File Access Policy Daemon - Fapolicyd

Radovan Sroka | Senior Software Engineer | Red Hat Inc.

What Is An Application Whitelisting?

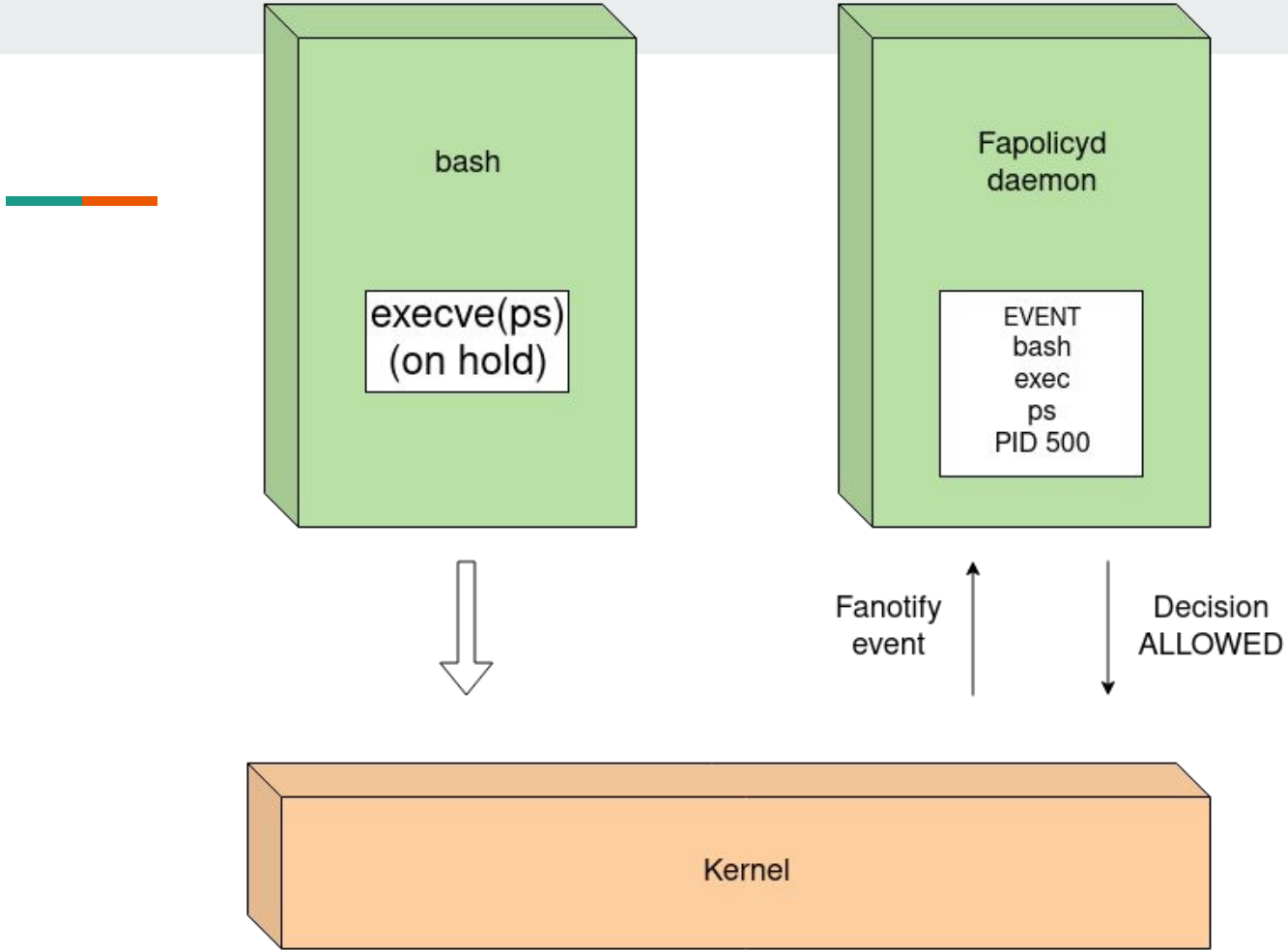
- Security practise
- Ability to specify and run only trusted applications
- Admin defines what is allowed and what is not

