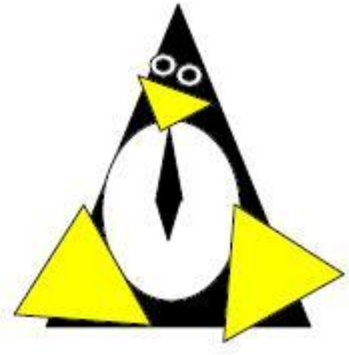
Linux Security Modules Architecture Roundtable

Kees Cook - Casey Schaufler

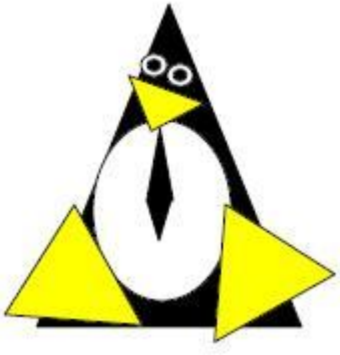
Linux Security Summit

September 2011



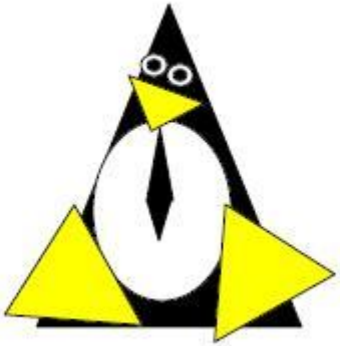
Today’s Discussion

- Multiple concurrent LSMs
- Which LSM is active
- Sharing /proc/*pid*/attr
- Conventions for /sys/kernel/security
- What should –Z show



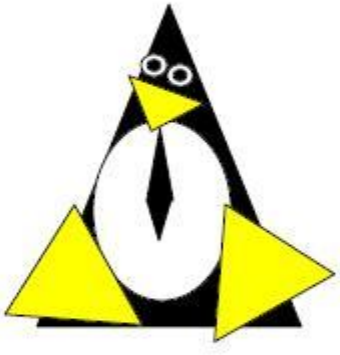
Multiple Concurrent LSMs

- David Howell’s February Patch Set
- Casey Schaufler’s Promised Patch Set
  - Once it works for all 4 LSM’s at once



Modular LSMs

- Free resources of inactive security modules
- Requested for distributions

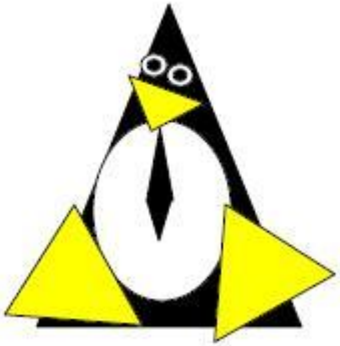


Which LSM is Active

- Currently ad hoc
- /sys/kernel/security/lsm
  - Name of the active LSM

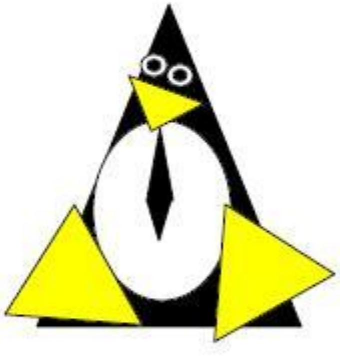
Sharing /proc/<pid>/attr

- Conflict exists over **`current`** today
  - smack-current
  - apparmor-current
  - selinux-current
- Deprecate current over time?



Conventions for /sys/kernel/security

- A single LSM independent library?
- Is that even rational?



User Space Tools

- Generic use of “ls –Z”
- What beyond core utilities?