INTERNET-DRAFT
<draft-daviel-http-geo-header-05>
Expires: Jun 7, 2008
Intended status: Standards Track

Vancouver Webpages
December 7, 2007

Geographic extensions for HTTP transactions

Status of this Memo

Abstract

This memo describes a method of adding simple geographic position or region information to HTTP transactions using extension headers. It allows location-based services on the World Wide Web, without the additional overhead of geographic query requests and possibly graphical input. Extension headers transmit predefined or detected position information to reflect a location that the requesting agent is interested in. This information may be used by a server to present appropriate position-dependent responses, such as search engine results or weather maps.

1. Introduction

Many resources on the World-Wide-Web are associated with a particular place on the Earth's surface. HTML documents may contain geo tags as described in [RFC2731],[1] but more information with geographic data is stored in databases (e.g. "yellow pages"). Resource discovery on the Web has thus far focused on document title and open-text keyword searching, in the case of yellow pages postcodes or map selection are also used. However, resource discovery based on geographic criteria is not widespread because it calls for extensive user-input in terms of graphical selection. Mobile devices especially will make use of geographic search but can only with difficulty specify the required location data (e.g. due to small displays or limited keypads). On the other hand, mobile devices often integrate a GPS receiver or can make benefit of network based positioning. It may be beneficial to facilitate automatic, but user- driven use of geographic information on the Web. A specification for standardized transmission of position data will allow advanced search modes, more user-friendly web pages (e.g. bus schedules in conjunction with nearest stations) and new location based services which are currently not available on the World-Wide-Web (e.g. local advertising at small scale). By including geographic extension headers in HTTP requests, it is possible to tailor responses to the location of the requestor, in the same way that the language of the response may be tailored by using the Accept-Language header [RFC2616].

2. Example Usage

An example of a commonly used resource on the World-Wide-Web is a weather map, used by a traveling person. Such a service usually covers different regions. On a map, the traveler could select the current position and even store it using cookie methodology [RFC2965]. However, when moving to another region the cookie will represent invalid location information.

Beside using cookies, this service is also able to process specific position information. It announces this capability by sending the following header: "Vary: Geo-Position". A browser can use this header if it is connected to a positioning source such as GPS or has preconfigured data (see region codes, section 3.3). Once the user decides to send position information in this specific case or in general, each request to this service includes another header representing the current position, e.g. "Geo-Position: 48.541;-123.843". In this case, the server may tailor the weather map to Vancouver Island without further input.

Other services may include positioning metadata such as accuracy and other parameters for identifying a nearby or distant object.

3. Implementation

3.1 Geographic Position

A request MAY include a geographic position using an HTTP extension header. The identifier "Geo-Position" is used for this purpose. Latitude, longitude and altitude are separated by a semicolon. Other values are given as key-value-pairs (e.g. hdn=130), separated by a whitespace. Latitude and longitude are mandatory and MUST be included in each geo-position request. Optional key-value-pairs:

```
epu       - estimated position uncertainty
hdn       - heading clockwise from true north
spd       - speed
```

Latitude (degrees north of the equator) and longitude (degrees east of the prime meridian on the [WGS-84] spheroid) values shall be expressed as decimal fractions of degrees. Whole degrees of latitude shall be represented by a decimal number ranging from 0 through 90. Whole degrees of longitude shall be represented by a decimal number ranging from 0 through 180. When a decimal fraction of a degree is specified, it MUST be separated from the whole number of degrees by a decimal point (the period character, "."). The number of decimal places given should reflect the precision of the position determination method or be reduced in order to reflect privacy issues (see section 5)

Latitudes north of the equator MAY be specified by a plus sign (+), or by the absence of a minus sign (-), preceding the designating degrees. Latitudes south of the equator MUST be designated by a minus sign (-) preceding the digits designating degrees. Latitudes on the equator MUST be designated by a latitude value of 0.

Longitudes east of the prime meridian MAY be specified by a plus sign (+), or by the absence of a minus sign (-), preceding the designating degrees. Longitudes west of the prime meridian MUST be designated by a minus sign (-) preceding the digits designating degrees. Longitudes on the prime meridian MUST be designated by a longitude value of 0. A point on the 180th meridian shall be taken as 180 degrees West, and shall include a minus sign.

