The Geohash HTTP Client Hint

Abstract

   This documents defines an HTTP Client Hint for sharing a client's
   rough location using the Geohash format.

Discussion Venues

   This note is to be removed before publishing as an RFC.

   Source for this draft and an issue tracker can be found at https://
   github.com/tfpauly/privacy-proxy.

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 3 April 2022.

Table of Contents

1. Introduction

HTTP Client Hints [RFC8942] defines a convention for HTTP headers to
communicate optional information from clients to servers as hints.
This can be done conditionally based on if a server claims supports
for a particular hint.

This document defines a client hint that can be used to send a
location that the client wants to use for influencing server
behavior. It uses the Geohash algorithm [GEOHASH] to encode latitude
and longitude coordinates into an alphanumeric token that can be
truncated to provide a less specific location.

This header is intended to be used to provide rough geolocation
hints to servers in situations where the server cannot directly
ascertain the location of the client. For example, a client that is
accessing a server through a proxy or a VPN might provide a rough
hint to a server when looking up information that may vary depending
on location.

This document also defines a how forward proxies can use proxy
status fields to inform clients about the result of their Geohash
hints.

1.1. Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and
"OPTIONAL" in this document are to be interpreted as described in

BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all
capitals, as shown here.

2. Geohash Header

The "Sec-CH-Geohash" is an Item Structured Header [RFC8941]. Its
value MUST be a String, and MUST have at least 1 character and no
more than 12 characters. The ABNF is:

Sec-CH-Geohash = sf-string

The string itself is an encoded Geohash, which uses the 32 different
characters from the "Geohash alphabet" [GEOHASH].

The following example shows an encoding of the coordinates
57.64911,10.40744:

 Sec-CH-Geohash: "u4pruydqqvj"

Servers that can provide different content based on Geohash hints
SHOULD include the headers in their "Accept-CH" list.

 Accept-CH: Sec-CH-Geohash

Servers also SHOULD indicate for any cacheable content if the
Geohash hint will influence the cached content, using the "Vary"
header.

 Vary: Sec-CH-Geohash

3. Server Behavior

Upon receiving a Geohash Client Hint, a server can use the
information to influence its behavior in various ways.

The server can use the Geohash to determine the content of HTTP
responses, as a replacement for inferring location from client IP
addresses.

If the server is acting as a forward proxy, such as a CONNECT proxy,
it can use the Geohash to determine an appropriate geo-mapped IP
address to use for outbound connections, or a client subnet to
present in the EDNS0 Client Subnet extension for DNS queries
[RFC6891] [RFC7871].

3.1. Proxy Behavior

If a proxy receiving the Geohash hint cannot respect the location
indicated by the hint, it SHOULD include a Proxy-Status header [I-

D.ietf-httpbis-proxy-status] in its response, with the "details"
parameter containing the string "invalid geohash".

Proxy-Status: ExampleProxy; details="invalid geohash"

4. Security Considerations

The use of the Geohash Client Hint MUST use the Sec- header prefix
as recommended in [RFC8942].

Client location can be used to fingerprint and tracker users, so
clients MUST have a default policy around when to allow use of the
Geohash Client Hint, as well as a default length of Geohash.
Shorter, truncated Geohashes provide less specific locality.

Servers MUST NOT use Geohash Client Hints for making security or
access-control decisions, as the value can be spoofed by a client.
The hint is intended only for use in optimizing behavior.

5. IANA Considerations

5.1. HTTP Headers

This document registers the "Sec-CH-Geohash" header in the
"Permanent Message Header Field Names" registry <https://
www.iana.org/assignments/message-headers>.

```
+----------------------+----------+--------+---------------+
| Header Field Name    | Protocol | Status |   Reference   |
+----------------------+----------+--------+---------------+
| Sec-CH-Geohash       |   http   |  exp   | This document |
+----------------------+----------+--------+---------------+
```

6. References

6.1. Normative References

[I-D.ietf-httpbis-proxy-status] Nottingham, M. and P. Sikora, "The
          Proxy-Status HTTP Response Header Field", Work in
          Progress, Internet-Draft, draft-ietf-httpbis-proxy-
          status-06, 16 August 2021, <https://www.ietf.org/archive/
          id/draft-ietf-httpbis-proxy-status-06.txt>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
          Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/

RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8941] Nottingham, M. and P-H. Kamp, "Structured Field Values for HTTP", RFC 8941, DOI 10.17487/RFC8941, February 2021, <https://www.rfc-editor.org/info/rfc8941>.

[RFC8942] Grigorik, I. and Y. Weiss, "HTTP Client Hints", RFC 8942, DOI 10.17487/RFC8942, February 2021, <https://www.rfc-editor.org/info/rfc8942>.

6.2. Informative References

[GEOHASH] "Geohash", 2020, <https://en.wikipedia.org/wiki/Geohash>.

[RFC6891] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, RFC 6891, DOI 10.17487/RFC6891, April 2013, <https://www.rfc-editor.org/info/rfc6891>.

[RFC7871] Contavalli, C., van der Gaast, W., Lawrence, D., and W. Kumari, "Client Subnet in DNS Queries", RFC 7871, DOI 10.17487/RFC7871, May 2016, <https://www.rfc-editor.org/info/rfc7871>.

Authors' Addresses

Tommy Pauly
Apple Inc.
One Apple Park Way
Cupertino, California 95014,
United States of America

Email: tpauly@apple.com

David Schinazi
Google LLC

Email: dschinazi.ietf@gmail.com