Internet Draft
Document: draft-cuellar-geopriv-reqs-02.txt

J. Cuellar
Siemens AG

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

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

Expires: Nov. 2002

May 2002

Geopriv requirements

Status of this Memo

Copyright Notice

Abstract

Location-based services, navigation applications, emergency services, management of equipment in the field, and other location-dependent services need geographic location information about a target (user, resource or other entity). There is a need to securely gather and transfer location information for location services, protecting the privacy of the individuals involved.

This document describes the requirements for the geopriv Location Object (used to transfer location data and perhaps some other

information) and for further IETF protocols that use this Location Object as an embedded protocol. We focus on authorization, integrity and privacy requirements.

Table of Contents

1. Overview

Location-based services (applications that require geographic location information as input) are becoming increasingly common. The collection and transfer of location information about a particular device and/or target can have privacy implications.

The ability to derive or compute a device's location, and access to the derived or computed location, are key elements of the location-based services privacy equation. Central to a target's privacy are (a) the identity of entities that have access to raw location data, derive or compute location, and/or have access to derived or computed location information, and (b) whether those entities can be trusted to know and follow the target's (or better rule-maker's) policy.

In this paper we assume that "location information" is a relatively specific way of describing where a device is located and that the location information is either (a) derived or computed from information generally not available to the general public, or (b) determined by a device that is not generally publicly addressable or accessible. For example, location information could include information calculated by triangulating on a wireless signal with respect to cell phone towers, or longitude and latitude information determined by a device with GPS (global positioning satellite) capabilities.

Excluded from the discussion below is the determination of location information wholly without the knowledge or consent of the target (or the target's network or access service provider), based on generally available information such as an IP or e-mail address. It is important to note that information like IP address can enable someone to roughly or in some instances precisely estimate a location. Commercial services exist, for example, that offer to provide rough location information based on IP address. Currently, this type of location information is typically less accurate and has a coarser granularity than the type of location information addressed in this document. This less accurate type of location computation still raises significant potential privacy and public policy concerns, but such scenarios are generally outside the scope of this document.

For the purposes of this document, "policies" or "privacy rules" are rules that regulate an entity's activities with respect to location information, including, but not limited to, the collection, use, disclosure, and retention of location information. These rules must generally comply with fair information practices. For example, see the OECD (Organization for Economic Co-operation and Development) Guidelines on the Protection of Privacy and Transporter Flows of Personal Data at http://www1.oecd.org/dsti/sti/it/secur/prod/PRIVEN.HTM. The application of these rules is described briefly in the scenarios. However, they must be fully explored in a separate document prior to creating location privacy technologies.

The main principles guiding the requirements exposed in this paper are:

1) Security of the protocol is of utmost importance to guarantee the correctness (integrity) and the confidentiality of the location information. This includes authenticating the main entities of the protocol and securing the exchanged messages.

2) A most important role is played by user-controlled policies, which describe the permissions (or consent) given by the user. The policies specify the necessary conditions that allow a Location Server to forward (transformed or filtered) location information to a Location Recipient and the conditions under which and purposes for which location information can be used. That is, using policies, the user is able to specify which

component or derived measure of the information is to be released to whom and in which granularity or accuracy. The exact form or expressiveness of policies is not further discussed in this paper.

3) Whenever possible, the location information should not be linked to the real identity of the user or a static identifier easily linked back to the real identity of the user (ie. phone number). Rather, the user is able to specify which local identifier, pseudonym, or private identifier is to be linked to the location information.

4) The user may want to hide the real identities of himself and his partners not only to eavesdroppers but also to other entities participating in the protocol.

Although complete anonymity may not be appropriate because of legal constraints or because some location services may in fact need explicit identifications, in most cases the location services only need some type of authorization information and/or perhaps anonymous identifiers of the entities in question.

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].

Note that the requirements discussed here are requirements on privacy protocols for location services. Thus the requirements sometimes refer only to the capabilities of these protocols. For example, requiring that the protocol support integrity is not the same thing as requiring that all protocol traffic be authenticated. In other cases, the requirement may be that the user always obtains a notice when his location data was not authenticated. This is clearly not just a capability of the protocol.

