Security & Hardening

Steven Barth

New infrastructure in Chaos Calmer

Package Signing

SHA-256 package lists
now signed with EdDSA

Filesystem Jails

restrict process fs-access
r+w whitelist in init-script

Seccomp

restrict syscalls
call whitelist files

```
start_service() {
        procd_open_instance
        procd_set_param command "$PROG"
        procd_set_param seccomp /etc/seccomp/mdns.json
        procd_set_param respawn
        [ "$(uci get mdns.@mdns[-1].jail)" = 1 ] && procd_add_jail mdns ubus log
        procd_close_instance
}
```

```
{
        "whitelist": [
                "read",
                "write",
                "open",
                "close",
                "time",
                "brk",
                "ioctl",
```

WiP in Designated Driver

Buildsystem Hardening

format-security checking
user-space stack-smashing protection
kernel-space stack-smashing protection
global source-fortification
RELRO / bind now: protect ELF sections + GOT

Reproducible Builds

thanks to reproducible.debian.net
toolchain and packaging changes
byte-by-byte reproducible images and packages

In other Designated Driver news

- musl replaces uclibc
  - active releases
  - cleaner & more robust
- telnet be gone
- experiments with new security announcements

ToDo

- Finish global ASLR support: Position Independent Executables
- More jailfs-files
- More seccomp-files
- More privilege dropping

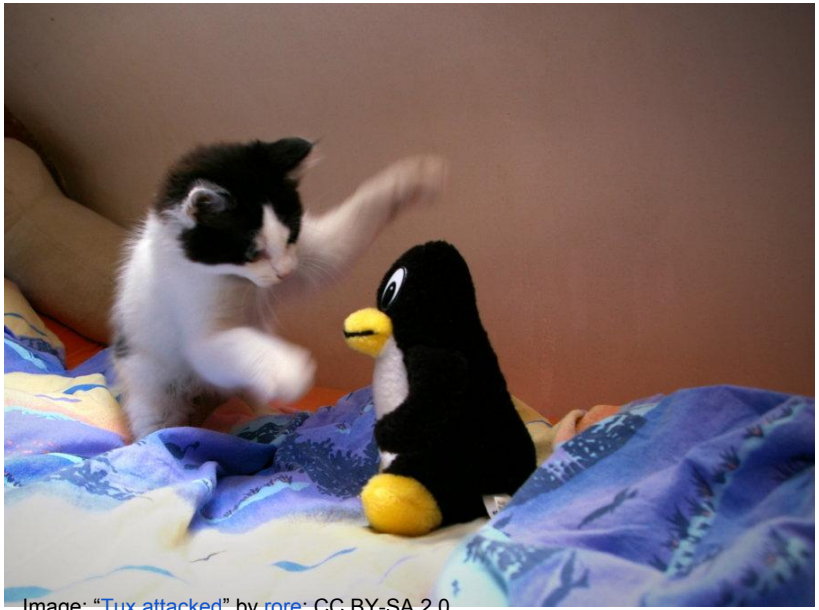

Image: “Tux attacked” by rore; CC BY-SA 2.0

Thank you for your attention! Questions?

Steven Barth
<cyrus@openwrt.org>