Internet Draft
Document: draft-morris-geopriv-core-00.txt
Expires April 28, 2003

John B. Morris, Jr.
Center for Democracy
and Technology

D. Mulligan
Samuelson Law, Technology,
and Public Policy Clinic

J. Cuellar
Siemens AG

October 2002

Core Privacy Protections for Geopriv Location Object

Status of this Memo

Copyright Notice

Abstract

In designing the requirements for the Geopriv Location Object (LO), a key question for the working group is whether to include privacy-protecting rules inside the LO itself, and if so, how many and what rules should be contained in the LO. The Internet-Draft first suggests that the LO should contain at least a limited set of privacy rule fields, and second proposes a set of rules for inclusion in the Location Object.

Table of Contents

1. Introduction and Overview

A critical question facing the Geopriv working group is whether the Location Object (LO) to be designed should include fields for particular privacy-protecting rules, or instead should simply refer to an external set of privacy rules.

There are at least four plausible answers to this question, labeled somewhat arbitrarily as follows:

* "Entirely External" -- the LO should only contain a URI reference to an external set of privacy rules that must be followed by any recipient of the LO.

* "Bare Bones Internal" -- the LO should contain at most one or two rules that specify, for example, that the Location Information (LI) shall not be retained past xyz date (or longer than xyz duration), along with a URI reference to an external set of privacy rules that must be followed by any recipient of the LO.

* "Limited Internal" -- the LO should contain a limited set of rules (say, 4 to 7 rules) that cover the great bulk of likely privacy situations (as well as the ability to include a URI reference to an external set of privacy rules if more robust rules are needed, or external rule storage is preferred).

* "Full Internal" -- the LO should be defined to be able to contain a full, robust, and potentially complex set of privacy rules.

The "Full Internal" option would yield the most complex LO, would be the most complex to define and implement, and may not be consistent with the goal of enabling the use of the Geopriv LO on constrained devices or with limited bandwidth.

Some working group participants have expressed the view that the "Entirely External" approach would be the quickest for the working group to accomplish, and that if fully implemented in the marketplace the approach could give end users a great deal of control and flexibility in the protection of Location Information.

Other WG participants (including at least some of the authors here) have argued that the most effective way to ensure that users have some privacy control is for the LO to be able to carry a limited number of privacy rules.

It is not the purpose of this Internet-Draft to attempt to advance and defend a definitive answer to this critical question. Instead, this I-D articulates one approach to the "Limited Internal" set of privacy rules. By specifying one view of how the Limited Internal set of rules might be expressed, the Internet-Draft hopes to allow the WG to assess some detailed specifics of that option.

Note that the "Limited Internal" approach is effectively a superset of the "Entirely External" and "Bare Bones Internal" approaches, so that both of those models could be implemented in appropriate situations even if the LO can carry a larger set of rules. Thus, where a particular location service application in fact offers users robust and effective means to create and maintain an external set of privacy rules, that application could simply transmit the URI/URL of those external rules in the Location Object. But where an application lacks robust and effective external rule servers, the "Limited Internal" approach would allow a core set of rules to be carried with the LO.

Five separate things follow below. First, there is a brief and broad-brush statement of the core privacy elements that we think should be contained in a "Limited Internal" design of the Location Object. Second, there is a more precise proposal on exactly how to articulate and express these elements; significantly, this proposal combines three of the elements into one "permissions table." Third, there is an alternate proposal that adds a few additional elements to the proposed permissions table, and thereby significantly enhances the power of the LO privacy protections. Fourth, there are a few additional comments about the proposals. Fifth and last is language

in the form of a Requirement that could be inserted into a requirements document if the WG chooses the "Limited Internal" approach.

2. Conventions used in this document

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 [1].

3. Core Privacy Elements for the "Limited Internal" Approach

The following are seven elements suggested to be included in a "Limited Internal" approach to the Location Object. The first five elements (A - E) describe specific possible privacy rules. The sixth element (F) allows a reference to an external set of privacy rules if the first five rules are insufficient in scope or complexity, or if external rule storage is preferred in a given application. The final element (G) would facilitate the development of third party location and privacy-protecting services, and would permit a constrained Device to direct a Location Sighter to send Location Information to a specific destination with a specific instruction.