3. Usage Model

The following usage model will be discussed more extensively in another framework and scenarios document. We present here a summary of the terminology of the usage model for convenience.

3.1. Roles and attributes

The entities of a geopriv application or scenario may be given explicit roles:

Target:
The entity whose location is desired by the Location Seeker. In many cases the Target will be the human "user" of a Device

or an object such as a vehicle or shipping container to which the device is attached. In some instances the target will be the device itself.

Device:
The technical device the location of which is tracked as a proxy for the location of a Target. A Device might, for example, be a Global Positioning Satellite (GPS) receiver, a laptop equipped with a wireless access device, or a transmitter that emits a signal that can be tracked or located. In some situations there may be no Device, in the sense of this definition, but for instance a user is entering the location information manually.

Rule-Maker:
The individual or entity who has the authorization to set the applicable privacy rules, collectively known also as the policy. In some cases this is the user who is in possession of the Device, but is some cases it is not. For example, parents may control what happens to the location information derived from their children's cell phones. The Rule-Maker is often, but not always, the "owner" of the Device used to track location. For example, a company may own and provide a cell phone to an employee but permit him/her to set the privacy rules. Other proposed names are "Owner (of the privacy rights)" or "policy maker"

Unintended Target:
A person or object tracked by proximity to the Target. This special case most frequently occurs if the target is not a person. For example, the Target may be a rental car equipped with a GPS device, used to track car inventory. The rental company may not care about the driver's location, but the driver's privacy is implicitly affected. Working group protocols may or may not protect or affect the privacy of Unintended Targets, but the impact on Unintended Targets should be acknowledged.

Data Transporter (“DT”):
An entity or networking that receives and forwards data without processing or altering it. A Data Transporter could theoretically be involved in almost any transmission between a Device and a Location Processor, a Location Processor and a second Location Processor, or a Location Processor and a Location Seeker. Some location tracking scenarios may not involve a Data Transporter.

Location Seeker (“LS”)
An individual or entity who seeks to receive location data about a Target.

Computational Location Server (“CLServ”)
A Device or entity that computes or processes raw data to compute or derive location data, or processes location data to transform or refine the data into new location data.
<Why is this CLServ needed?>

Location Storage (“LStor”)
(. Location Server: Think of pure storage devices as disks. They matter for privacy purposes!)
A Device or entity that stores raw or location data.

Rule Repository (“RR”)
A repository that contains private or public policies, identifiers, and perhaps also requests are stored.

Attributes

An entity that who seeks to access the location data is a Location Seeker and may act in one or more of the following roles: as the Location Sighter (Location Data Source), as a Location Server, or as an Ultimate Location Recipient.

Location Sighter (LoSi), or Location Data Source
The original source of the sighting of a target in a given transaction.

Location Server (LS), or Intermediate Location Recipient:
A Device or entity that provides access to raw data or location data after processing or altering it or not. Some location tracking scenarios may not involve a Location Server.

Ultimate Location Recipient (ULR):
An individual or entity who receives location data about a Target and does not transmit the location information or information based on the Target's location (such as driving directions to or from the target) to another party distinct from the target or the Rule-Maker.

A data transporter may be an

Initial Access Provider (“IAP”):
A data transporter that provides the initial network access or other data communications services essential for the operation of communications functions of the Device or computer equipment in which the Device operates. Most commonly, an IAP will be a wireless carrier, an Internet Service Provider, or an internal corporate network, used by the Target and the Target's Device and over which location services are provided or utilized. In many cases the IAP is the location sighter. In some instances the IAP’s infrastructure may be owned and

controlled by another party who should be identified. Some location tracking scenarios may not involve any IAP.

The rules of the Target may be accessible to a Location Server in the form of Private or Public Rules Repositories:

Public Policy Repository:
A repository where signed policies, identifiers, and perhaps also requests are stored.

Private Policy Repository:
A repository of authenticated policies, identifiers, and perhaps also requests are stored, for the private use of one Location Server.

