November 13, 2017
IETF100-Singapore

On Implementing Time

draft-aanchal-time-implementation-guidance-00

Aanchal Malhotra[1], Martin Hoffmann[2], Willem Toorop[3]
Boston University[1], Open Netlabs[2], NLnet Labs[3]

Motivation

- functionality and security of apps hinges on some notion of time.
- choose from multiple time values on systems.
- applications oblivious to implications of choosing one or the other time value for implementation

This draft

- describes properties of various time values available on modern operating systems
- discusses trade-offs of using one over the other
- provides guidance to help implementers make an informed choice

Outline

- define available clocks
- how they are different?
- expressing time: time stamps vs time spans
- current implementation & why is it bad?
- alternative approaches

Different clocks

- **Wall time**: agreed upon “ideal time”
- **Raw time:** unadjusted system time
- **Adjusted raw time:** raw time fixed for clock drift
- **Real time**: adjusted raw time shifted to match wall time

Differences from wall time

<table>
<tr><th>raw time</th><th>adjusted raw time</th><th>real time</th></tr>
<tr><td colspan="2">difference in time b/w two points</td><td>absolute time value</td></tr>
<tr><td colspan="2">monotonically increasing</td><td>can jump in either direction</td></tr>
<tr><td>not adjusted for clock drifts</td><td colspan="2">adjustable (manually/ network time protocols)</td></tr>
</table>

Expressing time
time spans vs time stamps

- **Time spans**: represent desired length of time
  e.g. time-out values or time-to-live (TTL) values

- **Time stamps**: represent a point in wall time
  e.g. validity of objects from and to a fixed time

```
d0.dig.afilias-nst.info. 83797  IN     AAAA    2a01:8840:9::1
ns-ext.nlnetlabs.nl.     7598   IN     RRSIG   A 8 3 10200 20171129015003 20171101015003 02
393 nlnetlabs.nl. zOcSBB8C06IpUZ+8OGxdafqMv9gCYGHkCG9wDayetxwn/D/kxnec6uNU unYrsMDuVZUPYo6Gr
lo3AHM17HnuDPYoFuPXIuAQNGCej8hXm2DB/NbR QotCaaXUuoQ4hqiiifwK4qbW8W9QT79Jc251CKBsCL28TOmcVYFq
h02H kGQ=
```

How do software implementations deal with time stamps & time spans?

COMMON APPROACH

Time spans - translated to time stamps.

Time stamp =? current system time

Updated by NTP

Why is it bad?

- Real Time
  - can be set or overwritten manually
  - subject to adjustments by timing protocols
    - Recent attacks [1,2,3] show off-path time-shifting and Denial-of-Service attacks on these protocols

Note: Time stamps always based on wall time

Alternative implementation approaches for time spans

- **SHOULD NOT** use real time
- Other options?
  - raw time
  - adjusted raw time
- Application specific: tolerate clock drift to a certain amount can use raw time, otherwise adjusted raw time

Way forward for the draft?

References:

[1] **Attacking the Network Time Protocol.**

A. Malhotra, I. Cohen, E. Brakke, S. Goldberg. In the proceedings of The Network & Distributed System Security Symposium (NDSS), CA, 2016.

[2] **Attacking NTP's Authenticated Broadcast Mode**.

A. Malhotra, S. Goldberg. ACM SIGCOMM, Computer Communication Review, 2016.

[3] **The Security of NTP's Datagram Protocol.**

A. Malhotra, M.V. Gundy, M. Varia, H. Kennedy, J. Gardner, S. Goldberg. In the proceedings of 21st International Conference on Financial Cryptography and Data Security (FC), 2017.