draft-barnes-geopriv-lo-sec-05

IETF 74

Motivations

- W3C Geolocation WG poses serious threat to Geopriv and its long-term success
- In pushing Geopriv at W3C, we encountered perceptions that:
  - Geopriv was not aimed at the Web
  - Geopriv was hard to understand
- Goal of revised approach to documents:
  - Provide easier intro to Geopriv
  - Address issues, tensions that developed over time

Overview

1. Introduction
   - Creative Commons and classification systems as existing examples of binding data to policy
   - Location-specific privacy risks: comprehensiveness, sensitive destinations, stalking, government access
   - Departure from current privacy paradigm
2. Architecture overview
   - Basic entities: Target, RM, LG, LS, LR
   - Formats: Privacy Rule, Location Object
   - Protocols (later)

Overview

3. Location life-cycle: generalizing privacy and security considerations for protocol interactions in each phase
   – Positioning: LG determines Target's location
   – Distribution: LS sends location from one LS to another
   – Receipt: LR receives location and uses it
4. Security considerations from lo-sec-04
5. Example scenarios
   – 2 Web-based, emergency calling, combination
6. Glossary: attempt to unify terms

Additions and clarifications (?)

- Access control rules vs. usage rules
  - Access control: describe which entities are authorized to receive location
  - Usage: describe what uses of location are authorized
- Protocols
  - Positioning: LG/Target exchange to determine Target's location
  - Rules: used by RM to send Rules to LS
  - Conveyance: used by LS to send LO
- Local Rules vs. Forwarded Rules
- LSa / LSi distinction
  - Authorized LS (LSa): Rules from RM or LO
  - Independent LS (LSi): Rules from LO only

Proposed further changes

- Better integrate security considerations from lo-sec-04
- Discuss the role of identity/pseudonyms
- Clarify that at the end of Positioning the LG knows the location of the Target and that depending on use case the LG may be the Target
- Call out the special case of LCPs in their own section and confine the discussion of LCPs to that section
- Limit example rules to things that are expressible by Common Policy and Geopriv Policy
- Add a quick intro to privacy rules in section 1

Outstanding issues

- If LG <> LS, is LG’s relationship with LS(es) constrained at all?
  - Need to clarify usage of “LG,” “LS-init,” "first LS," and “LS.”
- Do LOs exist as part of the Positioning phase or not?
- Is idea of an LR as an "ultimate" endpoint impractical?
- Is there utility in classifying protocols and giving them labels?
  - What should labels be? Which labels apply to which existing protocols?
- Are life-cycle labels right? Is "Use" better than "Receipt?" Is "Acquisition" better than "Positioning?”
- Is there utility in distinguishing Local Rules from Forwarded Rules? Are Forwarded Rules better named "Sticky Rules?”
- Should we be using 2119 language?

Outstanding issues

- Others from the WG?