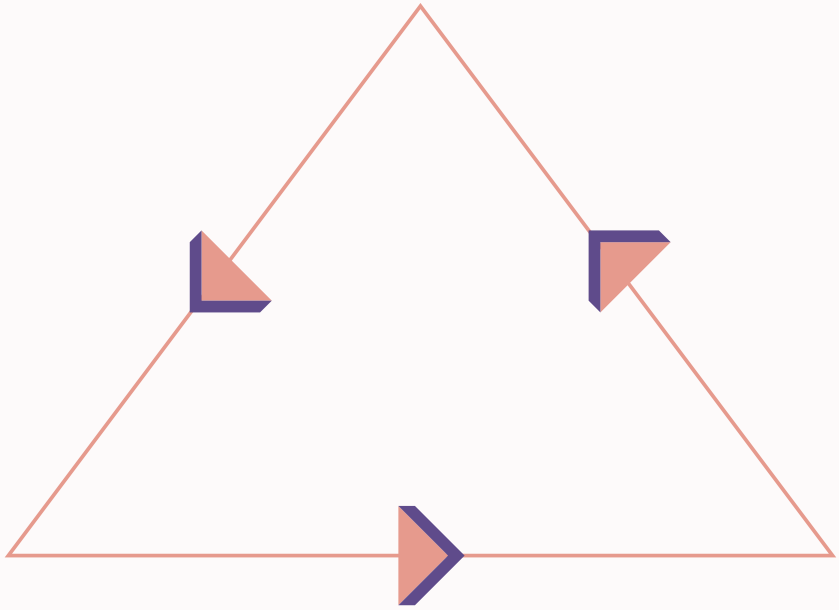
Could you tell me the time?

Securing time with NTS



Trifecta Tech Foundation

Introduction

- Hi all! My name is **Ruben Nijveld**
- I work at **Trifecta Tech Foundation**, a Dutch non-profit
- We mostly work on open infrastructure software
- My own focus is on time synchronization software
  - **ntpd-rs** (NTP)
  - **statime** (PTP)
  - **nts-pool**

Can anyone tell me the current time?

What is the current time, anyway?

- I was looking for the current time in UTC
  - but with an offset of +1 hour, because we're in Belgium right now and it is winter
- UTC is the worldwide standard for time
  - There are also TAI and UT1, but let's skip those for today
- Network Time Protocol (NTP) is the most used protocol to synchronize time over the internet

What is the current time, anyway?

- I was looking for the current time in UTC
  - but with an offset of +1 hour, because we're in Belgium right now and it is winter
- UTC is the worldwide standard for time
  - There are also TAI and UT1, but let's skip those for today
- Network Time Protocol (NTP) is the most used protocol to synchronize time over the internet

NTP is unprotected and can be spoofed trivially

Trifecta Tech Foundation

Why do we even care if time is synchronized?

- TLS connections (minutes)
- Kerberos tickets (minutes)
- TOTP tokens (seconds)
- Database synchronization (milliseconds)
- Logging in distributed systems (milliseconds)

But also: cellular networks (5G), internet exchanges, data centers, audio/video sync, streaming, high frequency trading, congestion control, work/task scheduling, power grid load balancing, astronomy

The world depends on UTC virtually everywhere

Knowing the current time is critical for security, and yet relies on a fundamentally insecure time synchronization protocol

Network Time Security (NTS) exists!

- An extension on top of NTP that adds a security mechanism to prevent third parties from sending forged messages
- NTS adds a key exchange phase based on TLS [1]
- NTP requests and responses include NTS extension fields
- Standardized in IETF RFC 8915 since September 2020

[1] Some might notice the interesting circular dependency here

Getting NTS on more devices

Unfortunately there are lots of devices that still use NTP by default

- We don’t know of any SNTP client that support NTS
- You can switch to a full NTP client with NTS support
  - NTPsec, Chrony or ntpd-rs
- We are patching systemd-timesyncd to support NTS [1]
  - We believe many users would benefit from a full NTP client, but acknowledge the usefulness of a very simple client

[1] https://github.com/systemd/systemd/pull/39010

Trifecta Tech Foundation

Pooling NTS servers

Your NTP client configuration probably points to `pool.ntp.org` [1]

- Pooling gives us an easy address everyone can use as a default
- The NTP pool uses DNS for sharing the NTP load of hundreds of millions of NTP requests per day between some 5000 NTP servers
- But NTS uses TLS for the key exchange step
  - issuing 5000 certificates for the same domain or sharing the same certificate between 5000 servers kills security
- We need alternative approaches

[1] Canonical uses their own time servers for Ubuntu, they actually switched to NTS in Ubuntu 25.10

NTS pool proposals [1]

- **KELB**: Use a load balancing proxy
  - No client-side modifications needed
  - Server needs modifications
  - Heavier load on the pool servers themselves
- **SRV**: Use DNS SRV records
  - Needs client-side modifications
  - No server modifications needed
  - Needs DNSSEC validation otherwise SRV records can be spoofed

[1] https://trifectatech.org/blog/enabling-pools-in-nts/

NTS pool

- **We need your servers and clients**
- Supported by ICANN Grant Program
- Highly experimental
- Will move domains once more stable
- We would like the best method to become IETF standard
- Patches available for Chrony, NTPsec and ntpd-rs

experimental.ntspooltest.org

Trifecta Tech Foundation

Join us in getting NTS everywhere!

Trifecta Tech Foundation

github.com/pendulum-project/nts-pool
trifectatech.org
experimental.ntspooltest.org

Ruben Nijveld
ntpd-rs, statime, nts-pool
ruben@trifectatech.org