Note that most of the elements and rules discussed below are phrased in terms of prohibitions ("do not disclose except to . . ."), but could probably as effectively be phrased in terms of permissions ("permitted to disclosed only to . . . ").

A. Limitation on length of data retention

B. Limitation on any retransmission or further disclosure

C. Permission to disclose only to specified individual/entity

D. Permission to disclose only to someone presenting a specified key (for instance, a shared key or the private key corresponding to a particular public key), or a special type of credential (an e-token to be defined).

E. Requirement that location granularity/precision of location information be reduced

F. Requirement that external privacy rules be followed

G. Instruction that location be transmitted to specified external privacy or location service with specified instruction.

Section 6 below contains some discussion of these elements (such as, for example, a reason to articulate elements C and D separately).

4. Specific Articulation of Core Privacy Elements

The following attempts to express the above broad principles in more precise language, combining three elements into a single "permissions table":

Rule 1: (Element A) Do not retain my location information [past xyz time+date OR longer than xyz duration].

Rule 2: (Element B) Do not retransmit or further disclose my location information.

Rule 3: (Elements C, D, E) Do not retransmit or further disclose my location information EXCEPT to [abc] if he presents [xyz] credential or key, and only at [uvw] accuracy, where

[abc] allows for wildcards including "any" or "any@some-specific-domain"
[xyz] allows for wildcards and "no additional credential required beyond the [abc] identity"
[uvw] has one of the following values:

A = no granularity change required
B = 10 kilometer radius (or within lat/long quadrant)
C = 100 kilometer radius (or within larger quadrant)
D = local or municipal civil designation (e.g., city)
E = state or regional civil designation (e.g., state)
F = national designation (e.g., country)
G = time zone

These elements would appear in a permissions table:

| Location seeker | Credential | Accuracy |
| | | | |

[abc1]	[xyz1]	[uvw1]
[abc2]	[xyz2]	[uvw2]
[abc3]	[xyz3]	[uvw3]
[abc4]	[xyz4]	[uvw4]

Rule 4: (Element F) Do not retransmit or further disclose my location information except in full compliance with the privacy rules located at [url/uri].

Rule 5: (Element G) Promptly transmit my location to [abc] individual or entity, along with [xyz] instruction (where the contents of [xyz] are NOT defined by Geopriv except for technical parameters such as maximum size).

5. Possible Alternate Implementation of Proposed Rule 3

The permissions table suggested in Rule 3 above could have some additional values that would greatly increase the flexibility of the LO rules, along the following lines:

LocSeek	Credent	LocRes	TimeRes	Notif	Consent	Accuracy	Val	Policy
[abc1]	[xyz1]	r1	t1	n1	c1	[uvw1]	tt1	p1
[abc2]	[xyz2]	r2	t2	n2	c2	[uvw2]	tt2	p2
[abc3]	[xyz3]	r3	t3	n3	c3	[uvw3]	tt3	p3
[abc4]	[xyz4]	r4	t4	n4	c4	[uvw4]	tt4	p4

where

r is a Location Restriction: r represents a region where this policy applies (for instance, if I am in Munich, then it is OK to pass this information)

t is a Time Restriction (only during working hours may my boss obtain my location)

n is a "notification bit": send me a notification if you send this Location Information to Location Seeker abc

c is a "consent bit": ask me for permission in real time (and let the Location Seeker abc wait until I tell you)

tt is a "valid-until" field: this permission is valid until time tt

p is the pointer to the privacy rules/policy that the Location Seeker has to obey for this specific [abc] Location Seeker

6. Additional Discussion of Proposed Privacy Elements and Rules

The following are additional comments and explanations of the above privacy elements and rules:

a. At least Rules 1 and 2 should be expressible in both machine-readable form as well as an optional human-readable form. Rules 3 - 5 are primarily intended to be read by Location Servers that have sufficient intelligence to process the rules. But when sending Location Information to an Ultimate Location Recipient, it is possible that the Geopriv Location Object (LO) itself would need to contain some human-readable information (for example, if the LO is sent to a ULR using SMTP or HTTP). This approach is analogous to the full and compact versions of privacy policies under P3P.