	IAP	ULR	Public RR	Private RR	Location Sighter
Target					x
Device					x
Rule Maker	x				x
Unintended Target					
Data Transporter	x				x
Location Seeker	x	x			
Location Server	x				x
Rule Repository			x	x	

3.2. Data

The main data used by the protocol is the Location Object. It contains the "sighting" information (the pair identity and location) and some other information to be determined, e.g. time information, some types of policies, authenticators, etc. (If no time information is included, this implicitly means "at the current time" or "at a very recent time".)

Sighting: the location information for a target. This is the main private data accessed by Location Servers and/or Ultimate Location Recipients. This sighting information is probably

included in the Location Object. Abstractly, it consists of two separate data fields:

(Sighting-Identifier, Location)

Sighting-Identifier is the identifier assigned to a device being sighted, and Location is the current position of a device being sighted.

Not all entities have access to exactly the same piece of sighting information. The sighting may be transformed to a new sighting pair:

(Sighting-Identifier-1, Location-1)

before it is provided by the Location Data Source or the Location Server to another Location Recipient.

Policy:
A set of rules that regulate an entity's activities with respect to location information, including the collection, use, disclosure, and retention of location information. In particular, the policy describes how location information may be used by an entity and which transformed location information may be released to which entities under which conditions. Policies contain "rules" or "assertions". Policies must be obeyed; they are not of advisory character. To make this more explicit, the term "rules" is also used instead of "policy".

Data attributes:
Filtered:
Location information that has been computationally modified.

3.3. Identification, Authentication, and Authorization

This subsection introduces some terms to be used later in the Requirements Section.

Entity-Identifier: The names used by the entities of the protocol to identify, authenticate or authorize themselves to other entities. Policies also use entity-identifiers to express which Location Seekers may receive which transformed sighting information.

The next type of identifier may not be used as an Entity-Identifier, since it can be shared by several, perhaps many, different entities:

Role identifier
("administrator", "member-of-club-A", etc.) The meaning of the role may be context dependent.

People use the word authentication with different meanings. Some people insist that authentication associates an entity with a more or less well-known identity. This basically means that if A authenticates another entity as being "B", then the label "B" has also a meaning for many entities different from A. In this case, the label "B" is called a publicly known identifier, and the authentication is "explicit":

Explicit Authentication
: The act of verifying a claimed static identity easily linked back to the real identity of the user, in the form of a pre-existing label from a predefined name space, as the sole originator of a message (message authentication) or as the end-point of a channel (entity authentication).

Authorization
: The act of determining if a particular right, such as access to some resource, can be granted to the presenter of a particular credential.

  Depending on the type of credential, authorization may imply Explicit Authentication or not.

3.4. Data Flows

Figure 1 presents the entities of a "typical" protocol setting, using the Location Object and the data flows between those entities. Not all steps discussed here necessarily occur in every scenario. The data flows may be one-step message exchanges, or multi-step sub-protocols and the actual transport of the Location Object may be done via some other transport entities not included in the diagram. The data flows to be considered by the geopriv WG, in the sense that WG will assess their authentication, authorization and privacy requirements, are the following. They are shown in Figure 1 by normal arrows ("--->")

LI (Location Information):
: the location data source sends the "full", raw location information to the location server.

FLI (Filtered Location Information):
: The location server sends filtered location information to the Location Recipient. The information is filtered in the sense that in general not the original information is being delivered, but for instance a less precise version of the information.

There is no technical reason for distinguishing Location Information from Filtered Location Information; it is just a way of insisting that the information sent by the location server is (or could be) different from the information he has received.

Pol (Policy):
The Rule-Maker(or in particular, the target itself) sends a Policy to the location server.

PolInfo (Policy Information):
the server informs the Location Seeker which data type(s) of filtered location information are available to him for a given target. This mechanism must be able to be invoked by the Location Seeker before he sends an LRequest.

LRequest (Location Information Request):
the Location Seeker requests location information for a target, a given class of targets, or for targets with a particular set of attributes. In this request, the Location Seeker may select which location information data type it prefers. The Location Seeker can also specify the need for periodic location information updates.

