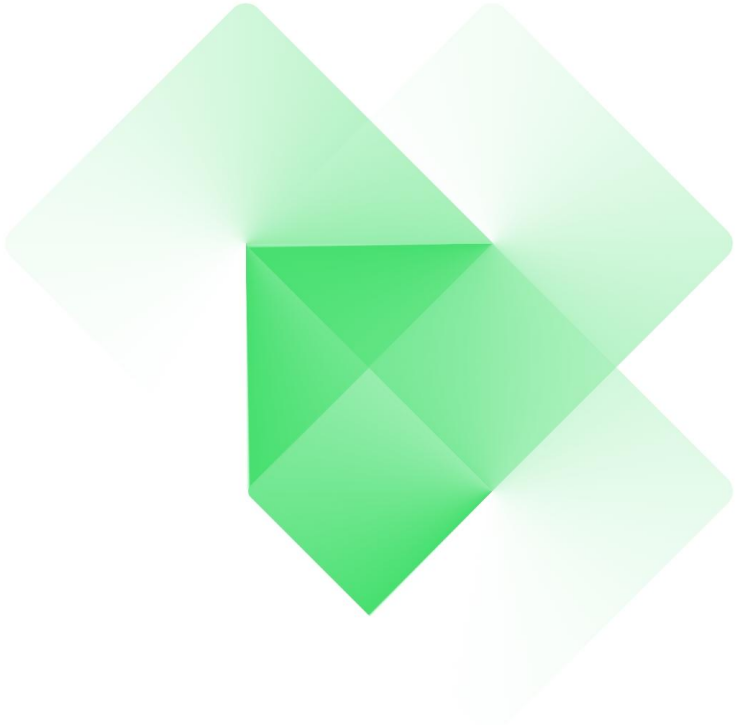
Pendulum Project



Who am I?

David Venhoek

- Technical lead for statime and ntpd-rs
- Background in physics and mathematics
- Active participant in the IETF ntp working group

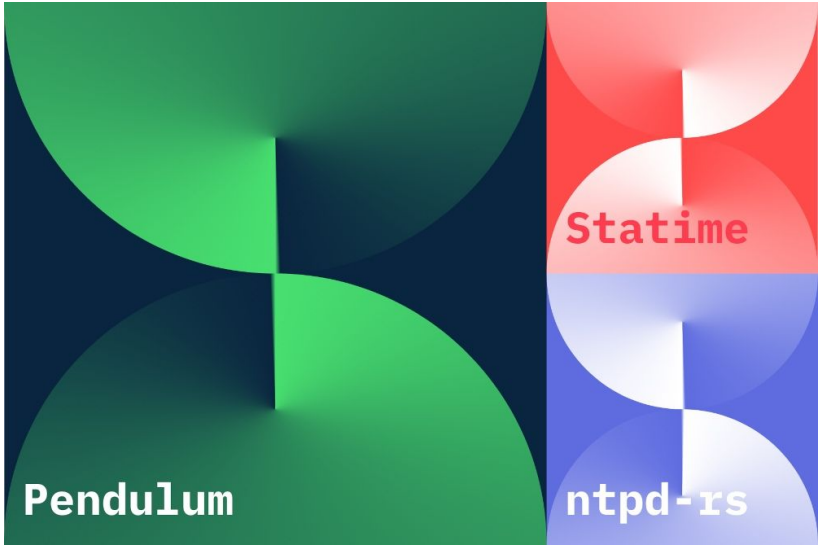
Outline

- Introduction to the Pendulum Project
- Deep dive into the project goals
- Dive into some implementation details
- Future directions

The Pendulum Project

Two software products

- ntpd-rs
  - Implementation of NTPv4
  - Including support for NTS
- statime
  - Library implementing IEEE1588-2019
  - A binary for PTP on Linux



The Pendulum Project

History:

- ntpd-rs
  - Started as project funded by ISRG
  - Initial aim: Memory safe implementation of NTP
- statime
  - Started as knowledge building exercise
  - Initial aim: 1588 implementation suitable for embedded devices

The Pendulum Project

Currently funded by Sovereign Tech Fund (German federal government)

- ntpd-rs
  - Get to a production-ready state (finished)
  - Work on future versions of NTP (primarily NTPv5)
- statime
  - Expand into a competitor for ptp4linux
  - Current quality target: Alpha/Beta

Project goal

Security oriented implementations of NTP and PTP.

Project goal

Security oriented implementations of NTP and PTP.

- Memory safety
- Ease of configuration
- Safe defaults
- Limiting scope

Project goal

Memory safety

- Use of rust
  - Core code is unsafe-free
  - Rely on battle-tested dependencies (Tokio, MIO) for async runtime
  - Minimal use of unsafe in network and clock abstraction libraries.

