Live Patching the Kernel with kpatch

Seth Jennings
Senior Software Engineer, Kernel Generalist
sjenning@redhat.com
1/14/15

What is kpatch?

kpatch is a set of open source tools developed by Red Hat that allow for the generation of “patch modules” directly from a source-level patch and the application of those patch modules to a running kernel without the need to reboot or restart any processes.

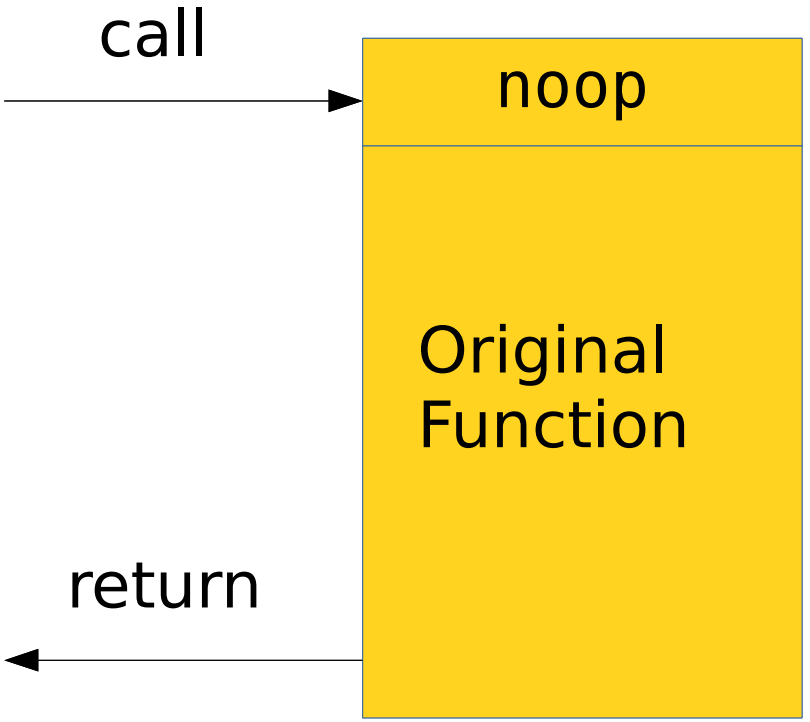
Use cases

- Primary
  - Urgent security fixes, CVEs
- Secondary
  - Urgent stability fixes, driver issues
  - Kernel development