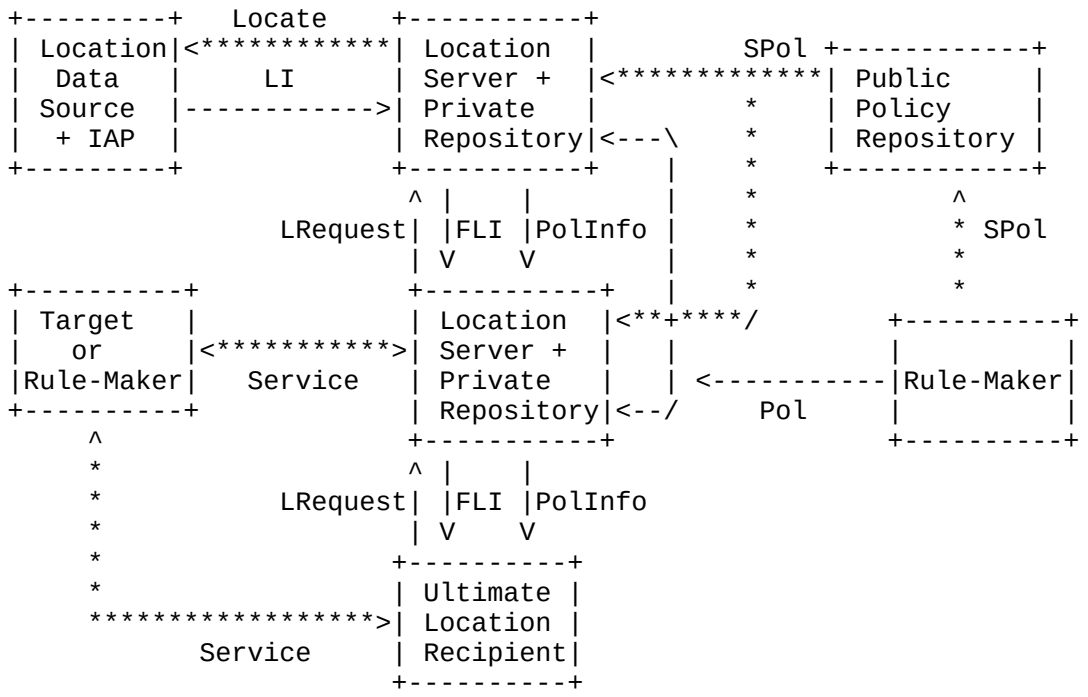


Figure 1: The Entities and Data Flows

The following Data Flows MAY be outside of the scope of the geopriv WG, but should be mentioned for understandability. They are shown in Figure 1 as while starred arrows ("***>").

Service: (Service Information, Negotiation and Delivery):
The target (or the Rule-Maker) and the client exchange information about the service and negotiate it. The client provides service delivery to the target and accounting or billing date, as necessary.

SPol (Signed Policy):
As an alternative to Pol, the Rule-Maker may write a policy and place it in the Open Repository. The entities access the repository via SPol.

Locate:
Request to locate the target. When a Location Server receives an LRequest for a target for which has no current location information, the server may send this "Locate" request to the Location Data Source.

3.4.1. Relationship framework

Location information can be used in very different environments. In some cases the participants will have longstanding relationships while in others participants may have discrete interactions.

The different relationships raise different concerns for the implementation of privacy rules, including the need to communicate privacy instructions. It is important that the Geopriv specification acknowledge the varied relationships between parties to location exchanges and set out a privacy framework suitable for each. A public rule repository for example seems to be superfluous in a trusted environment where more efficient methods of addressing privacy issues likely exist. We propose the following attributes as modifiers to a given data flow:

Trusted:
The data flow is governed by a contract that protects location privacy.

Non-trusted:
The data flow is not governed by a contract that protects location privacy.

