March 26, 2019
IETF-104 NTP/TICTOC WG

Roughtime
draft-roughtime-aanchal-01

Aanchal Malhotra*, Adam Langley^, Watson Ladd✓
*Boston University, ^Google, ✓Cloudflare

Motivation

Protocol	Authenticated Server	Server Malfeasance
NTP, Chronos	No	No
NTO-MD5	Yes*	No
NTP-Autokey	Yes*	No
NTS	Yes	No
Roughtime	Yes	Yes

* 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

Applications

many applications that do not necessarily require highly accurate and precise time information

- certificate verification
- delegated credentials lifetime
- IoT devices
- TOR service directory

Issue1: 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

Trust anchors & policies

Need trust anchor that can

- maintain and distribute list of trusted servers
- enforce appropriate policies

Questions & way forward?