Fapolicyd Framework

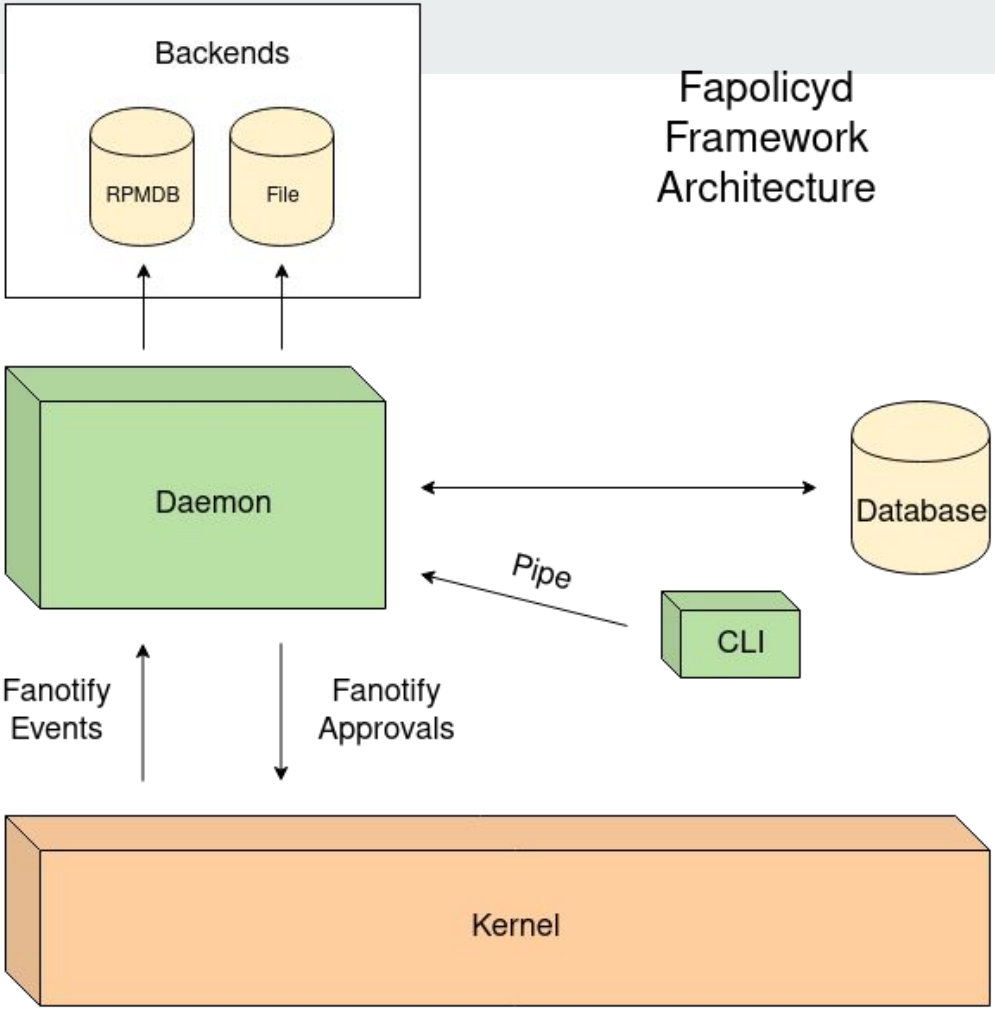
- Linux daemon and CLI utilities
- Lightweight solution
- RPM/DNF integration
- Audit support
- Relies on fanotify API

Fanotify API

- Kernel API
- Similar to inotify
- Stands for “File” “Access”
- Receive events from open/exec system calls
- Blockable on system call side, waiting for response


bash
execve(ps)
(on hold)
Fapolicyd
daemon
EVENT
bash
exec
ps
PID 500
Fanotify
event
Decision
ALLOWED
Kernel

Fapolicyd Framework Architecture



Fapolicyd Trust Philosophy

- Trusted
  - /usr/bin/ls
  - /usr/bin/mkdir
  - /usr/bin/sudo
- Not Trusted
  - /home/user/xyz.sh
  - /tmp/random_exploit.bin

Fapolicyd Trust Philosophy

- Trusted (installed from rpm)
  - /usr/bin/ls
  - /usr/bin/mkdir
  - /usr/bin/sudo
- Not Trusted (not installed from rpm)
  - /home/user/xyz.sh
  - /tmp/random_exploit.bin

Fapolicyd Trust Philosophy

- Trust files
  - Another source of trust
  - Stored in trust.d directory
- Others files can be enabled by adding to a trust file
  - Can be done via CLI
    - fapolicyd-cli -f add /home/user/user_script.sh

Rules

- Stored in rules.d directory
- Evaluated from top to bottom
- First match wins and apply decision
- Examples
  - deny_audit perm=open exe=/usr/bin/wget : dir=/tmp
  - allow perm=open exe=/usr/bin/python3.7 : ftype=text/x-python trust=1
  - deny_audit perm=any pattern ld_so : all
  - deny perm=any all : all

Patterns

- normal
- static
- ld_so
- ld_preload

Patterns (Security Concerns)

- normal
- static
- ld_so
  - Direct execution from dynamic linker
- ld_preload
  - Using of LD_PRELOAD during execution

Audit | Syslog Log Denials

```
rule:9 dec=deny audit  perm=execute  auid=1000 pid=600  exe=/usr/bin/zsh
: file=/home/rsroka/bin/my-bin  ftype=application/x-executable
```

Deployment of Fapolicyd Framework

```
[root@Axis ~] dnf install fapolicyd
```

```
[root@Axis ~] systemctl enable --now fapolicyd
```

Thank You!

- rsroka@redhat.com
- https://github.com/linux-application-whitelisting/fapolicyd