Any spatial address with a latitude of +90 (90) or -90 degrees will specify a position at the true north or true south poles, respectively. The component for longitude may have any legal value.

Altitude is expressed as a signed decimal number of metres above datum, which is [WGS-84]. Decimal places (if required) MUST be

separated by a decimal point ("."). Points having zero or positive elevation MAY omit the plus sign.

The estimated position uncertainty states the quality of the submitted position (latitude, longitude, altitude). It is expressed in metres, and describes a circle or sphere of 95% positioning probability.

Heading is expressed in decimal degrees clockwise from true north.

Speed is given in metres per second.

If a parameter is intended to be transmitted but the value cannot be ascertained due to technical reasons, it shall be given as "N/A" (without quotes).

3.1.1 Examples

(Host headers [RFC2616] are for exemplification only)

```
Host: maps.example.com
Geo-Position: -10;+60
```

requests for a map at position 10 degrees south, 60 degrees east. It must be assumed that a more precise position is not available.

```
Host: weather.example.com
Geo-Position: -10.28;60.84;120 epu=50
```

requests for a weather forecast for instance at position 10.28000 degrees south, 60.84000 degrees east, 120 metres above datum ([WGS-84]) with a 95%-confidence boundary of 50 metres (radius).

```
Host: tourism.example.com
Geo-Position: -10.28;60.84 epu=50 hdn=45
```

requests for information about an object in north-east direction from the given position (e.g. the city hall on a place).

```
Host: traffic.example.com
Geo-Position: -10.28;60.84 epu=50 hdn=45 spd=15
```

requests for traffic congestion reports for the area at the given position but traffic in north-east direction only. The service may assume an average speed for further area selections.

3.2 Negotiation

Use of negotiation is RECOMMENDED.

A geo-enabled server implicitly uses server-driven negotiation as described in [RFC2616]. For proper operation of HTTP caches, a Vary header SHOULD be send by the server to indicate that it will serve different content for requests with different values of the specified headers, and that a cache should not re-use a cached response unless a new request has matching headers.

A geo-enabled server SHOULD send appropriate Vary headers to indicate which client Geo headers will cause a tailored response to be generated.

A Vary header MAY be used as a means for a server to announce to a client that it will accept geo headers, triggering a filter dialogue (section 3.4).

3.2.1 Examples

Vary: Geo-Position

indicates that a server will serve different content in response to different values of Geo-Position header sent by the client.

Vary: Geo-Country, Geo-A1

indicates that a server will serve different content in response to to different values of either Geo-Country or Geo-A1 (national subdivision) headers.

3.3 Region Codes

Instead of position (or even additionally), a client may name an administrative area it is interested in. The identifier "Geo-Country" is used to specify a country code from [ISO3166-1]. The identifiers "Geo-A1", "Geo-LMK" etc. are used to specify a civic address or region [PIDF-LO]

They are used as extension headers. As an example,

```
Geo-Country: CA
Geo-A1: ON
```

requests a resource tailored to Ontario, Canada.

3.4 User Filters

While a geo position header in an HTTP request directs the server to

return information pertaining to a particular position, the server may infer that the position requested is the current location of the client. In order to protect the privacy of users against inadvertent leakage of their personal location information, a user must be able to control what information is sent to servers.

A Web browser, client or geo-enabling proxy MUST implement a mechanism for filtering geographic information sent to servers ([RFC3693]). It may maintain a list of trusted sites to which position data may be sent, or it may maintain a list of regular expressions which is applied to requested URLs. Position data sent to remote servers must be filtered using rules based on this list. The user MUST be provided with tools to maintain this list.

Such a list might contain fields for "address of web site", "allow/block", "precision", "auth" and "secure". The browser will send the current position in request headers providing that the site address is listed and allowed. Position information would be sent to the defined precision. If the "secure" field is present, then the browser will only send position information using an encrypted protocol ([3],[RFC4346]). If the "auth" field is present, then the browser will only send position information during an authenticated HTTP session (one in which an Authorization header is sent) ([RFC2617]).

