Linux kernel live patching

OWASP Security Tapas 2015-10-20

Mikael Falkvidd (@mfalkvidd)
Why live patches?

- Apply fixes for severe security problems quickly and without planning downtime - SUSE’s goal is CVSS 6 and above
- Stability fixes

- large in-memory databases - saving and re-reading data from disk can take hours
- virtualization hosts - patch hosts without affecting guests
- computing clusters - some calculations are hard to stop and resume
- large datacenters - rebooting thousands or tens of thousands of machines in a controlled way without affecting business can be hard
kpatch

- From Red Hat, released publically summer of 2014
- 10-40 milliseconds freeze
- All-or-nothing
- No performance impact after patching
kGraft

- From SUSE, released publically in November 2014
- No freeze
- Divides processes into different universes (with/without patch)
- Some performance impact after patching
Demo 1 - patch an exploit without rebooting
Demo 2 - create our own patch

--- orig/fs/proc/meminfo.c 2015-09-28 22:27:23.720627176 +0200
@@ -89,6 +89,7 @@
 * Tagged format, for easy grepping and expansion.
 */
    seq_printf(m,
+    "kpatch fungerar!\n"
    "MemTotal:  %8lu kB\n"
    "MemFree:   %8lu kB\n"
    "MemAvailable: %8lu kB\n"
Presentation available at this URL