Linux-WPAN Updates

Linux Plumber Conference, IoT MC
Richmond, 2023-11-15

Stefan Schmidt <stefan@datenfreihafen.org>
Alexander Aring <alex.aring@gmail.com>

Agenda

- Linux kernel updates
- Admin updates
- Userspace updates
- Link-Layer security status and problems

Linux wpan

- Low-power, low-rate wireless
- IEEE 802.15.4 subsystem in the kernel
- SoftMAC, netlink userspace interface, drivers
- 6lopwan adaption layer to IPv6

Linux Updates 1/3

Linux 6.0 (2022-10-02) 8 patches

- Bug fixes in driver and uninitialized value in dgram_sendmsg
- 6lowpan simplification from rb tree to array lookup for nhcid

Linux 6.1 (2022-12-11) 13 patches

- Bug fixes in drivers and missing init for list in mac802154
- Fixing LQI recording (zeroed out due late init)

Linux 6.2 (2023-02-19) 40 patches

- Introduction of coordinator interfaces
- Initial work on scanning with new netlink scan group

Linux Updates 2/3

Linux 6.3 (2023-04-23) 26 patches

- Added beaconing support to announce PAN’s
- Passive scanning support
- Driver conversion from platform_data to gpiod API

Linux 6.4 (2023-06-25) 12 patches

- Driver fixes and tree wide cleanups

Linux 6.5 (2023-08-27) 14 patches

- Active scan support
- Answering BEACON_REQ
- MLME handling for limited devices

Linux Updates 3/3

Linux 6.6 (2023-10-29) 4 patches

- Driver fixes

Linux 6.7

- Nothing scheduled, bug fixes from stable as usual

Linux 6.8 queued

- Internal PAN management
- Associations and disassociation between devices
- Netlink API to get association list

Admin Updates

- Finally a three person maintainer team since February 2023
- Round robin for stable and -next tree handling

Userspace Updates

- Beacon sending
- Scanning
- Associations (pending)
- Switch wpan-tools to use SPDX headers
- REUSE tool for compliance
- GitHub action CI pipeline for wpan-tools (gcc, clang, ubuntu 16.04 to latest matrix)

Link-Layer Security

- Who I am?
- Alexander Aring (Hobbyist in WPAN/6LoWPAN)
- Some works in upstream Linux
  - 802.15.4 (some drivers, nl802154, etc.)
  - 6LoWPAN (RPL, ndisc ops, fragmentation, etc.)
  - Lot of other stuff...
  - Check my talks at netdevconf!

Link-Layer Security

- History
- Introduced by Phoebe Buckheister
- SoftMAC implementation
- Changes by me to switch to nl802154
  - Close to IEEE 802.15.4 spec
  - Still experimental for various reason
  - iwpan (iw, dump/script is really terrible)

Link-Layer Security

DON’T USE IT!

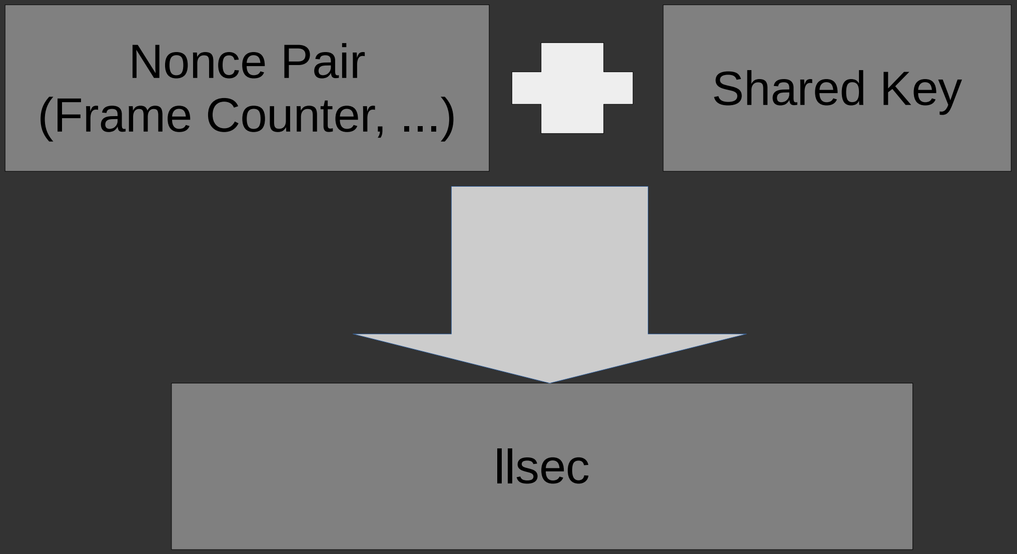
UNTIL YOU KNOW WHAT YOU ARE DOING!

- Certain parts of IEEE spec is Out of scope
- Speaking about Mesh Topology
- I’ve seen people using it…

Link-Layer Security

- Problem… the **Frame Counter**
- It’s part of Nonce Pair (Simplified)
- Number used **Once (with Shared Key)**
- Frame Counter part of Security MIB
- Each Node maintains Frame Counter

Link-Layer Security



Nonce Pair
(Frame Counter, ...)

Shared Key

llsec

Link-Layer Security

1. Problem

What if Frame Counter overflows?

Nonce Pair is not number used once anymore!

Replay attacks possible!

Link-Layer Security

1. Solution

Deploy a new shared Key

?Out of scope of IEEE 802.15.4?

Current behaviour Linux will just ignore overflows

Link-Layer Security

2. Problem

llsec Access Control List

ACL stores Frame Counter of each neighbor Node (and more stuff...)

Bootstrapping issue!

Link-Layer Security

Bootstrapping

Don’t init ACL Frame Counters with zero, only if the other Node Frame Counter is zero

But they are probably not because we likely join an operated network...

Higher Frame Counter as being in ACL is being trusted

Replay Attack issue!

Link-Layer Security

Bootstrapping

Out of Scope of 802.15.4 (Mesh Topology*)

Frame Counter is a Security Parameter

Current behaviour Frame Counter set by User

Link-Layer Security

- Bootstrapping Protocol...
- Commercial Solutions using proprietary protocols e.g. MLE not developed at IETF anymore :-((... but somewhere else)
- Commercial Solutions using Open Standards but proprietary DHCP like bootstrapping – Makes no Sense!
- Bootstrapping Frame Counter (and more async Connection -RPL, etc.) See my netdevconf talk!
  https://datatracker.ietf.org/doc/html/draft-kelsey-intarea-mesh-link-establishment-06
- Key Exchange with MLE (for new Keys, Frame Counter overflow!)

  https://datatracker.ietf.org/doc/html/draft-kelsey-intarea-mesh-link-establishment-06

Link-Layer Security

My message to everyone!

Don’t USE llsec without solving those issues!

And I think solving it is complicated… to make it compatible with other implementations…

But BLE Mesh solves it in their spec on link layer! Just IEEE doesn’t do that…