BPF LSM: Security Domains

LSF/MM/**BPF**

KP Singh

WARNING!

Heavy prototyping ahead..

“bpf” security domain

Only executables in the domain can load bpf progs

Simple prototype use case:

“Just allow bpftrace to load BPF programs”

Implementation:

```
xattr -l /usr/bin/bpftrace
security.domain: bpf
```

New helper:

```
bpf_getxattr
```

Light skeleton...

bprm_committed_creds

- Get the xattr from the executable
- Store security domain information in task blob

`task_alloc`

Transfer security domain information to child tasks

`bpf_prog`

Deny bpf syscalls for non-bpf domain tasks

`inode_setxattr`

Deny any attempt to set xattrs
(can be a new security domain)

lskel = loader config (more flexibility)

Small bug in LSM lskel for bpftool

Thank you!