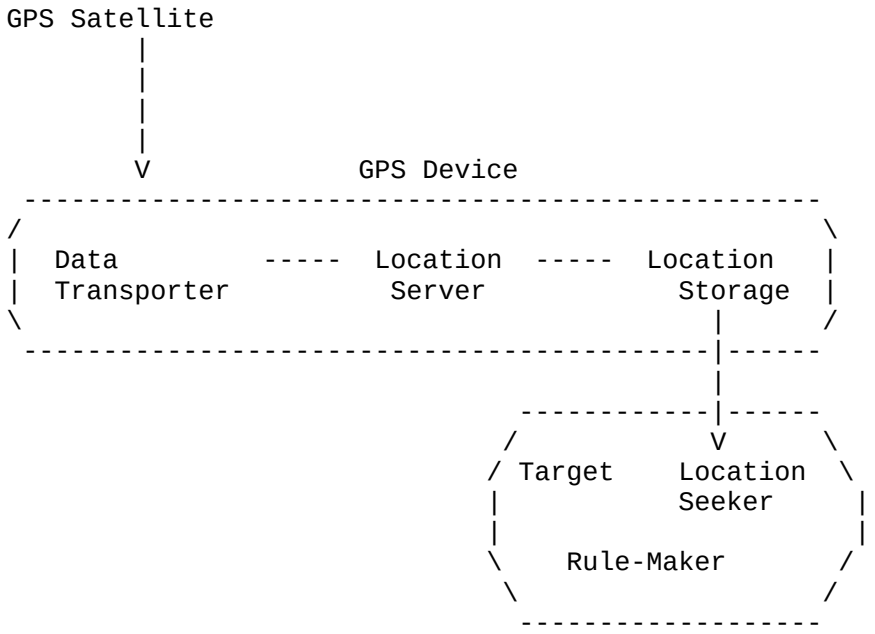
3.4.2. Scenarios of Data Flow

In this subsection we introduce two short scenarios to illustrate how these terms and attributes describe location information transactions.

SCENARIO 1: GPS Device with Internal Computing Power: Closed System

In this example, the target wishes to know his/her location using Global Positioning System (GPS) and the device is capable of independently processing the raw data to determine its location. The

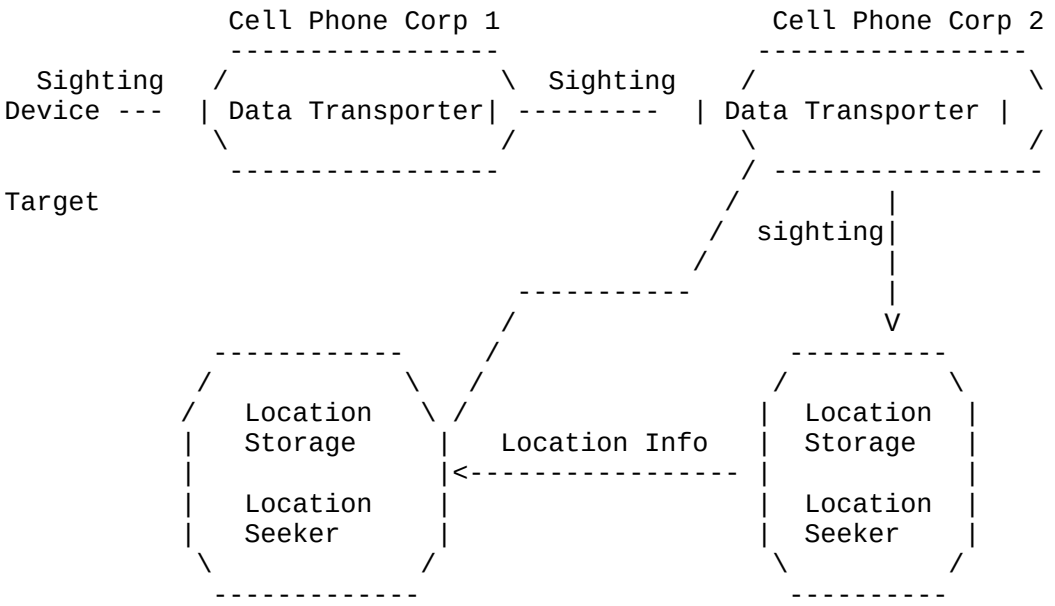
location is derived as follows: the device receives transmissions from the GPS satellites, internally computes and displays location. This is a closed system. For the purpose of this and subsequent examples, it is assumed that the GPS satellite broadcasts information, and has no capacity to record the identity or whereabouts of devices using the signal.



