DOUG GOLDSTEIN
STAR LAB

OPENXT SUMMIT
06/07/2016

SECURING XEN TODAY AND BEYOND

PRESENTER

DOUG GOLDSTEIN

- Star Lab
- Open Source Projects
  - Xen Maintainer
  - QEMU Contributor
  - libvirt committer
  - Gentoo Linux Developer

TODAY

XEN 4.7 RELEASE

- modularity with Kconfig
    - reduce the surface area by not building a feature in
    - run-time switches still remain when feature is built in
    - configurable components
        - tmem
        - kexec
        - live patch (xsplice)
        - profiling

XEN 4.7 RELEASE

- XSM
  - don’t default to permissive
  - default policy improvements
- Live Patch (xSplice)
  - ability to deploy hypervisor patches without bringing the system down
  - double edged sword however

XEN 4.8+

- more modularity
  - remove half a dozen compression algorithms and initramfs parsing
  - remove PV, HVM, and PVH modes
  - require hardware assist and remove the emulated fallback
- verification of Live Patch (xSplice)
- divide control domain permissions

XEN 4.8+ (CONT)

- XSM
    - enable it by default
    - improve default policy
        - modular policy
        - provide domD policies
- testing, testing, testing.

QEMU USAGE

- lockdown syscalls with seccomp
- remove out hardware that’s unnecessary
- improve toolstack invocation to limit the scope of its execution
- linux-based stubdom

DOM0 CHANGES

- disaggregated components by default
- restartable dom0
  - static environments could get rid of it
- handle missing services without a DoS
  - xenconsoled
  - xenstore
- constrain dom0 resources by default

BEYOND

TBOOT

- improve hand off and verification
  - EFI environments
- persistent verification of environment

QUESTIONS?