Workgroup: Internet Engineering Task Force
Internet-Draft:
draft-ietf-ntp-roughtime-ecosystem-01
Published: September 2021
Intended Status: Informational
Expires: 18 March 2022
Authors: W. Ladd M. Dansarie
Cloudflare

Roughtime Ecosystem

Abstract

This document specifies the roles of Roughtime validators, clients, and servers in providing a ecosystem for secure time.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 5 March 2022.

Table of Contents

1. Introduction

The Roughtime protocol enables servers to provide cryptographic proof of the times requests were made. This enables clients to expose cheating by servers. This document describes how these proofs are seralized and verified, as well as APIs to access and submit reports of malfeasnce in an automated manner.

2. Chaining in roughtime

Two responses are chained if the NONC field of the second is SHA-512(blinder || first) where blinder is a 64 byte value. Blinder MUST be generated uniformly at random to prevent tracking. The first response is serialized as a roughtime message. The first response is chained to the second.

A chain is a sequence of messages where each message is chained to the one before. Every contiguous subsequence of a chain is a chain.

3. Impeachement

For each index i, let m_i denote the timestamp of the response, r_i the radius around it. Then we have m_i-r_i the earliest actual time at which the response could have been generated, and m_i+r_i the latest actual time at which the response could have been generated.

If all requests are generated honestly m_i+r_i < m_{i+j}-r_{i+j} holds for all indices i and positive numbers j. A failure of this relation to hold demonstrates that at least one of the responses was generated incorrectly.

The more distinct servers and responses that are mutually consistent except for the questionable response, the more likey a failure of the generator of the errneous response is.

4. Serialization of chains

TODO

5. Submission API

6. Viewing Reports

7. Trust Anchors and Policies

A trust anchor is any distributor of a list of trusted servers. It is RECOMMENDED that trust anchors subscribe to a common public forum where evidence of malfeasance may be shared and discussed. Trust anchors SHOULD subscribe to a zero-tolerance policy: any generation of incorrect timestamps will result in removal. To enable this trust anchors SHOULD list a wide variety of servers so the removal of a server does not result in operational issues for clients. Clients SHOULD attempt to detect malfeasance and report it as discussed in this document.

Because only a single Roughtime server is required for successful synchronization, Roughtime does not have the incentive problems that have prevented effective enforcement of discipline on the web PKI.

8. Normative References

[I-D.ietf-ntp-roughtime] Malhotra, A., Langley, A., Ladd, W., and M. Dansarie, "Roughtime", Work in Progress, Internet-Draft, draft-ietf-ntp-roughtime-05, 24 May 2021, <https://www.ietf.org/archive/id/draft-ietf-ntp-roughtime-05.txt>.

Authors' Addresses

Watson Ladd
Cloudflare
101 Townsend St
San Francisco,
United States of America

Email: watsonbladd@gmail.com

Marcus Dansarie
Sweden

Email: marcus@dansarie.se
URI: https://orcid.org/0000-0001-9246-0263