Meinberg Funkuhren

NTP Work in Progress

Table of Contents

NTP Work in Progress

NTS

The **IETF NTPWG working group** works on **Network time Security** protocol extension (NTS), a replacement for NTP's `autokey`, which is less secure than originally expected, and a compatible, extensible format of the extension field for NTP network packets. See this article:

- NTP Authentication: Network Time Security (NTS)

ntimed-client

ntimed-client is a NTP client daemon written by **Poul-Henning Kamp** which implements some cool new features, including a modified approach to evaluate NTP time stamps, and leap seconds and TAI offset via DNS. Progress of the project as well as other ideas have been described at Poul-Hennings blog at

- http://phk.freebsd.dk/time/

The source code is available via a git repository:

- https://github.com/bsdphk/Ntimed

A Modified Approach to Evaluate NTP Time Stamps

This page illustrates the results of NTP queries to different servers on the local LAN, and on the internet:

- 20141024 – Filtering NTP
  http://phk.freebsd.dk/time/20141024/

And here's a different approach how to evaluate the time stamps from NTP packet exchanges:

- 20141107 – Probably Noon
  http://phk.freebsd.dk/time/20141107/

A Proposal how to Get Authenticated Time from HTTPS Servers

Poul-Henning Kamp proposed a way to get authenticated time from HTTPS servers. This approach doesn't provide the full accuracy of NTP, but may be a good plausibility check for the time returned via NTP protocol in the absence of **other authentication mechanisms**.

- 20151108 - The Authenticated Time issue
  http://phk.freebsd.dk/time/20151108/
- 20151115 - Do HTTPS servers know the time?
  http://phk.freebsd.dk/time/20151115/
- 20151129 Time over HTTPS specification
  http://phk.freebsd.dk/time/20151129/
- 20151212 Reference implementation “Time over HTTPS”
  http://phk.freebsd.dk/time/20151212/

Leap Seconds and TAI Offset via DNS

Poul-Henning Kamp's Proposal

Poul-Henning Kamp proposed to use DNS to distribute leap second announcements and the current TAI offset. This is much easier than distributing a leap second file and standard runtime library calls can be used to implement this. The idea is to to let a function like getaddrinfo() resolve a specific hostname, but don't interpret the returned number as IPv4 address. Instead decode it in a specific way to extract leap second information and TAI offset from the returned bit pattern.

- 20151122 - Leapseconds via DNS
  http://phk.freebsd.dk/time/20151122/

Tony Finch's Example DNS Server

Tony Finch runs a DNS server installation where you can get a cryptographically signed leap second table in various formats using a DNS lookup of `leapsecond.dotat.at` (ask for `HINFO` records to get a terse summary of the formats).

For example:

```
host -t HINFO leapsecond.dotat.at
;; Truncated, retrying in TCP mode.
leapsecond.dotat.at host information "A" "The months that end with a leap
second encoded per http://phk.freebsd.dk/time/20151122/ plus an illegal
record to terminate the list"
leapsecond.dotat.at host information "TXT" "The intervals between leap
seconds in months, separated by a + or - for positive or negative leap
seconds, and terminated by a ?"
leapsecond.dotat.at host information "AAAA" "The date and time of the last
second in months that end with a leap second, plus the last second of the
known validity period if that is not a leap second"
leapsecond.dotat.at host information "TYPE65432" "Compressed binary encoding
```

```
of the TXT record"
```

Here is a blog post that describes the text format:

- **Compact encoding of the leap seconds list**
  https://fanf.dreamwidth.org/120995.html

and another post that describes the binary format, which is more compact:

- **Even more compact encoding of the leap seconds list**
  https://fanf.dreamwidth.org/121672.html
- Tony Finch's git project **Publish list of leap seconds in the DNS**
  https://dotat.at/cgi/git/leapseconds.git and detailed information:
  https://dotat.at/cgi/git/leapseconds.git/blob/HEAD:/syntax.md

Information was published by Tony Finch on the IETF NTP mailing list:

- https://mailarchive.ietf.org/arch/msg/ntp/oYCF5og4sy65CPDiUrVT5bfJ8WY

— Martin Burnicki martin.burnicki@meinberg.de 2020-02-18