In this scenario the GPS device is both the IAP and the LoSi. The interaction occurs in a Trusted environment because it occurs in the rulemaker's device.

SCENARIO 2: Cell Phone Roaming: Cell Phone Company Outsourced Billing and IT

In this example, a cell phone is used outside its home service area (roaming). Also, the cell phone service provider (cell phone Corp 2) outsourced the billing of cell phone usage. The cell phone is not GPS-enabled. Location is derived by the cell phone network in which the target and device are roaming. When the target wishes to use the cell phone, cell phone Corp 1 (IAP) provides the roaming service for the target, which sends the raw data about usage (e.g. duration of call, location ú roaming network, etc.) to cell phone Corp 2, the home service provider. Cell phone Corp 2 submits the raw data to the billing company which processes the raw data for the billing statements. Finally, the raw data is sent to a data warehouse where the raw data is stored in a location server (e.g. computer server).



Here cell phone corp 1 is the IAP and the LoSi. Cell phone corp 1 could be Non-trusted (the rulemaker does not have a contract protecting location information with corp 1 and there is no contractual relationship with privacy provisions between corp 1 and corp 2) or Trusted (contract with privacy protections between cell phone corp 2 and corp 1). Cell phone corp 2 is Trusted.

3.5. Further explanations

<Note: This section is unnecessarily long! Most of text will be removed afterwards, but it may be useful in the discussions. The contents of this subsection may be out of the scope of the work of the working group. They are presented here to facilitate the understanding, present some possible examples, or suggest why some requirements are feasible.>

3.5.1. Location Data Types

Two apparently different data types may contain the same information if it is possible to transform one data type into the other and vice-versa without information loss.

One location data type DT1 may contain more location information than another DT2 in at least two different senses:

- DT1 may have the same dimensions as DT2 has, plus some extra ones. (For instance, DT1 contains velocity, while DT2 does not).

- DT1 may be more accurate than DT2.

In general, if DT1 has more information than DT2, then there is one a function that "translates correctly" from DT1 to DT2. There are other types of transformations that introduce errors (obfuscation: intentionally make the location values less accurate by adding randomness). During a transformation, information can be lost, but not gained. Of course, a transformation that merges information from several sources clearly increases the information of each one. Thus a transformation is a filtering of information. For instance there are transformation functions from both data types "(latitude, longitude, altitude)" and "(country, state, province, city)" to the data types "(country, state)" and "time zone", but not vice-versa.

Notice that if the space regions determined by different location values of DT2 do not overlap, then there is at most one transformation from DT1 to DT2. If the space regions of DT2 overlap, then usually there is some choice, which can be given by a (pseudo-) random function.

If DT1 does not have more information than DT2, then there is no function that "translates correctly" from DT1 to DT2. In other words: there are many functions that translate from DT1 to DT2, but all introduce some degree of error. We believe that this kind of functions should be avoided.

3.5.2. Public Global Identities

If A has some information about a public global identifier "ID" and A discloses this information to B, then B may associate this information with the same entity as A did. In this way, B may accumulate information about the entity labeled by "ID".

A public identity is a well-known label that identifies an entity for a (rather large) group of entities.

A public identity may be the subscription identity at the home domain (if applicable), a well-known identity (name, address or Tel Number), etc.

An entity may regard the disclosure of his public identity (in connection with some activity of him, his location or other attribute) as a violation of his privacy right.

3.5.3. Authorization without Explicit Authentication

In order to remain anonymous, an entity may use private identifiers. Private identifiers convey less information than public identities, because they are meaningful to a smaller number of entities and in use for a shorter duration. Thus if A discloses a private identifier

to B, B is less likely to associate this information with a known individual or entity than if a public identifier was disclosed.

Short-lived identifier
an identifier that is used only for one or a limited number of "sessions".

Short-lived identifiers may be used to anonymously authenticate entities in some settings.

In many situations, including pre-paid services, token-based or role-based authorizations, unauthenticated key agreement, and purpose-based identifiers, there is no need for explicit authentication.

