The State of SELinux

Paul Moore, Red Hat

August 2014

SELinux Core Update

- Policy wizards can now detect constraint violations
  - audit2why / audit2allow provide better answers
- Policy boolean changes no longer trigger a relink
  - setsebool is much quicker
- Auditing built in to libsemanage
  - No longer reliant on applications for auditing
- Permissive mode flag in AVC audit records
- Started porting SELinux userspace to Python 3

SELinux Tools / Policy Update

- SELinux tools
  - Resizable sandbox windows (“sandbox -X”)
  - SELinux policy GUI (“sepolicy”)
- System tools
  - Labeled networking support in systemd
    - Work in progress, based on xinetd
- SELinux policy
  - Lots of good progress on CIL
  - Upstream merge expected “soonish”

SELinux / Containers / Packaging Update

- Integration with various container technologies
  - libvirt-lxc (“virt-sandbox”)
  - Docker
- RPM-OSTree / Fedora Atomic support
  - Delivers atomic system image updates with rollbacks
  - Initially developed for container based services

SEAndroid Update

- Shipping in Enforcing mode by default
  - Samsung 4.3 devices (Galaxy S4)
  - Google Android 4.4
  - Mandated by the Android CDD/CTS
- Android L preview confines 49 out of 61 domains
  - All third party applications
  - Almost all services

SELinux Links

- SELinux GitHub (Userspace tools / libraries)
  - 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