Situations

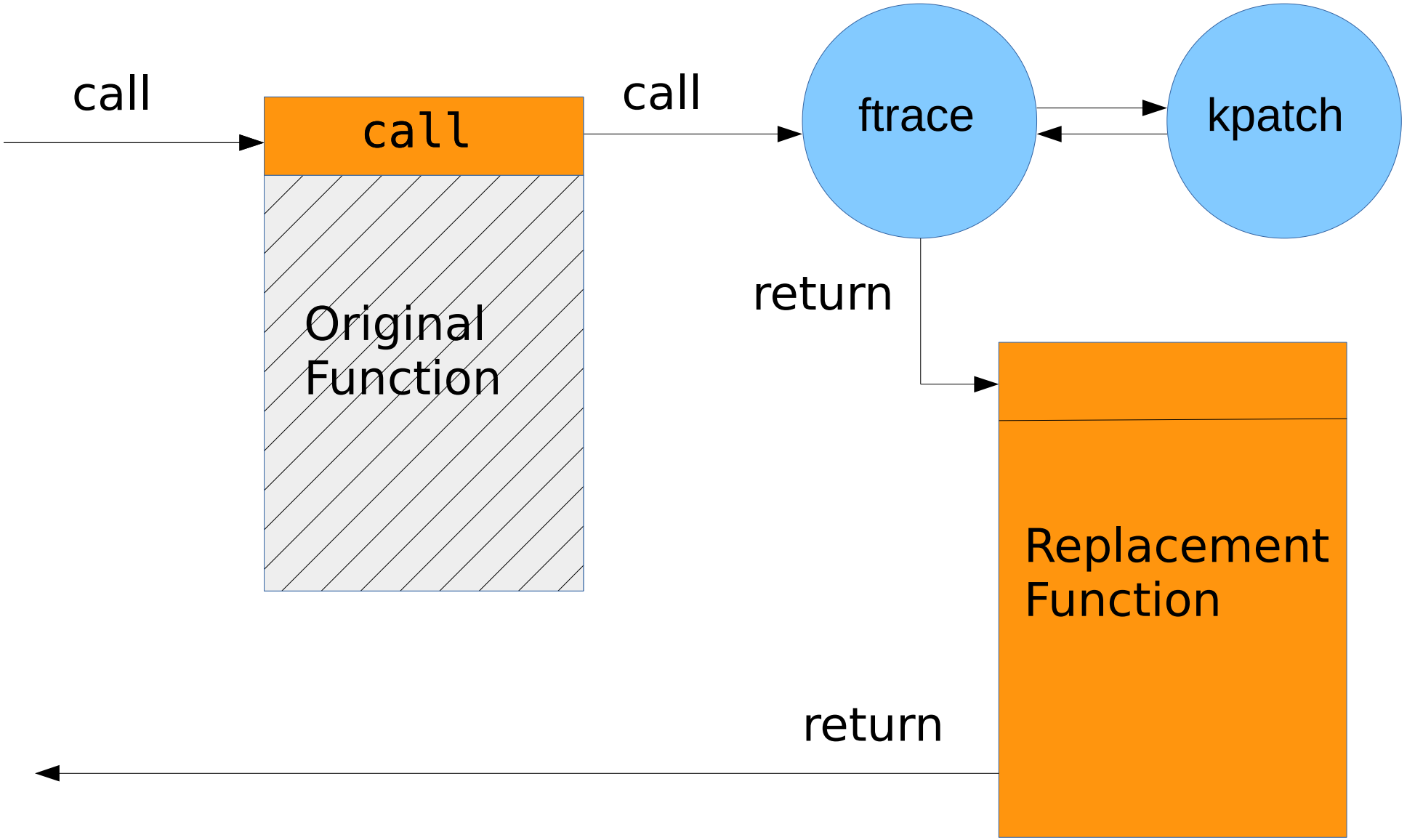
- Big non-virtualized machine with workload that can't be taken down easily
  - Scheduled downtime process, maintenance windows
  - Server remains vulnerable until the reboot can be performed
- Hypervisor or container host
  - Non-migratable tenant guests
  - Remove the machine from the compute scheduler and hope the existing guests shutdown soon

How it works (before)



thanks to Josh for the diagrams!

How it works (after)



Components

- Builder side, needed to build patch modules
  - kpatch-build command
  - Done internally by Red Hat
    - Human analysis, generation, testing, rpm build
- User side, needed to apply patch modules
  - kpatch command
  - kpatch modules

kpatch Packages

- kpatch-<version>.rpm
  - Contains the tools for applying hot patches to the system
- kpatch-patch-<version>.rpm
  - Contains the kpatch modules for all kpatch supported kernels
  - Includes a post install hook for applying the patch (kpatch load) and installing it into the initramfs (kpatch install)

kpatch command

- Manages the application of patch modules
  - kpatch install/uninstall <module>
    - Adds/removes patch modules from the system and initramfs
  - kpatch load/unload <module>
    - Loads/unloads patch modules from the running kernel
  - kpatch replace <module>
    - Atomically unload all existing patch modules and load the given patch module
  - kpatch info
  - kpatch list

Demo!

Customer Workflow

- Customer
  - yum install kpatch-patch
- Red Hat
  - CVE reported and fix found
  - Adapt upstream fix as a kpatch module
  - Add kpatch module to kpatch-patch rpm and bump package version

Customer Workflow (con't)

- Customer
  - yum update kpatch-patch
  - System is now protected
  - Install new kernel version that includes fix
  - During next maintenance window, reboot into fixed kernel version

Current State

- Under active development
- Completely open
  - https://github.com/dynup/kpatch
  - Issues and pull requests through Github
- Working with upstream kernel
  - Currently the kpatch core kernel module is more feature rich than the upstream driver named “livepatch”
  - Incrementally getting feature set accepted
  - First driver with basic functionality heading for 3.20

Resources

- Project members
  - Seth Jennings <sjenning@redhat.com>
  - Josh Poimboeuf <jpoimboe@redhat.com>
- Demo
  - https://www.youtube.com/watch?v=juyQ5TsJRTA
- Mailing list
  - http://www.redhat.com/mailman/listinfo/kpatch
- Github (very useful REAMDE)
  - https://github.com/dynup/kpatch
- RHEL Blog
  - http://rhelblog.redhat.com/2014/02/26/kpatch/

Questions?