Using weaker forms of authentication, the communication partner may still want to make sure that he is communicating to the same entity during the whole session, or that he is communicating with an authorized entity. Thus message authentication codes are used, based on "unauthenticated keys".

Authorization credentials may be used in the same way as authentication credentials to secure a key agreement in the following sense: one party is assured that no other party aside from the owner of the authorization credentials (and possibly additional identified trusted parties) may gain access to the agreed secret key. The resulting keys are called authorized keys. Those keys may be used for message authentication, without implying an explicit authentication.

In real life this corresponds for instance to the following situation: at a cloakroom a person deposits his coat and receives a credential that he may use later to obtain back the coat.

One possible goal of the Rule-Maker is to hide the identity of the Location Recipient to the Location Server. Nevertheless, the Location Server has to be sure that the Rule-Maker has authorized the Recipient to access the location. This is a case of authorization without explicit authentication: the Location Server has to be sure that the Location Recipient is a particular (i.e., authorized) communication partner of the Rule-Maker.

This may be done for instance as follows: consider a Location Seeker that obtains a set of "traveller's cheques" from the Rule-Maker. The cheques will be used to "buy" location information from a Location Service. Initially, the Location Seeker signs for a first time the cheques with any "signature" that he wants to use. The Rule-Maker, through his own signature, authorizes the signature of the Location Seeker. When presented to the Location Server, the cheques may be countersigned so that the server is sure that the signer is the same as the one who was authorized by the Rule-Maker. This countersignature does not only authenticate the Location Seeker to the verifier, but also indirectly to the Rule-Maker, when the cheque

is later presented to him. Incidentally, the Rule-Maker may achieve full information about who has accessed to his location information.

To hide the real identity of the Rule-Maker to the Location Server, the following dual solution can be used. The Rule-Maker buys (say, using e-cash) a service from a Location Seeker (e.g. a navigation service). During this transaction, the Location Seeker and the Rule-Maker agree on one or several pseudonyms and a set of "traveller's cheques" that the target may use later to authenticate himself to the server and thus indirectly also to the Location Seeker.
Since e-cash protocols may be also anonymous, this may be used to hide simultaneously,

- the identity of the target from the Location Server,
- the identity of the Location Seeker from the Location Server,
- the identity of the target from the Location Seeker.

But notice that the Location Data Source is in general not able to localize the target based on some short-lived identifier. In this scenario, the Location Data Source should be a Location Server, a different one from the one from whom the identity of the target is to be hidden.

4. Requirements

4.1. Protocols

Req. 1. The geopriv protocol MUST be an embedded protocol: it defines a Location Object, together with the security mechanisms used to secure it. The security mechanisms are of two types: on one hand the Location Object as such is secured, using cryptographic checksums or encryption as part of the Location Object itself, and on the other hand security mechanisms may be provided by the embedding transport protocol that uses the Location Object. If possible, security mechanisms on the Location Object itself are to be preferred.

We refer to the embedded protocol also as the geopriv protocol and to the combination of both the embedded protocol and the transport protocol as the combined protocol.

4.2. Policy based Location Data transfer

Req. 2. The decision of a Location Server to provide a Location Seeker access to location information is based on user-defined privacy policies.

Req. 3. The Location Data Source may be unaware of the full policies defined by the Rule-Maker, but in that case it

will have to obey another set of "generic" policies, consented to by the Rule-Maker, to transfer Location Data (raw or not) to another entity.

Req. 4. An Ultimate Location Recipient does not need to be aware of the full policies defined by the Rule-Maker, but it will obey a set of policies regarding the use and retention of the location information.

4.3. Location Object, Location Data

Req. 5. The embedded protocol MUST define one Location Object (both in syntax and semantics) that must be supported by all geopriv entities. Some fields of the Location Object MAY be opaque to the embedded protocol.

Req. 6. The Location Object MAY define at least one Location Data Type (both syntax and semantics) that must be supported by all geopriv entities, or the Location Data field(s) of the Location Object MAY be opaque. The Location Object MAY define at least one Location Data Type

When transmitting location information, (LI and FLI in Figure 1), the sender and the receiver must agree on the data type of the location information. The combined protocol may specify that the data type information is part of the Location Object or that sender and receiver have agreed on it before the actual data transfer. Thus

Req. 7. The Location Object MAY contain a field for the data type of the Location Data. This field MAY also be opaque.

