Security Subsystem Report: Yama

Linux Security Summit 2012
Kees Cook
(pronounced "Case")
keescook@chromium.org

http://outflux.net/slides/2012/lss/lsm/

Overview

- Past
- Present
- Future

Past ("ruler of the departed")

- May 2010: rejected for not being an LSM
    - symlink restrictions
- Jun 2010: LSM sent to LKML
    - hardlink restrictions, ptrace attach restrictions
- Jul 2010: grew process relationship API
- Aug 2010: reverted for being an LSM
- Oct 2010: released in Ubuntu 10.10
- Nov 2011: clarified what an LSM can be
- Dec 2011: released in Chrome OS
- Feb 2012: LSM half merged upstream for 3.4
- Apr 2012: more ptrace restriction levels

Present

- link restrictions in VFS for 3.6
  - at least 16 years old (Aug 1996)
  - had to switch to year-based serial numbering
- bug fixes
  - PTRACE_TRACEME
  - lockdep
  - 32-bit compat prctl

Future

- module restrictions
  - load from fd
  - tie loading to specific file system
- stacking
  - hard-coded in Chrome OS and Ubuntu

Questions?

keescook@chromium.org

http://outflux.net/slides/2012/lss/lsm/