Project goal

Ease of configuration

- Declarative configuration (toml file)
  - Indicate desired functional state, not how to get there
  - Inhibit accidental overriding of earlier settings
- Clear separation into sections
  - Keeps related configuration together.
  - Ease of reading/reviewing the configuration.

Project goal

Safe defaults

- Absent in configuration should mean no security impact.
- Examples (NTP):
  - No acting as a server unless asked
  - No implicit sources of time
  - No observability unless explicitly configured

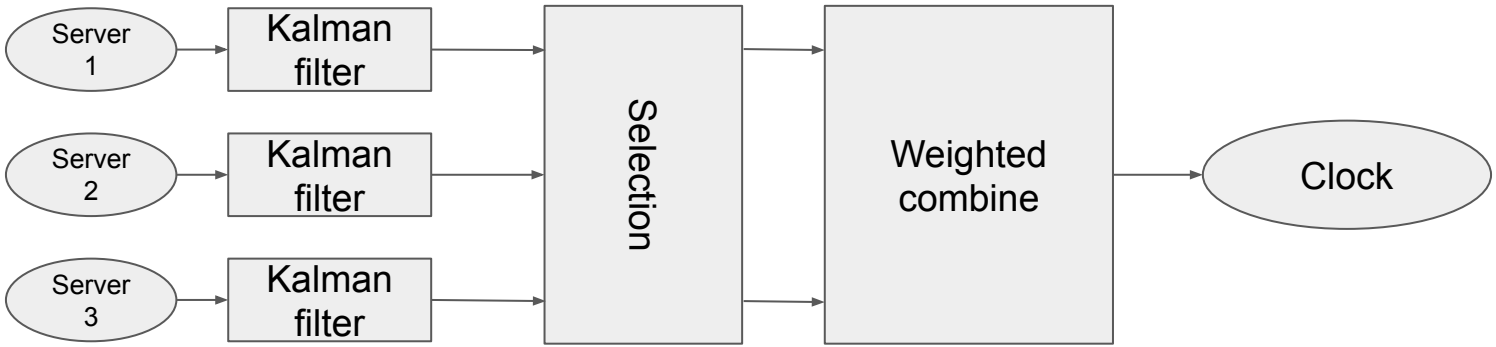
Project goal

Limiting scope

- NTP
  - No broadcast mode
  - No symmetric mode
  - No MD5 MAC

Implementation details: Clock steering

Kalman filter based approach



Implementation details: Clock steering

Kalman filter noise estimates

- Measurement noise:
  - Estimation through variation of round trip delay
- Process noise
  - Assumption: frequency random walk
  - Estimate clock stability through likelihood

Implementation details: PTP Master only

- IEEE1588-2019:
  - When a port is master only, all received announce message must be ignored
  - Result: BMCA always recommends master mode for the port
- Our implementation
  - When a port is master only, the slave state is prohibited
  - Why: Provides more flexibility

Implementation details: PTP Master only

Why?

- Gives no interop problems
- Original functionality can be attained with help of acceptable master list
  - Enable master mode
  - Empty acceptable master list
- But we can also support a “firewall” type use
  - Port can provide time to downstream network, but never accept time.
  - Can support redundant setups by allowing bmca to still select the master.

Future directions

NTPv5

- Full revision of the loop detection mechanism
  - Detect all potential loops, including when using multiple time sources in a server
- Support multiple timescales
  - TAI
  - UTC
- Removal of several potential information leak paths

Future directions

We would like to

- Get statime to a production-ready state
- Support local reference clocks
  - GPSd support
  - Pulse per second support
- Contribute to future protocol development
  - Getting NTPv5 standardised
  - Leap smearing time scales

Call to action

- Try out ntpd-rs and/or statime!
- Report bugs/issues
- Read NTP working group drafts
  - Feedback is needed, also from end users
  - In particular, consider reading draft-ietf-ntp-ntpv5-requirements
- Feel free to contact us if you need
  - Specific features
  - Need/want a support contract

Interesting URIs

- ntpd-rs: https://github.com/pendulum-project/ntpd-rs
- statime: https://github.com/pendulum-project/statime
- NTPv5 requirements: https://datatracker.ietf.org/doc/draft-ietf-ntp-ntpv5-requirements/
- NTPv5 draft: https://datatracker.ietf.org/doc/draft-ietf-ntp-ntpv5/

Thanks

Getting in touch

Contact someone or checkout Tweede golf on https://tweedegolf.nl or LinkedIn

David Venhoek

Tech lead ntpd-rs and statime
david@tweedegolf.nl