# AMD64 boot->kernel handoff

Konstantin Belousov `kib@FreeBSD.org`

June 10, 2021, `git date: 2021-06-10`

# What it affects

- locore
- create_pagetable
- EFIRT
- KEXEC
- KASLR

# How amd64 kernel starts

- kernel .text+.data are put at physical 2M (KERNLOAD)
- mode is set to Long (64bit %cs)
- 4-level page table maps low 1G 1:1, then same 1G is repeated till end of VA ($KERNLOAD \rightarrow KERNBASE$)
- jump to btext in locore
- locore asm sets up initial bootstack and calls hammer_time()
- hammer_time() -> pmap_bootstrap() -> create_pagetables()

# The problem

- System memory map can be incompatible with kernel put at KERNLOAD phys
- e.g. EFIRT might claim that memory
- KEXEC wants to put kernel at the place of existing kernel (copying trampoline)
- KASLR ...

# Changes required

- Kernel must be made relocatable
- ... but still use kernel memory model and mapped at upper 2G
- Something must relocate it (loader or kernel ?)
- Anyway this changes handoff interface
- Flag day