State of AppArmor

2016 Linux Security Summit

Presentation by
John Johansen
john.johansen@canonical.com
www.canonical.com

August 2016

Last Year

“Ideally nothing until ...
Finish cleanup and upstream out tree kernel patches”

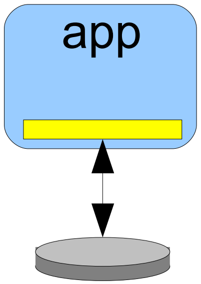
Misc

- Documentation (apparently users want this)
- User space utils cleanup
- Coarse parallel policy compiles
- started slowly moving userspace to git
- prototyping "change_profile/setcon" for all threads in a process - launcher
- Improve user space perm checking/caching
- Userspace 2.10, 2.11-betas

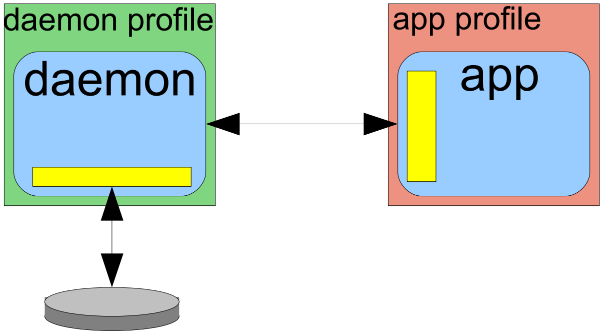
- And Lots of bug fixing, and revision of ...

gsettings/dconf mediation

- gsetting/dconf
  - mmaps files and access directly

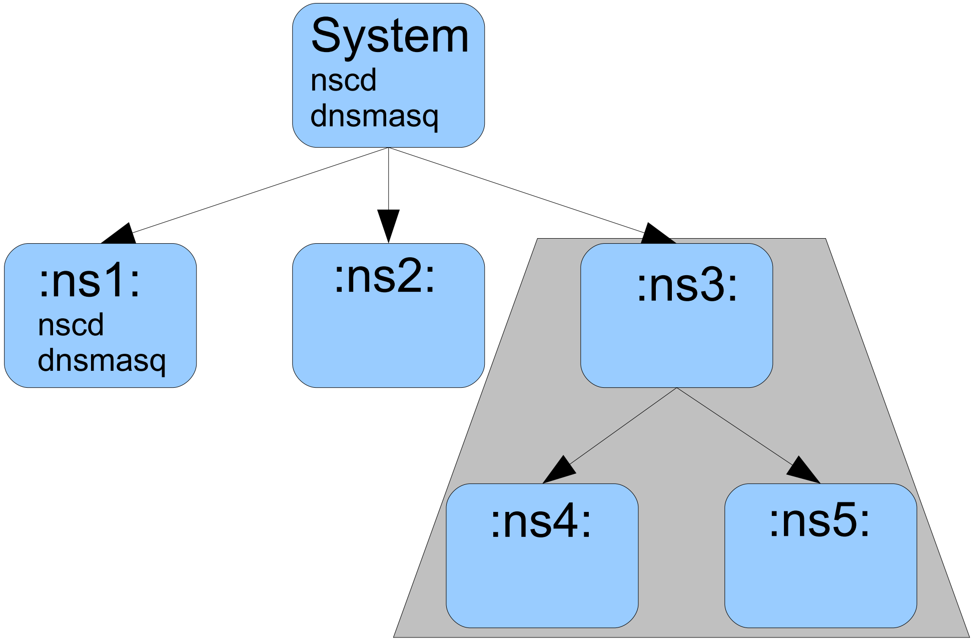


- Mediate access via priv-sep
  - Policy denies access to files
  - Policy extended to support gsettings
  - Trusted daemon does the file access
    - Daemon checks with policy
  - lib transparently talks to daemon
    - caches settings of interest
    - caches perms for speed
    - staticly linked, against old lib, apps denied access
    - sets up watchpoints to be notified of settings changes



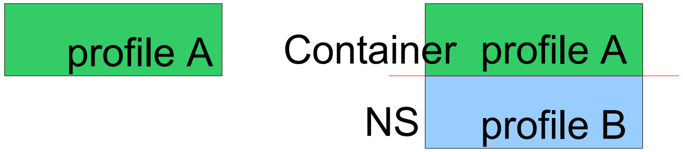
Policy namespaces

- Yet another namespace!
- Hierarchical
- Own set of policy
- Control what/where policy can be loaded
- Controls what policy can be viewed
  - Virtualized most interfaces
    - Except policy dir
- uses
  - Logically grouping policy
  - User defined policy
  - Containers



Stacking

- Iteration on implementation
- Bug fixing



profile A

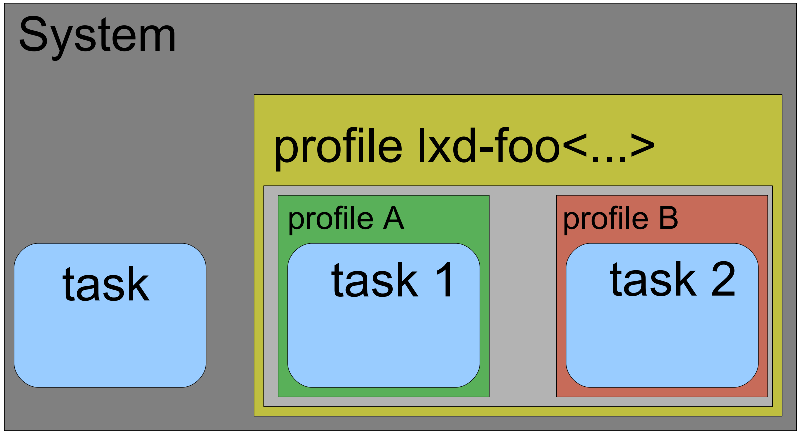
Container profile A

NS profile B

- Task can be confined by more than 1 profile
- Deepest NS in stack is current namespace
- Child can't see parent NS (theoretically)
- Tasks within a namespace can only see manipulate the “current” namespace
- Stack across Namespaces
- Enforce a system hardening on a container
- Container can then enforce its own policy
- permission checks are only between labels in same namespace

Integrating with containers (lxd/lxc)

- Poking at namespaces
  - Lukasz Pawelczyk smack namespaces
  - Ideally we would want a few more hooks
    - unshare, pivot_root
    - But … not until base code is upstream



- Container does manual setup
  - policy namespace
  - stack
- AppArmor enforces/requires
  - 1-to-1 restriction on policy ns to user ns
  - user ns need cap mac admin to load policy

Backlog

- Upstreaming

Backlog continued

- Fix-up improve namespace/stacking
  - Virtualize policy dir
  - Better integration/control of namespacing
  - Check point/restore support for policy
- Better systemd integration
- Ioctl white listing
- Overlayfs support
- Fine grain network mediation
- Delegation
- Performance improvements
- Learning mode improvements
- Bring-up mode improvements
- Tool improvements

Questions please

Thank you

John Johansen

john.johansen@canonical.com

www.canonical.com