If the client receives an HTTP response containing a Vary header which specifies a Geo header, and if the site is not in the filter list, the browser should open a dialogue with the user to ask them whether position data should be sent. The agent may ask, for instance, whether position data should be sent once, always, or never and will save this information appropriately. It may also ask for optional data to be sent.

Fuzzing of position information (decreasing its precision) may typically be done by rounding or reducing the number of decimal places in latitude and longitude. In order to avoid a "line crossing" effect, where the exact position of a moving client may be deduced as, for example, 43.13000 at the instant its declared coordinate changes from 43.12 to 43.13, it is recommended that a random offset be added before truncation.

The filter may support a default setting for unlisted sites, for instance to use a 10km precision for secure sites and to block insecure sites. The installation value of such a default setting must be chosen to minimize privacy impact. It should not send more precise positions than may typically derived from the client Internet address, such as a metropolitan area or university campus.

3.4.1 Disposition of Location Information

Location information MUST NOT be forwarded to another entity by the server to which it was sent (the entity that has satisfied the user's privacy filter). For instance, if alpha.example.com is trusted but redirects an HTTP request to beta.example.com, a Geo-Position header must not be sent to beta.example.com unless that site is also trusted.

3.5 Proxy

Geo headers may be generated directly in a client, such as a geo-enabled Web browser, or may be added by a geo-enabled HTTP proxy agent, allowing a standard browser to be used. The proxy agent may be included on the same platform as the client, as might be the case where location data is available from an integral GPS receiver. Alternatively, the proxy agent may be external, as might be the case where location data is determined by wireless triangulation from a number of fixed base stations. If location data is added by an external proxy agent, the user MUST be able to filter such data.

Geo extension headers are end-to-end header fields and should be transmitted to the ultimate destination of the declaration (the server). They should be forwarded and ignored by non-geo-enabled proxy agents.

4. Formal Syntax

The syntax uses augmented BNF, described in [RFC2616].

```
DIGIT   = %x30-39   ; 0-9
UCASE   = %x41-5A   ; A-Z
PLUS    = %x2B      ; +
MINUS   = %x2D      ; -
DECIMAL = %x2E      ; .
CRLF    = %x0D.%x0A ; return, linefeed
SIGN    = MINUS / PLUS

country     = 2UCASE                                ; [ISO3166-1]
latitude    = [ SIGN ] 1*2DIGIT [ DECIMAL 1*DIGIT ] ;  -90  -  90
longitude   = [ SIGN ] 1*3DIGIT [ DECIMAL 1*DIGIT ] ; -180  - 180
altitude    = [ SIGN ] 1*DIGIT [ DECIMAL 1*DIGIT ]  ;      metres
uncertainty = 1*DIGIT [ DECIMAL 1*DIGIT ]           ;      metres
heading     = 1*3DIGIT [ DECIMAL 1*DIGIT ]          ;       0-360
speed       = 1*DIGIT [ DECIMAL 1*DIGIT ]           ; metre/sec.
```

```
lat        = latitude
lon        = longitude
alt        = altitude
epu        = "epu" "=" uncertainty *LWS
hdn        = "hdn" "=" heading *LWS
spd        = "spd" "=" speed *LWS

Vary            = "Vary" ":" ( "*" | 1#field-name )
region-header   = "Geo-Country:" country-code CRLF
position-header = "Geo-Position:" LWS
                  lat;lon[;alt] *( epu | hdn | spd ) CRLF

response-header = accept-header
request-header  = [ region-header ] [ position-header ]
```

4.1 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

5. Security Considerations

This draft raises certain issues of privacy. The position information sent in a request is a qualification of the HTTP request, and does not necessarily represent the actual position of the requesting agent. However, if geo extensions are added to an HTTP request, the server may infer the location of the person making the request. If a Geo-Position extension is given to a high degree of accuracy for a request made from a fixed location such as a private residence, the server may be able to uniquely identify the street address. If no controls are implemented, it would be possible to identify a person's location and perhaps identity from their general Web browsing activity.

