HELD Identity
Update, Open (and Closed) Issues

draft-ietf-geopriv-held-identity-extensions-01

James Winterbottom, Martin Thomson, Hannes Tschofenig, Richard Barnes

Progress since -00

- Two issues raised, closed for -01
- Security review posted:
  - http://www.ietf.org/mail-archive/web/geopriv/current/msg08064.html
- Two open questions
  - Need WG input

Issue #19

- Changes to security and privacy sections
  - See issue, http://www.ietf.org/mail-archive/web/geopriv/current/msg08017.html
- Summary:
  - Two types of request: LCP(-like), and authorized third party
  - For an LCP, return routability is sufficient for authentication; using identity for the same (or similar) task requires at least the same level of assurance
  - Policy needs to identify authorized recipients…
  - …and how they are authenticated

Issue #27

- Note on application of policy when a subjective identifier is used
- Proposed text:

  Authorization policy can be affected by a subjective network view if it is applied based on an identifier, or it's application depends on identifiers. The subjective view presented to the LIS and Rule Maker need to agree for the two entities to understand policy on the same terms.

  For instance, it is possible that the LIS could apply the incorrect authorization policy if it selects the policy using a subjective identifier. Alternatively, it may use the correct policy but apply it incorrectly if subjective identifiers are used.

Solution Scope

- The following questions were raised in relation to providing examples of identifier usage:
  - How does the 3rd party get this non-IP identifier?
  - How does the LIS differentiate 3rd-party and LCP requests?
  - How does the LIS authenticate LCP requests?
- These are valid questions, but this document does not need to answer them
  - Caveat: examples may demonstrate how the principles already outlined in the document might be applied
- Proposal: place these out of scope

Solution Scope (Proposed Text)

- Add to Section 1.1:

  This document does not describe how a requester acquires an identifier for a Device.

  This document does not describe how a requester is authenticated by a LIS. For a Device requesting its own location, the method depends on the nature of the access network; a set of privacy and security principles are described, upon which any method can be judged. Establishing authorization for a third-party requester is expected to depend on specifying how that requester authenticates with the LIS.

- Add to Section 5.1:

  Unless the LIS is able to prove that the identifier used by a requester uniquely identifies that requester, it MUST assume that the request is a third-party request.

Need Examples

- Idea: Provide an example to demonstrate how the principles in the document are applied
- ISSUE: no agreement on what principles these examples need to demonstrate

Alphabet soup

- The only comment from the SECDIR review was that the document was a little heavy on the acronyms.
- Proposal: not possible to address completely, but a few editorial changes can help
  - i.e. expand acronyms more often
- Include in next update

!

- Update to -02 with proposed changes shortly
- Is this ready for WGLC?
- If so, what comes after this?
  - There are still three gaps in the solution:
    - draft-winterbottom-geopriv-deref-protocol
    - draft-thomson-geopriv-held-measurements
    - draft-thomson-geopriv-res-gw-lis-discovery