Roughtime

□□

- Background
- Next steps

Roughtime is a simple, flexible, and secure authenticated time protocol developed by Google.

Background

Endpoints on the Internet often synchronize their clocks using the Network Time Protocol (NTP). NTP provides precise synchronization, but is frequently deployed without a means of authentication. This is due to a combination of issues.

As a result, a man-in-the-middle attacker can easily influence a victim's clock. By moving them back in time, the attacker can, for example, force a victim to accept an expired (and possibly compromised) TLS certificate or session ticket.

For many applications, *precise* network time is not essential. It is sufficient to have *accurate* time to mitigate these kinds of attacks, such as within 10 seconds of real time. This observation is the primary motivation behind Roughtime.

Next steps

For more technical details on Roughtime, refer to the introductory blog post.

To get started, refer to Get the Roughtime. For more practical guidance on using the Roughtime, refer to our how-to guide.

□□□ #2
□ □□□ □□□ 2026-11-01 04:55:35 UTC
□ □□□ □□□ 2026-11-01 04:55:36 UTC