In cases where a portion of the data path from client to server includes an unencrypted link, it may be possible for data including position information to be intercepted by a third party. This third party may be able to determine the location of the mobile device, and may be able to associate the mobile device with a particular person visually based on location data. This association may exacerbate the loss of privacy inherent in using an unencrypted wireless data path.

5.1 Encryption

It is suggested that, where possible, HTTP requests including geo

headers be encrypted using an encryption scheme such as SSL or TLS [3],[RFC4346]. This mechanism provides a degree of trust in the identity of the server, and guards against disclosure of possibly sensitive position information by proxy agents, firewalls or recording devices.

Another mechanism which may be used to protect the privacy of the user is to use a trusted proxy agent such as Squid [4]. Use of a proxy which does not forward the client address will prevent an untrusted server from tracking the position of a particular client by address, though tracking by cookies [RFC2965] may be possible if these are enabled, or by "web bugs" [5].

6. IANA considerations

The message header fields below should be added to the permanent registry (see [RFC3864]).

6.1. Geo-Position

Header field name: Geo-Position Applicable protocol: http Status: standard Author/Change controller: IETF Specification document: this specification (Section 3.2)

6.2. Geo-Country

Header field name: Geo-Country Applicable protocol: http Status: standard Author/Change controller: IETF Specification document: this specification (Section 3.3)

7. Internationalization considerations

Geo-Position, Geo-Velocity and Geo-Country values are defined using US-ASCII.

8. References

8.1 Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2616] Fielding, Gettys, Mogul, Frystyk, Masinter, Leach, Berners-Lee, "Hypertext Transfer Protocol HTTP/1.1", RFC 2616, June 1999.

[RFC3864] Klyne, Nottingham, Mogul, "Registration Procedures for Message Header Fields", BCP 90, RFC 3864, September 2004.

[WGS-84] United States Department of Defense; DoD WGS-1984 - Its Definition and Relationships with Local Geodetic Systems; Washington, D.C.; 1985; Report AD-A188 815 DMA; 6127; 7-R-138-R; CV, KV;

[ISO3166-1] International Organization For Standardization, "Codes for the representation of names of countries and their subdivisions - Part 1: Country codes", Standard ISO 3166-1:2006, November 2006.

10.2 Informative References

[1] Daviel, Kaegi, "Geographic registration of HTML documents", Internet Draft draft-daviel-html-geo-tag-08, Sept. 2007

[3] Frier, Karlton, Kocher, "The SSL 3.0 Protocol", November 1996.

[4] Wessels, Claffy, "ICP and the Squid web cache", IEEE Journal on Selected Areas in Communication, April 1998.

[5] Smith, "The Web Bug FAQ", November 1999.

[RFC2731] Kunze, "Encoding Dublin Core Metadata in HTML", RFC 2731, December 1999.

[RFC2965] Kristol, Montulli, "HTTP State Management Mechanism", RFC 2965, October 2000.

[RFC4346] Dierks, Rescorla, "The Transport Layer Security (TLS) Protocol", RFC 4346, April 2006.

[RFC2617] Franks, Hallam-Baker et al., "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617. June 1999

[RFC3693] Cuellar, Morris et al., "Geopriv Requirements", RFC 3693, February 2004

[PIDF-LO] M. Thomson, J. Winterbottom, Revised Civic Location Format for PIDF-LO, draft-ietf-geopriv-revised-civic-lo-07, December 2007

9. Acknowledgments

Rohan Mahy and Patrik Faltstrom of Cisco Systems, for semantics.

10. Authors' Addresses

Andrew Daviel, BSc.
Vancouver Webpages, Box 357
185-9040 Blundell Rd
Richmond BC
V6Y 1K3
Canada

Tel. (604)-377-4796
Fax. (604)-270-8285
advax@triumf.ca

Felix A. Kaegi
Dipl.Informatik Ing. ETH (M.Sc.)
Friedensgasse 51
CH-4056 Basel
SWITZERLAND

Phone +41 61 383 10 01
Fax +41 79 625 27 41
skype felix_kaegi
felix.kaegi@gmail.com

Martin Kofahl
University Rostock
Geodesy and Geoinformatics
D-18051 Rostock
GERMANY

Phone +49 381 498 3212
Fax +49 381 498 3202
m.kofahl@gmx.net

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.