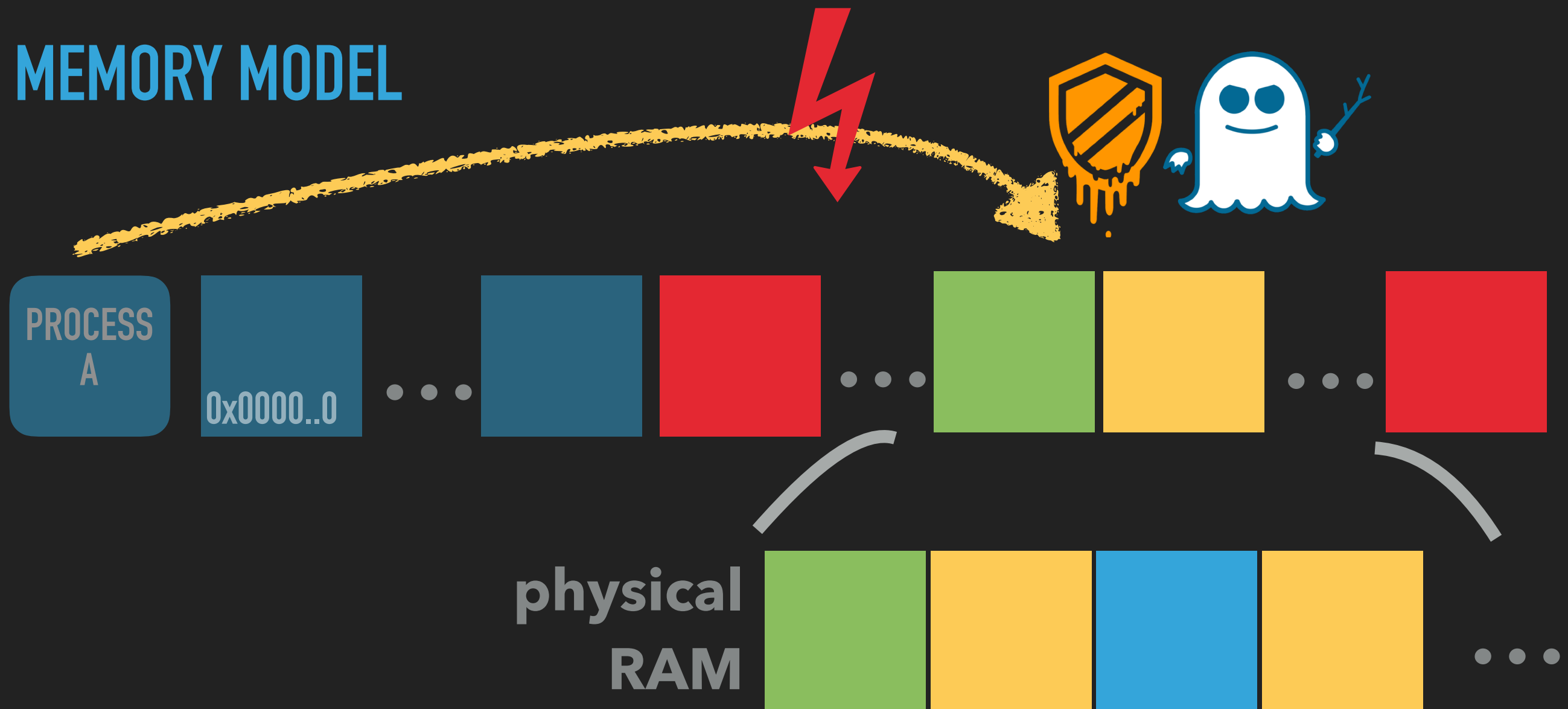


MEMORY MODEL

Virtual memory map with 4 level page tables:

```
000000000000000000 - 00007fffffffffffff (=47 bits) user space, different per mm
hole caused by [47:63] sign extension
ffff800000000000 - ffff87ffffffffffff (=43 bits) guard hole, reserved for hypervisor
ffff880000000000 - ffffc7ffffffffffff (=64 TB) direct mapping of all phys. memory
ffffc80000000000 - ffffc8ffffffffffff (=40 bits) hole
ffffc90000000000 - ffffe8ffffffffffff (=45 bits) vmalloc/ioremap space
ffffe90000000000 - ffffe9ffffffffffff (=40 bits) hole
ffffe9a000000000 - ffffea0000000000 (=40 bits) virtual memory map (1TB)
... unused hole ...
fffffec000000000 - fffffbffffffffffff (=44 bits) kasan shadow memory (16TB)
... unused hole ...
                vaddr_end for KASLR
ffffffe000000000 - ffffffe7ffffffffffff (=39 bits) cpu_entry_area mapping
ffffffe800000000 - ffffffefffffffffffff (=39 bits) LDT remap for PTI
fffffff000000000 - ffffffff7fffffffffffff (=39 bits) %esp fixup stacks
... unused hole ...
ffffffffff00000000 - ffffffffeffffffffffffff (=64 GB) EFI region mapping space
... unused hole ...
fffffffff800000000 - ffffffff9fffffffffffff (=512 MB) kernel text mapping, from phys 0
ffffffffffa0000000 - ffffffffeffffffffffffff (1520 MB) module mapping space
[fixmap start]    - ffffffff5fffffffffffff kernel-internal fixmap range
fffffffffff600000 - ffffffff600000ffff (=4 kB) legacy vsyscall ABI
fffffffffffe00000 - ffffffff0000000000 (=2 MB) unused hole
```

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