4.4. Policies

Req. 8. The Location Object MAY contain a field for policies that may be passed to the location server or may be stored in a public (open) repository.

Req. 9. The Location Object MAY contain a field for identifiers that may be passed to the location server or may be stored in a public (open) repository.

Req. 10. The Location Object MAY contain a field for requests from the clients.

Req. 11. The combined protocol MAY specify a policy language. This policy language MAY be an existing one, an adaptation of an existing one or a new policy language.

If specified, the policy language MUST be strong enough to express policies of the form: a group G of clients are allowed to know a certain transformation A of the location

L of a target together with a given identifier I of the target for a given purpose, for a given period of time.

If specified, the policy language MUST be strong enough to express conditions on G and A as follows:
G, the group of clients SHOULD be characterized by the possession of (identifiers, credentials) with a certain syntactic property.
A, the transformation function MAY be specified by data type of the expected filtered location information.

Within those constraints, the policy language SHOULD be as simple as possible, or it SHOULD be an existing policy language.

4.5. Identity Protection

Req. 12. When a location server accepts a policy that uses a role identifier, the Rule-Maker MUST prove the ownership of the claimed role identifier. This is a property of the combined protocol.

Req. 13. The combined protocol MUST be able to hide the real identity and static identifiers association with the real identity of the Rule-Maker, the target, and the device from the Ultimate Location Recipient.

This may be easily done using short-lived or role identifiers.

Req. 14. The combined protocol MUST be able to hide the real identity of the Location Recipient to the Location Server.

<Give an example where hiding the identity of the Location Recipient is what should be required: The target is not concerned about the Server identifying him and knowing his location, but identifying his business partners, and therefore habits, etc.>

Req. 15. The combined protocol MUST be able to hide the real identity of the Rule-Maker to a Location Seeker, including a Location Server.

4.6. Authentication Requirements

Req. 16. The combined protocol MUST allow different authentication schemes. The combined protocol MUST guarantee that appropriate keys (shared or asymmetric) are generated and available to secure the Location Object within the embedded protocol.

Req. 17. The combined protocol MUST allow authorization without explicit authentication.

4.7. Actions to be secured

Req. 18. The embedded protocol MUST be able to secure the Location Object for the following message flows (mutual end-point authentication, data object integrity, data object confidentiality, replay protection, in the absence of a time parameter): LI, Pol, LIF, LRequest, and PolInfo.

Req. 19. The embedded protocol MUST specify a minimum mandatory to implement Location Object security including mandatory to implement crypto transforms.

Req. 20. The embedding protocol MAY provide extra security for these flows (hop-by-hop or end-to-end).

In full details, these requirements have many consequences: the communicating parties MUST have security relationships between them, allowing them to construct secure channels between them. This may imply that some scenarios should not be permitted in general. The Rule-Maker MAY choose to use the security provided by the embedded or by the embedding protocol, or none.

Req. 21. When a Location Server accepts a policy from the Rule-Maker, the target MUST prove to the combined protocol that he owns the claimed group or role identifier that should be passed to the Location Recipient.

(For instance, if a Target wants the role identifier "medical doctor" to be passed to a Location Recipient, the Target must prove the claims to be a medical doctor.)

Req. 22. The "generic" policies (as opposed to the policies created by the Rule-Maker) used by the Location Data Source, by the Ultimate Location Recipients and by the Location Server of some special scenarios to be discussed yet MUST be made explicit.

5. Security Considerations

The purpose of the geopriv protocol is to allow a policy-controlled disclosure of location information for location services. Only the information carried within the Location Object is secured in a way compliant with the privacy and security policies of the target. This does not mean that geopriv secures the target against general traffic analysis attacks or other forms of privacy violations.

The Location Server is assumed to be trustworthy.

6. References

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

7. Author's Addresses

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

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

8. Full Copyright Statement