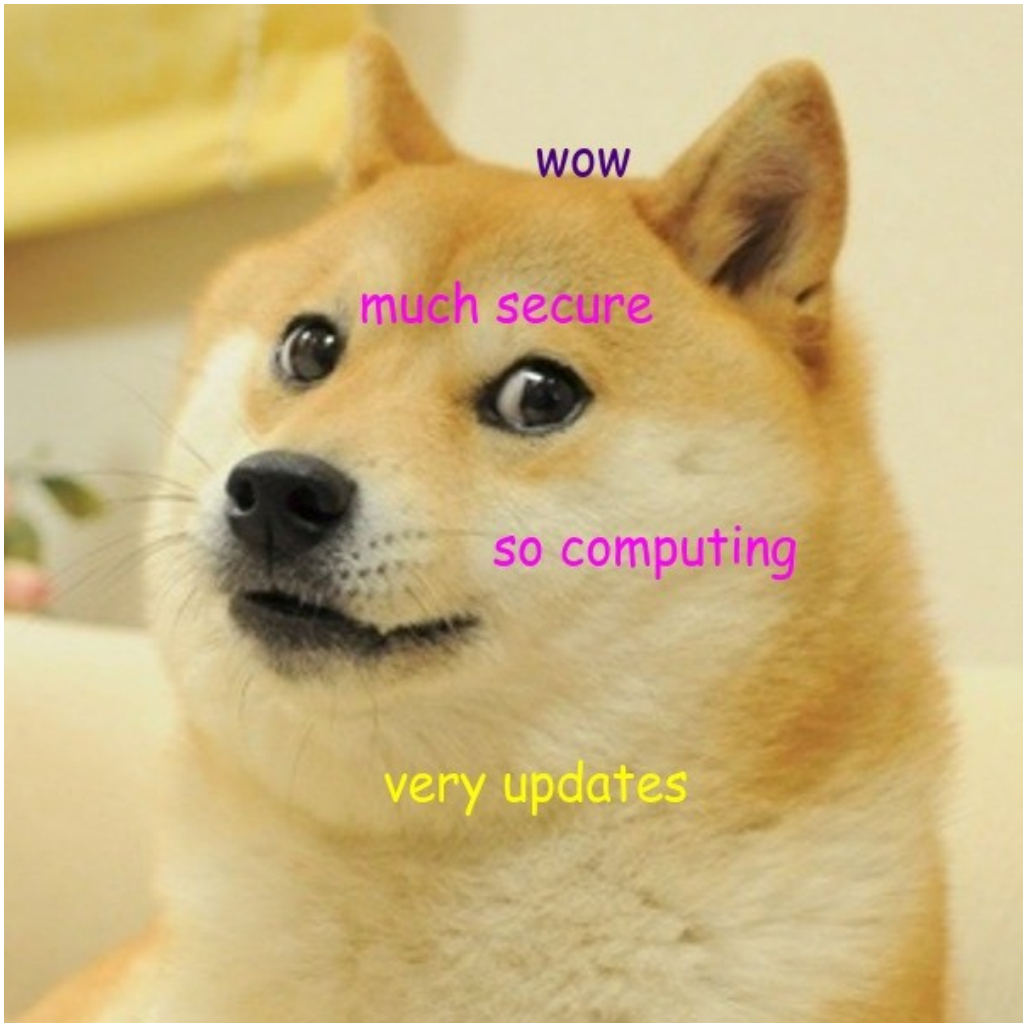
seccomp update



http://outflux.net/slides/2014/lss/seccomp.pdf

Linux Security Summit, Chicago 2014

Kees Cook <keescook@chromium.org>
(pronounced “Case”)

chrome

Overview

- Architectures
- Thread synchronization
- Syscall
- Regression testing
- Maintainership

Architectures

- x86: 3.5 (21 Jul, 2012)
- s390: 3.6 (Sep 30, 2012)
- arm: 3.8 (18 Feb, 2013)
  - redirection bug fix in 3.16 (3 Aug, 2014)
- mips: 3.15 (8 Jun, 2014)
- arm64: it's happening! (3.18 maybe?)

Thread synchronization

- seccomp filters applied on a per-thread basis
- some libraries start threads during their init
- proper solution had to deal with loads of crazy thread group locking
- generous reviews by many people especially Andy Lutomirski and Oleg Nesterov
- oh, and only via a syscall ...

Syscall (or “please CC linux-api”)

```
$ man writev | wc -l
124
$ man prctl | wc -l
374
$ man prctl | sed -n \
    '/PR_SET_SECCOMP/,/PR_SET/p' | wc -l
33
$ wc -l Documentation/prctl/seccomp.txt
225
$ man ../man-pages/man2/seccomp.2 | wc -l
245
```

Regression testing

- Will Drewry wrote original test suite, continues to be extended for fun corner cases (now with 46 tests!)
  - anyone know how to change syscall via ptrace on s390?
- https://github.com/redpig/seccomp
- https://github.com/kees/seccomp/tree/trace
- Morbid^WExciting test names featuring:
  - Verbs! poke drop trap kill fail
  - Nouns! chain child sibling

Maintainership

Questions?

http://outflux.net/slides/2014/lss/seccomp.pdf

keescook@chromium.org

keescook@google.com

kees@outflux.net