b. Element B and Rule 2 could possibly be omitted as a separate flag or field, because a "do not distribute" instruction should be a fundamental default for the Geopriv Location Object. Nevertheless, there is value in having an express "do not redistribute" indicator, especially to emphasize that instruction to Ultimate Location Recipients (who, as discussed above, may well be humans receiving the LO essentially directly).

c. Elements C (disclose only to specified individual) and D (disclose only to someone presenting a key or credential) could theoretically be consolidated, because establishing the identity in C would effectively be using some form of credential. The elements, however, are expressed separately to emphasize that a Rule Maker should be able to allow access to defined individuals or groups of individuals, and ALSO to anonymous requestors who present a specified key or credential. In the proposed Rules, those two elements are consolidated into Rule 3, but the possibility of an anonymous-but-credentialed Location Seeker is preserved.

d. Obviously, the alternate proposal for Rule 3 (suggested in Section 5) is more complex, but it also would enable the Location Object to be more robust. It would also be possible to include parts of the alternate proposal without including all of the additional fields suggested.

e. Element G and Rule 5 do not themselves directly advance a privacy objective, but they would greatly facilitate the future development of privacy protecting (and other) business models. They would also promote the ability of a Target to bypass the location services offered by an Location Sighter (such as a wireless carrier) in favor of location services offered by a competitive third party.

f. To be clear, the proposal of a "Limited Internal" approach does NOT mean that all of the proposed privacy rules would be transmitted in every Location Object within a given location transaction. It is quite possible that a LO at an early stage of a location transaction (say, from a Location Sighter to a Location Server) might carry full specifics on Rules 1 - 5. But a later stage of the same location transaction (say, from the Location Server to an Ultimate Location Recipient) might only carry Rules 1 and 2 (which would be the only rules directly applicable to the ULR).

7. Draft Requirements Language for "Limited Internal" Approach

If the working group were to adopt the "Limited Internal" approach, the following is a draft requirement that could be included in the Geopriv Requirements document. The proposed elements are drawn directly from those listed in Section 3 above:

Req. 1. (Limited Policy language) Geopriv MUST specify a limited policy language capable of expressing a limited set of privacy rules concerning location information. This policy language MAY be an existing one, an adaptation of an existing one or a new policy language. The Location Object MUST include sufficient fields and data to express the limited set of privacy rules. The limited set of rules MUST include, at a minimum, the following elements:

A. Limitation on length of data retention

B. Limitation on any retransmission or further disclosure

C. Permission to disclose only to specified individual/entity

D. Permission to disclose only to someone presenting a specified key (for instance, a shared key or the private key corresponding to a particular public

key), or a special type of credential (an e-token to be defined).

E. Requirement that location granularity/precision of location information be reduced

F. Requirement that external privacy rules be followed

G. Instruction that location be transmitted to specified external privacy or location service with specified instruction.

8. Security Considerations

Security is, of course, is a core goal of the Geopriv working group. The questions addressed in this Internet-Draft -- where privacy rules should be stored and whether some or all of those rules should be transmitted with the Location Object -- have significant security implications, most directly on the security of the privacy rules themselves. The inappropriate disclosure of some privacy rules could itself harm privacy, and thus a decision to include some privacy rules in the Location Object could expose those rules to a higher chance of security (and thus privacy) violation. On the other hand, if including rules in the Location Object increases the likelihood that those privacy rules would in fact be known and followed, then the added security risk of transmitting those rules may be outweighed by the added privacy protection afforded.

9. Acknowledgements

We wish to thank Jon Peterson for his constructive criticism of the proposals advanced in the document.

10. References

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

11. Author's Addresses

John B. Morris, Jr.

Director, Internet Standards, Technology & Policy Project
Center for Democracy and Technology
1634 I Street NW, Suite 1100
Washington, DC 20006 Email: jmorris@cdt.org
USA http://www.cdt.org

Deirdre K. Mulligan
Samuelson Law, Technology and Public Policy Clinic
Boalt Hall School of Law
University of California
Berkeley, CA 94720-7 Email: dmulligan@law.berkeley.edu

Jorge R Cuellar
Siemens AG
Corporate Technology
CT IC 3
81730 Munich Email: Jorge.Cuellar@mchp.siemens.de
Germany

12. Full Copyright Statement