State of SELinux

Paul Moore
paul@paul-moore.com

October 2018

What is SELinux?

Flexible Mandatory Access Control

- Flexible policy language
  - Support for multiple policies
  - Granular access controls
  - Label based policy
- Administrator controls the policy
  - Admin controls security rights, not the object owners
- Policy is enforced by the Linux Kernel
  - Userspace required to load and manage policy, not enforcement

SELinux System Components

- Boot / init / systemd
  - Load SELinux policy
  - Mount filesystems
    - File/mount labeling
- Runtime / kernel
  - Manage SELinux labels
    - Filesystem objects
    - Running processes
  - Enforce security policy
- Management
  - Updates (kernel, policy, etc.)
  - Policy customization

SELinux Access Decisions

Subject	Access	Object
Apache	Read	File
httpd_t	file:{ open read }	httpd_sys_content_t

SELinux Advantages

- Restrict high risk services
  - Preemptive exploit mitigation
- Secure virtualization and containers
  - Enforced separation
  - Controlled sharing
  - QEMU/KVM, Kubernetes, etc.
- Wide platform support
  - Traditional Linux systems
  - Android / embedded
- Common Criteria certified MLS capabilities

SELinux in 2018

SELinux Anniversaries

- SELinux is almost 18 years old
  - First released on December 22, 2000
- Mainline Linux for 15 years
  - Linux v2.6.0-test3 released on August 9, 2003
- Enterprise Linux for 13 years
  - RHEL-4.0 released on February 15, 2005
- Android for 5 years
  - Android 4.3 released on July 24, 2013
  - Enabled on ~96% of devices (as of July 23, 2018)

SELinux Kernel Changes

- New access controls for eBPF
- Added proper SCTP access controls
- SO_PEERSEC on socketpair(2) sockets
- Moved mailing lists to vger.kernel.org
  - selinux@vger.kernel.org

SELinux Kernel Contributors

Sep 2017 to Aug 2018

- Top 10 contributors by lines changed
  - Stephen Smalley 1,947 (62.7%)
  - Richard Haines 438 (14.1%)
  - Peter Enderborg 182 (5.9%)
  - Chenbo Feng 166 (5.3%)
  - Eric W. Biederman 71 (2.3%)
  - Jann Horn 45 (1.5%)
  - Alexey Kodanev 32 (1.0%)
  - Paul Moore 27 (0.9%)
  - Richard Guy Briggs 27 (0.9%)
  - Greg Kroah-Hartman 26 (0.8%)

SELinux Userspace Changes

- Toolchain support for SCTP and InfiniBand
- List homedir labels with “semanage”
- Manage multiple modules with “semodule”
- Python 3 support for “selinux-gui”
- Moved mailing lists to vger.kernel.org
  - selinux@vger.kernel.org

SELinux Userspace Contributors

Sep 2017 to Aug 2018

- Top 10 contributors by lines changed
  - Nicolas Iooss 5,413 (61.3%)
  - Petr Lautrbach 805 (9.1%)
  - Jan Zarsky 707 (8.0%)
  - Stephen Smalley 569 (6.4%)
  - Marcus Folkesson 438 (5.0%)
  - James Carter 332 (3.8%)
  - Vit Mojzis 310 (3.5%)
  - Richard Haines 107 (1.2%)
  - Jason Zaman 45 (0.5%)
  - Yuli Khodorkovskiy 25 (0.3%)

SELinux Reference Policy Changes

- Migrated to GitHub's "SELinuxProject"
  - All SELinux development in one place
  - Merged the "contrib" submodule into the main tree
- Moved mailing lists to vger.kernel.org
  - selinux-refpolicy@vger.kernel.org

SELinux Policy Contributors

Sep 2017 to Aug 2018

- Top 10 contributors by lines changed
  - Chris PeBenito 117,494 (96.6%)
  - Sven Vermeulen 1,591 (1.3%)
  - Dave Sugar 808 (0.7%)
  - Richard Haines 440 (0.4%)
  - Jason Zaman 393 (0.3%)
  - Guido Trentalancia 189 (0.2%)
  - Christian Göttsche 159 (0.1%)
  - Luis Ressel 134 (0.1%)
  - Nicolas Iooss 123 (0.1%)
  - James Carter 56 (0.0%)

Get Involved

- Kernel (mirror) / Userspace / Reference Policy / Tests
  - https://github.com/SELinuxProject
- Kernel (official)
  - git://git.kernel.org/pub/scm/linux/kernel/git/pcmoore/selinux.git
- Mailing Lists
  - Main SELinux list: http://vger.kernel.org/vger-lists.html#selinux
    - Archive: https://lore.kernel.org/selinux
  - SELinux Reference Policy list: http://vger.kernel.org/vger-lists.html#selinux-refpolicy
    - Archive: https://lore.kernel.org/selinux-refpolicy
- Me
  - Twitter: @securepaul
  - Mail: paul@paul-moore.com