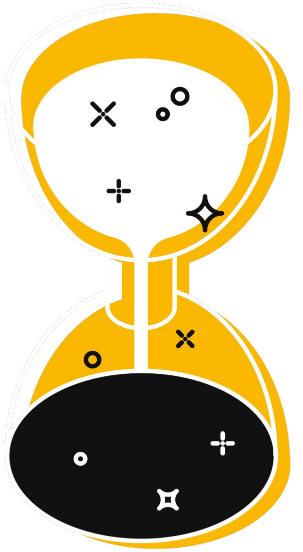
Roughtime: Securing time for IoT devices

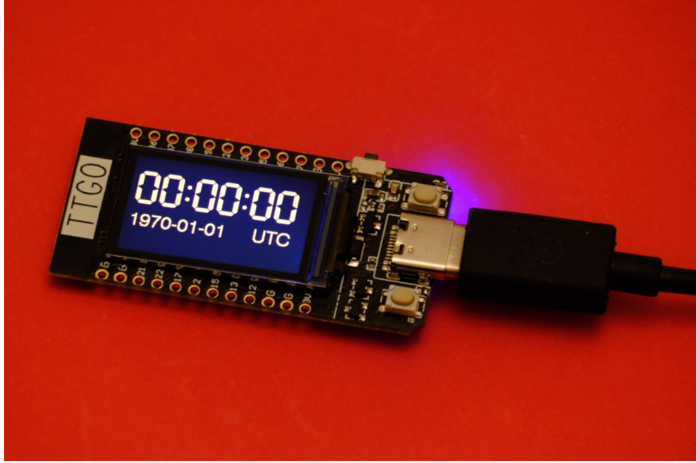
Christer Weinigel, Netnod

Accurate time is important

- Many security critical protocols need accurate time
  - DNSSEC and TLS
- The application itself might need time

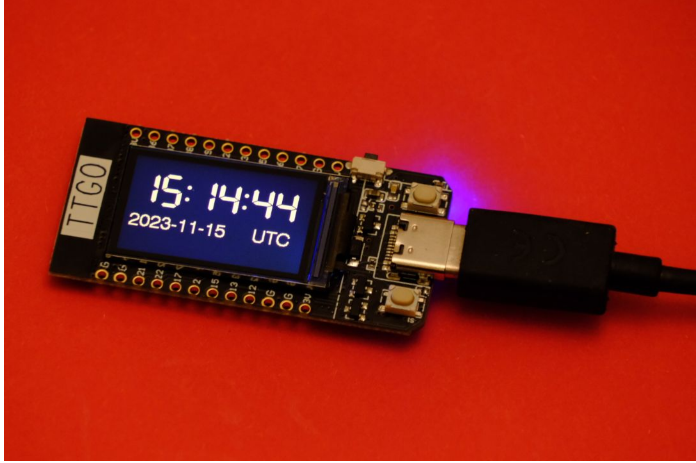


Keeping time



- All devices can keep time
  - When powered on
- But not when powered off
  - IoT devices may not have a Real Time Clock (RTC)
  - Raspberry Pi - has RTC hardware, but no battery backup by default
  - "Shipping mode"
    - Even with a battery the clock will not run before first power on because the battery is not connected

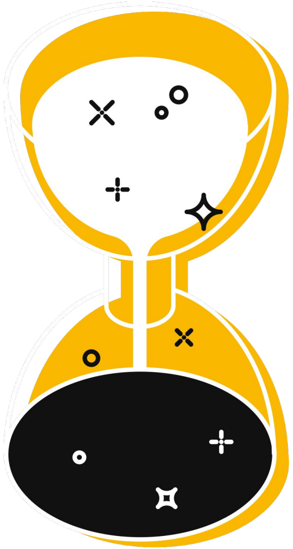
Getting time over the network



- NTP (Network Time Protocol)
  - Lacks security
- NTS (Network Time Security)
  - Adds security
  - Bootstrapping problem
    - NTS depends on TLS
    - Which depend on having accurate time
  - Heavyweight, not suited for resource constrained devices

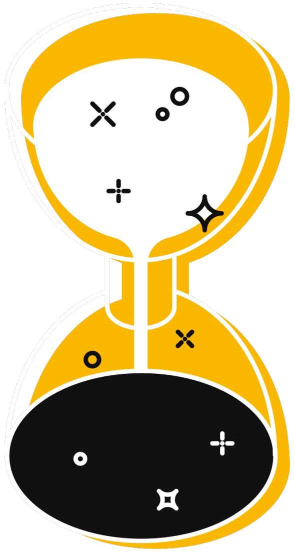
Possible solution: Roughtime

- Protocol is an IETF Draft
- Started out as a way to solve the bootstrapping problem
  - Secure
  - Was not intended to replace NTP
    - Only 10 second accuracy
  - Fairly low CPU usage and small memory footprint



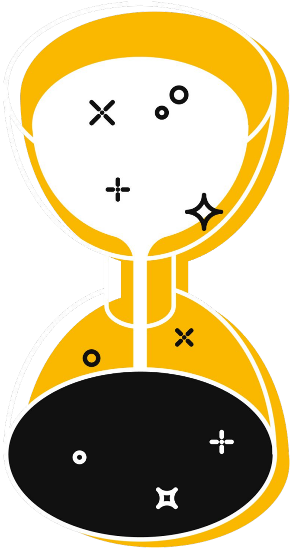
Roughtime: evolution

- It is now a decent generic time protocol
  - With better accuracy than 10 seconds
    - Microsecond resolution
  - Which is secure
  - Which can run on resource constrained client
  - Which still solves the bootstrapping problem



Next steps

- Roughtime development has stalled
  - RIPE community funded project to revive it!
- Going forward
  - Kickstart work on protocol
  - Collect requirements
    - What do we need to secure time on IoT devices?
    - Getting community involvement and feedback.
  - Update draft based on requirements
    - Add missing features, maybe drop unnecessary features
  - Update implementations
    - Hackathon
  - Submit Roughtime to IETF RFC Editors



Resources

- Roughtime Draft
  - https://datatracker.ietf.org/doc/html/draft-ietf-ntp-roughtime
- Working client implementation of draft version 4, 5 and 7
  - https://vadarklockan.readthedocs.io
- Roughtime servers
  - Netnod: sth1.roughtime.netnod.se, sth2.roughtime.netnod.se (v7)
  - Marcus Dansarie: roughtime.se (v7)
- Mailing list: "proto-roughtime"
- Blog posts with background about Roughtime
  - https://blog.cloudflare.com/roughtime/
- Longer talk in the IoT WG later
- Contact me: wingel@netnod.se