Roughtime

draft-roughtime-aanchal-01

Aanchal Malhotra*, Adam Langley^, Watson Ladd✓

*Boston University, ^Google, ✓Cloudflare
## Motivation

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Authenticated Server</th>
<th>Server Malfeasance</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP, Chronos</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>NTO-MD5</td>
<td>Yes*</td>
<td>No</td>
</tr>
<tr>
<td>NTP-Autokey</td>
<td>Yes*</td>
<td>No</td>
</tr>
<tr>
<td>NTS</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Roughtime</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

* has serious known issues
What is Roughtime?

Protocol that:

• achieves “rough” time synchronization
• detects servers that provide inaccurate time
• Provides cryptographic proof of their malfeasance
many applications that do not necessarily require highly accurate and precise time information

- certificate verification
- delegated credentials lifetime
- IoT devices
- TOR service directory
Issue 1: Time scale?

Currently in draft:

- MIDP - number of microseconds since the Unix epoch.
- RADI - server's estimate of the accuracy of MIDP at the time they compose the response packet.
- LEAP - TAI-UTC offset at MIDP
Need trust anchor that can

- maintain and distribute list of trusted servers
- enforce appropriate policies
Questions & way forward?