Requirements draft Issues

Geopriv: Geographic Location Privacy

draft-ietf-geopriv-reqs-01.txt

Nov 18, 2002

Jorge.Cuellar@siemens.com

Key questions:

- Open issues that are not *protocol* open issues
- Any requirements missing from draft?
- Ready for WGLC?

Jorge.Cuellar@siemens.com

Issue 25: „Emergency Call Authentication“: a) Closed

- Req. 14.3) The protocol SHOULD allow a bypass if authentication fails in an emergency call.

- The issue addressed in the last point is that an emergency call in some very unfavorable situations my not be completed if the minimal authentication fails. This is probably not what the user would like to see. The user may prefer an unauthenticated call to an unauthenticated emergency server than no call completion at all, even at the risk that he is talking to an attacker or that his information is not secured.

Jorge.Cuellar@siemens.com

Issue 25: „Emergency Call Authentication“: b) Open

- Making an emergency call on a VoIP phone which is not "logged in".
  In the mobile world, you have to be able to make a call to emergency services even if the phone is not authorized (i.e. it has no service agreement).
- Problem: if the user may not authenticate itself, whose policy to use?
  A default one: this loc information can only be sent to an emergency center.
- Problem: If additionally the emergency center is not authenticable?

Jorge.Cuellar@siemens.com

Issue 13: „LO fields“: Closed

- What are the contents (fields/attributes) of the Location Object? (This is a "MUST implement", not all location objects have to contain all fields)

1 Target Identifier

2 Location Recipient Identity

May be multicast or group identity

3 Location Recipient Credential

4 Proof-of-Possession of the Credential

5 (One or more*) Location Field(s) each containing one or more Location Representations, which can be in different formats.

*Issue 15: Out of scope: For privacy reasons, there is no need for multiple locations

Jorge.Cuellar@siemens.com

Issue 13: „LO fields“: Closed

6 Location Data Type
Formats for both lat/long/altitude and "civil" locations

7 Motion and direction vectors

8 Timing information:
a When was the LI accurate? (sighting time)
b Until when considered current? TTL (Time-to-live)

9 Policy Field (See also Issue 17)
MAY be a pointer, e.g. an URI, to a full policy
or it MAY contain a Limited Policy
or both

10 Security-headers and -trailers, e.g. encryption information, hashes, or signatures

11 Version number

Jorge.Cuellar@siemens.com

Issue 17: (Limited) Policy Language" or "Core Set“: Closed

- Do we want to define a simple policy language?

- Yes, but it may be very simple:

  MAY be simply: "delete-by *date*„

  In the Draft replace the text: „The Location Object should be able to carry a limited but core set of privacy policies. This core set is defined below and discussed more extensively in a separate document. Beyond the core set of privacy policies, the user or Rule Maker should be able to define a more robust and complex set of policies. „

  By:

  „The Location Object should be able to carry a limited but core set of privacy policies. The exact form or expressiveness of policies in the core set or in the full set is not further discussed in this paper, but is discussed more extensively in a separate document.“

Jorge.Cuellar@siemens.com

Issue 29: „Full Policy“: Out of scope

- Do we want to define a full policy language?
- Perhaps.
- Note: It is outside of our scope how Privacy Policies are managed, how a Location Server has access to the Privacy Policies, and if he is or not aware of the full set of rules desired by the Rule-Maker. Note that it might be that some rules contain private information not intended for untrusted parties.

Jorge.Cuellar@siemens.com

Issue 15: „ Multiple locations issue“: Out of scope

- Is it necessary for the geopriv object(s) to be able to carry multiple locations for the target?

- Out of scope: For privacy reasons, there is no need for multiple locations

Jorge.Cuellar@siemens.com

Issue 8b: „Accuracy flag„: Closed

- It is not useful to provide an accuracy attribute in object, i.e., a flag saying "I'm not telling you the whole truth.„
- But: if the LO is used for requesting a position, an accuracy level may be *requested.*
- This is an open *protocol issue*: out of scope for this document.

