"Vad är klockan?"

Swedish for "What time is it?"

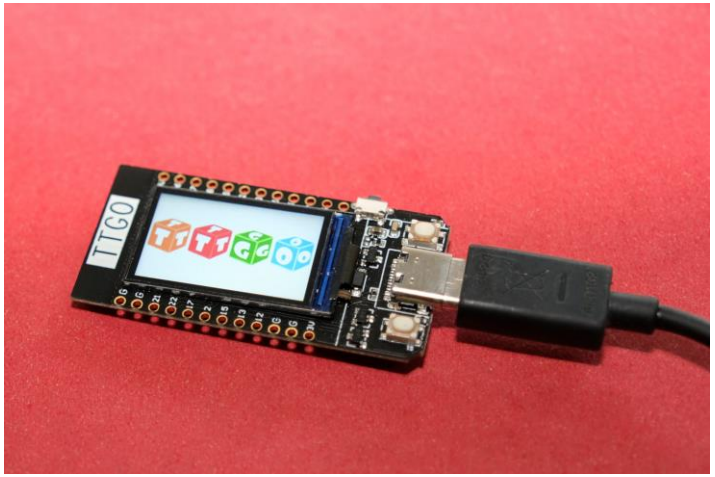
A secure way to find out what time it is

Christer Weinigel, Netnod 2023-01-26

Why accurate time is important

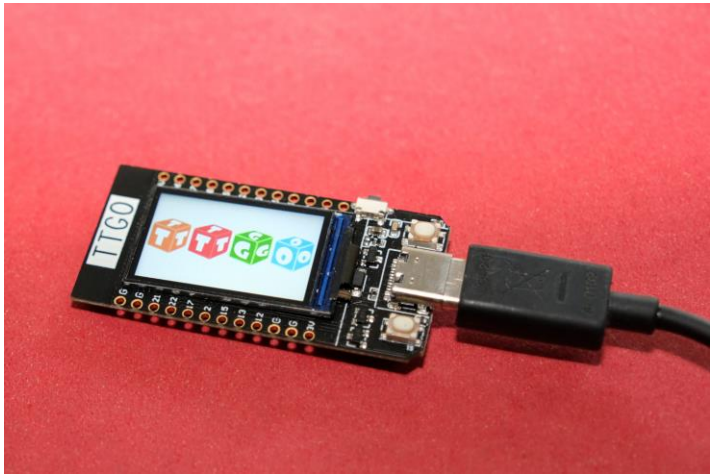
- Many security critical protocols need accurate time
  - Within a few minutes or hours
  - DNSSEC, secure domain name lookups
  - TLS/SSL, X509 certificates, the basis of many other protocols
    - HTTPS, everything on the web
    - SMTPS, IMAPS, POP3S, secure mail
  - Risk: fall back to insecure algorithms, leaked information
- The application itself might need accurate time
  - Example: electronic door lock

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 a RTC, but no battery backup by default
  - "Shipping mode"
    - Even with a battery clock will not run before first power on
- "Ten year on the shelf problem"

Problems



- NTP (Network Time Protocol)
  - Lacks security
- NTS (Network Time Secure)
  - Depends on DNSSEC/TLS
    - Which depend on having accurate time
  - Complex protocol not suited for resource constrained devices
- Bootstrapping
- What if a time server fails or is compromised?

Goals

- Something that can bootstrap time
- Should not rely on already having time
- Should not rely on a single server
- Should preferably work on resource constrained devices
- Create a library
  - Portable to many platforms (Linux, Arduino, FreeRTOS, Zephyr)
  - Easy to use, and easy to use correctly
  - With example code and documentation

Possible solution: Roughtime

- Protocol is an IETF Draft by Anchal Malhotra
- Long term "certificates" that never expire
  - Are not X509 certificates
  - Ed25519 public/private key pair
- Client asks many servers for time
  - Consensus, client uses time if enough time servers agree
  - Hope that enough servers are still up and running 10 years later
- Update list of servers when firmware is upgraded
- Same principles could be used with other time protocols

Results

- C and Python implementations, Linux, Arduino, ESP32
  - https://github.com/Netnod/vadarklockan
- Documentation
  - https://vadarklockan.readthedocs.io/en/latest/
- Netnod provides roughtime servers
  - sth1.roughtime.netnod.se, sth2.roughtime.netnod.se
- Other roughtime servers
  - Marcus Dansarie, roughtime.se

Future

- Adoption
  - Get people to use and improve our library
  - Make roughtime an IETF RFC
  - More servers
- People
  - Christer Weinigel <wingel@netnod.se>
    - Feel free to contact me if you have any questions
  - Calle Lindkvist <lindkvistcalle@gmail.com>
  - Filip Eriksson <filip_eriksson@live.se>

Thanks for listening!

Visit ut at netnod.se