The State of SELinux

Paul Moore
Red Hat
August 2015

2015 – The Year of CIL

- Common Intermediate Language provides multiple benefits
  - Policy operations can be 50% ~ 75% faster than before
  - Policy module store provides prioritized modules
  - Enables the creation of higher level policy languages
- CIL shipped in SELinux Userspace release 2015-02-02 (v2.4)
  - Fedora will include CIL in Fedora 23 (est October 2015)

Performance Gains Everywhere

- CIL provides numerous speed gains
  - F23 systemd loads the policy in half the time at boot
  - F23 setsebool takes less than a second
- Improvements in userspace (neverallow checking in libsepol)
  - Memory usage reduced by ~65%
  - Time reduced by ~85%
- Improvements in the kernel (avtab hash table optimizations)
  - The avtab longest chain length dropped ~97% (Fedora policy)

Shiny New Features

- Access control for individual ioctls (Jeff Vander Stoep's talk)
- Add genfscon labeling for sysfs, debugfs, and pstore
  - Allows initial labeling via policy as well as runtime modification
- Updated netlink classes and mappings
  - Improved fine grain access control for netlink messages
- Upstreamed the Binder LSM/SELinux hooks from Android
  - SELinux access controls for Android's IPC mechanism
- Bounded domain transitions for NO_NEW_PRIVS and NOSUID
  - Permit domain transitions inside “sandboxes”
- Additional tests added to the selinux-testsuite project

SELinux and Android

- >60% of active Android devices run SELinux
- Starting with Android 5.0 (Lollipop) everything from system daemons to third party applications are confined by SELinux policy.
- Ongoing work to synchronize Android with SELinux upstream

SELinux to the Rescue

- Shellshock (Bash)
    - Applications contained with SELinux (Apache) were not vulnerable to privilege escalation
- Venom (QEMU)
    - Libvirt's SELinux/sVirt VM isolation prevents compromised VMs from attacking the host or other guests
- Firefox ?
    - Due to the complexities of Firefox, it is not contained by default (Fedora policy)

More Information on SELinux

- SELinux GitHub
  - https://github.com/SELinuxProject
- SELinux Developers Mailing List
  - http://www.nsa.gov/research/selinux/list.shtml
- SELinux Reference Policy Mailing List
  - http://oss.tresys.com/mailman/listinfo/refpolicy
- SEAndroid
  - http://seandroid.bitbucket.org