kexec, kdump, and crash

Presented by: Ben Buzbee

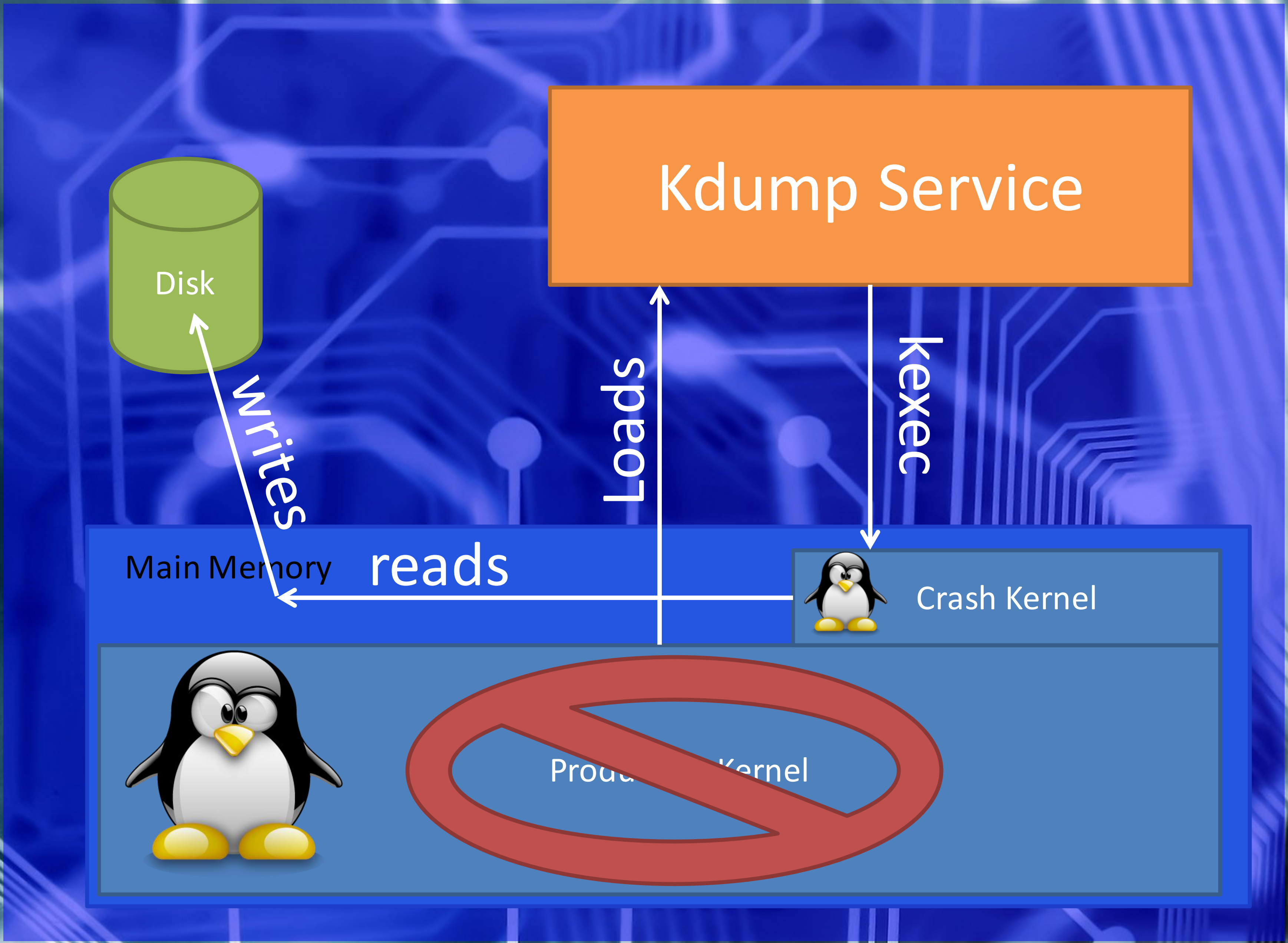
Pika-Tux

Overview

- Overview of System
- Kexec
- Kernel compilation parameters
- Kdump
- Analysis

Kdump Overview

- We compile two kernels of the same version
- We run the first kernel (production kernel) until it crashes
- When it crashes, the kdump service uses kexec to load our section kernel (crash kernel) which dumps the crash parameters of the first



Kdump Service

Disk

writes

Loads

kexec

Main Memory

reads

Crash Kernel

Production Kernel

Crash tool

- Crash analyzes kernel memory
  - Requires the context of vmlinux
- Can analyze a crashed kernel's memory dump
- Can analyze a running kernel's memory

Kexec

- Packaged with kdump
- Used to execute a Linux kernel directly
- Serves the function of a bootloader
- *apt-get install kdump-tools*
  - Installs all the tools we need

Kernel Compilation Parameters

- CONFIG_KEXEC=y
  - Allows kexec to run the kernel directly
- CONFIG_CRASH_DUMP=y
  - Enables crash dumps so that kdump can work
- CONFIG_SMP=n
  - Required if you have multiple processors, kdump only works with one. (Symmetric Multi-Processing)

Parameters Continued

- CONFIG_DEBUG_INFO=y
  - Builds with symbols
- CONFIG_PHYSICAL_START=0x1000000
  - Where the production kernel starts, must leave enough room for crash kernel before it

Crash Kernel

- Configure the same way as above, except must not use compression
- Since it’s uncompressed, will be vmlinux
- Append –kdump

Configure Kdump

- /etc/sysconfig/kdump
- KDUMP_RUNLEVEL=1
  - Runlevel for the crash kernel
- KDUMP_SAVEDIR=file:///var/log/dump
  - Where to save dump

Edit the Boot Loader

- Edit grub to reserve some memory for the crash kernel
  - crashkernel=XM@YM
    - X is the offset, Y is the size (In MB)
- This is probably where I made a mistake
  - New grub menu? I did something wrong? Can't tell.

Problems…

- So that didn’t work…
- Next approach: can I get crash to work on live memory?

Crash Utility

- Analyzes kernel memory
  - Primarily, to determine the cause of a crash
- Best use:
  - Analyze memory dumped after a crash (kdump)
- Resigned use:
  - Analyze running memory from /dev/mem

Curse you kexec…

- Tried to execute manually
- Now every time I reboot, it tries to do this and fails
  - Wrote a value somewhere that it doesn’t clean up?

Crash

- CONFIG_STRICT_DEVMEM=n
  - Otherwise we can't view kernel memory while its running
- Syntax: crash vmlinux System.map
  - Must be uncompressed (i.e. not vmlinuz)
  - Made me use the System.map even though the versions were the same – not sure why

Crash - Problem

- Read error: kernel virtual address: c124edb8 type: ‘cpu_possible_mask’
- Solution: Unknown
- Workaround: --minimal
  - – Not ideal: Only allows a small subset of the total command set

(Minimal) Commands

- Log
  - Dump message buffer
  - Usefulness: High on crashed kernels, low otherwise
- sym <symbol>
  - Translates symbol to virtual address
  - Usefulness: Low-Moderate (with rd)

(Minimal) Commands

- rd
  - Read memory
  - Usefulness: Moderate
- dis
  - Disassembles code at a given address
  - Usefulness: Low

(Minimal) Commands

- eval
  - Evaluates an expression
  - Usefulness: Low (I have a calculator)

Conclusion

- The setup is very involved and detailed
- I failed at it miserably
- The live analysis using crash is not particularly helpful
- The dump analysis using crash is moderately helpful
  - Maybe not worth the trouble of setup?