Jorge.Cuellar@siemens.com

Issue 20: „Who defines the Identities (ID Mngt)“ Out of scope

- Out of scope, see draft Section 9.7
- May the using protocol define the Identifiers or must the using protocol use and authenticate Pseudonyms proposed by the policies, chosen independently of the using protocol?
- Of course, if the using protocol has an appropriate namespace, containing many unused names that may be used as pseudonyms and may be replaced by new ones regularly, then the Location Object may be able to use the name space.
- For this purpose, the user would probably have to write his policies using this name space.
- Note that it is necessary to change the used pseudonyms regularly, because identifying the user behind an unlinked pseudonym can be very simple.

Jorge.Cuellar@siemens.com

Issue 16: "Full integrity issue“: Closed

- Is there a provision in the protocol to prohibit the users to send false location information?
- SHOULD the protocol support transformations that introduce errors?
- Both: No. There are no such requirements.
- For more discussion, see „draft-morris-geopriv-location-object-issues-00.txt“

Jorge.Cuellar@siemens.com

Issue 27 („Single packet exchange“): Out of scope

- Tracking a small object has several implications:
  1. small device
  2. delta format
  3. The "geopriv protocol" needs to be at most a single packet exchange. The first transaction in a tracking application could be more than this, but we need a low overhead mechanism for incremental updates
- Only 2 is now a requirement, but all should be possible.

Jorge.Cuellar@siemens.com

Issues 18, 19: “Generic policies“ (used by LoSi)

- Location Sighters (LoSi) and Ultimate Location Recipient (ULR) need in general no full rule-maker defined policies?

- Req. 7. (LoSi Policies) Even if a Location Sighter is unaware of and lacks access to the full Privacy Policies defined by the Rule Maker, the Location Sighter MUST transmit Location Information in compliance with instructions set by the Rule Maker. Such compliance MAY be accomplished by the Location Sighter transmitting LI only to a URI designated by the Rule Maker.

Jorge.Cuellar@siemens.com

Issues 18, 19: “Generic policies“ (used by ULR)

- Location Sighters (LoSi) and Ultimate Location Recipient (ULR) need in general no full rule-maker defined policies?

- Req. 8. (ULR Policies) An Ultimate Location Recipient does not need to be aware of the full policies defined by the Rule Maker (because an ULR SHOULD NOT retransmit Location Information), and thus an ULR SHOULD receive only the subset of Privacy Policies necessary for the ULR to handle the LI in compliance with the full Privacy Policies (such as, for example, an instruction on the time period for which then LI can be retained).

Jorge.Cuellar@siemens.com

Issue 28 (Multicast Issue): Closed

- Include the location object in multicast-based using protocols.
- Yes

Jorge.Cuellar@siemens.com

Issues 21, 22: „Group or role identifiers issue“: Out of scope

- Will the protocol support Role identifiers (like "administrator", "member-of-club-A", etc.)
- Also with context dependent meaning?

- Identities may be used to represent groups or multicast, but this is outside of our scope.

- Group or role identifiers are probably not somehow explicitly supported (in V. 1)

Jorge.Cuellar@siemens.com

Issue 14: „Implementation of a Location Format“: Closed

- Location Data Formats?
- The embedded protocol MUST define data type format for location data that must be supported by all geopriv receivers.
- But not all geopriv Location Objects have to contain data in this format.

Jorge.Cuellar@siemens.com

Issue 26: „ Security Features“: closed

- Req. 13. The Location Object MUST support fields suitable for protecting the Object to provide the following security features:
  - Mutual end-point authentication
  - Data object integrity
  - Data object confidentiality
  - Replay protection

Jorge.Cuellar@siemens.com

Issue 23: “Disallow anonymous location-requests“: Closed

- Need requirement:
  if location recipients decline revealing their identity,
  ==> this must be a designated type of identity,
  allowing the policy to prohibit anonymous location-getting.

- This is not a requirement

Jorge.Cuellar@siemens.com

Issue 24 b): „Law enforcement issue“: Closed

- Law enforcement policies are not under user-control

Jorge.Cuellar@siemens.com