State of SELinux

Paul Moore

August 2016

Containers

- SELinux support added to rkt and runC
    - Joins existing Docker support
        - Newer Docker versions leverage runC support
- SELinux/overlayfs support
        - Critical as a container filesystem
- Separate capability checks for init and non-init userns
    - Grant capabilities only in non-init userns (not host)
    - Enables Chrome and other sandboxed applications
- Improvements to the type bounding implementation
    - Enables type hierarchy with NNP

Filesystems

- File label invalidation/revalidation
  - Distributed filesystems can update labels on clients
  - GFS hooks/support included in Linux v4.5
- Userspace access to validatetrans policy constraints
  - Necessary for filesystems outside the VFS layer
- Proper SELinux/overlayfs support
  - In testing stage for Linux v4.9 (selinux#next branch)

Labeled Networking

- Added support for CALIPSO / RFC 5570
  - Will be part of Linux v4.8 (currently in Linus’ tree)
  - Standards based labeled networking for IPv6
  - Interoperability verified against Solaris TX

Everything Else in the Kernel

- New access controls for loading kernel modules
    - Access control using domain and module file labels
    - Similar capabilities to LoadPin LSM
- Expanded execstack controls to thread stacks

SELinux Userspace Tools

- New SELinux userspace v2.5 release
  - Proper support for fine grained ioctl() access controls
    - Whitelisting individual ioctls
  - Improved CIL support
    - Generate CIL via policy.conf
  - Improved documentation

SEAndroid Progress

- SEAndroid installed base growing significantly
  - KitKat (v4.4) started running SELinux in enforcing
    - One year ago 60% of Android devices ran KitKat+
    - Currently 80% of Android devices run KitKat+
  - Lollipop (v5.0) adds policy enforcement for everything
    - One year ago 18% of Android devices ran Lollipop+
    - Currently 50% of Android devices run Lollipop+
- Functional improvements
  - Decomposed mediaserver based on least privilege
  - Increased restrictions on ioctls

All the Other Things

- Brillo
  - Google IoT OS with SELinux enabled and enforcing
- OpenEmbedded
  - Updated SELinux userspace
- OpenXT
  - Hardened virtualization client
  - Uses Xen Security Modules / Flask and SELinux

SELinux Resources

- Kernel
  - git://git.infradead.org/users/pcmoore/selinux
- Userspace / Tests
  - https://github.com/SELinuxProject
- Reference Policy
  - https://github.com/TresysTechnology/refpolicy
- Mailing List
  - https://www.nsa.gov/what-we-do/research/selinux/mailing-list.shtml
- Me
  - paul@paul-moore.com