draft-barnes-geopriv-lo-sec-02

Richard Barnes
Matt Lepinski
Hannes Tschofenig
Henning Schulzrinne

IETF 71
Philadelphia, PA, USA

Agenda

- Motivation / context
- Location dissemination architecture
- Security requirements
- Questions for the WG

Motivation / Prior work

- RFC 3693 & 3694
  - Address **privacy** concerns in the context of **presence**-based location dissemination
- draft-ietf-geopriv-l7-lcp-ps
  - Design team realized that there are security risks not covered by RFC 3693/3694
  - These concerns were the starting point for this document

Goals

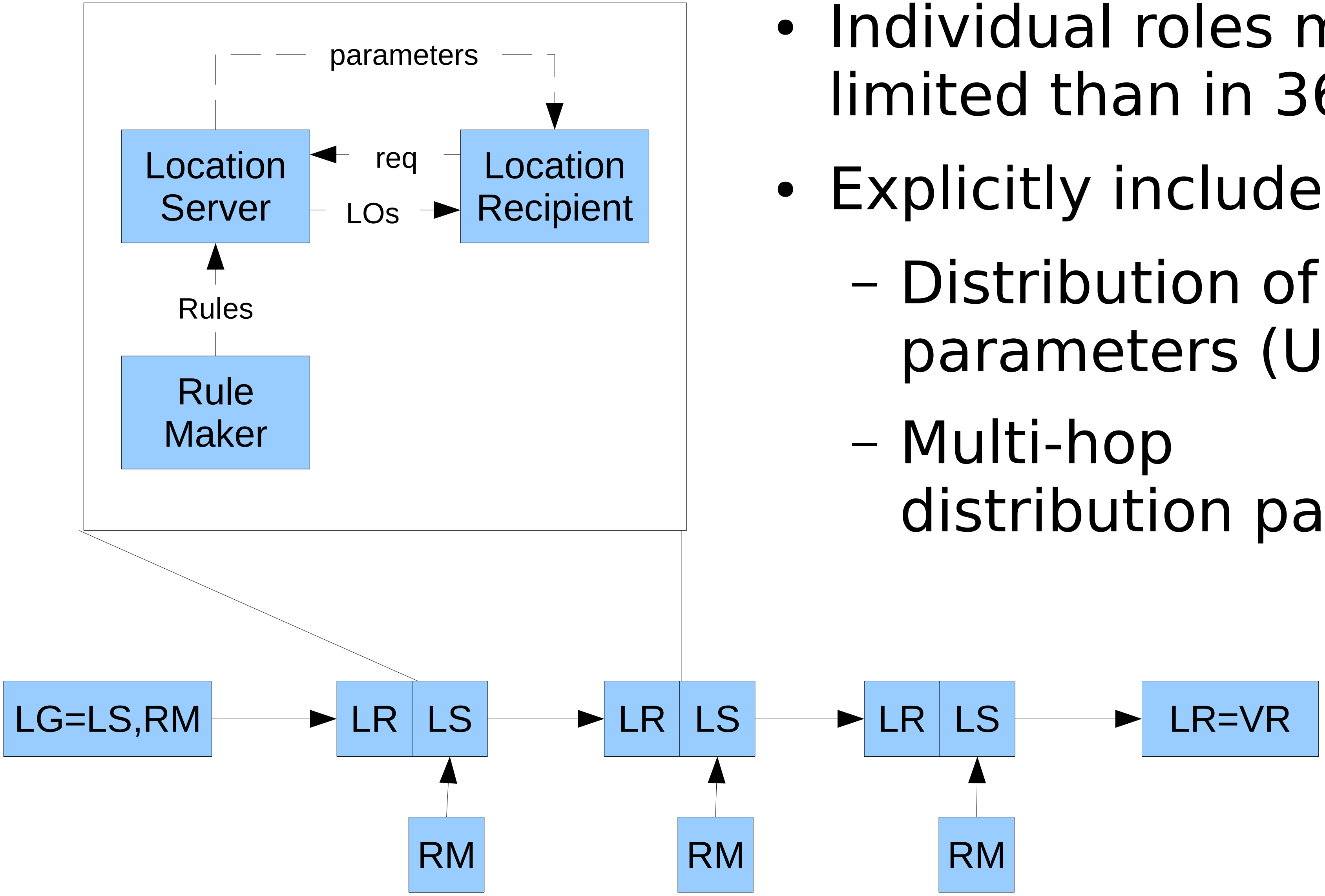
- Define a more general architecture for policy-based location dissemination
  - Include end-to-end and end-to-middle scenarios as well as single hop
  - Include non-presence protocols
    - DHCP, LLDP-MED, HELD, RADIUS-LO, etc.
  - Generalize policy model to be applicable outside of presence scenario
- Requirements for security features in constituent protocols
- Guidelines for setting distribution policy

Concept for how to use this

- This document could be a “check-list” for protocols used to communicate location
- This document a list of “assurances” along with security features required for each
- Future protocols can satisfy requirements by either
  - Providing the security features to provide each assurance
  - Stating which assurances they do not provide

Location Distribution Architecture

- Individual roles more limited than in 3693
- Explicitly includes:
  - Distribution of parameters (URIs)
  - Multi-hop distribution paths



parameters

Location Server

req

LOs

Location Recipient

Rules

Rule Maker

LG=LS,RM

LR

LS

LR

LS

LR

LS

LR=VR

RM

RM

RM

Roles and Assurances

- Within a transaction:
  - RM: Rules are installed correctly and followed
  - LS: LOs are transmitted according to policy
  - LR: LO is faithfully transmitted from the proper LS
- End-to-end:
  - LG: LO is accessible only to authorized VRs
  - VR: LO is trustworthy, e.g., originating from a trusted source
- Target acts as one or more of the above

Security Requirements

- Provides requirements for
  - Location Conveyance Protocols (LS->LR)
  - Rule Conveyance Protocols (RM->LS)
  - LO formats (multi-hop)
  - Standard protections: Confidentiality, authenticity, integrity
- Makes recommendations for LS policy
  - Access control policies
  - Usage of opaque/random references

Security Requirements

- Requirements are grouped by assurances
  - For example, to ensure that an LS can transmit an LO only to authorized LRs, a Location Conveyance Protocol needs
    - Authentication of the LR to the LS
    - Confidentiality protection of LO
- Concept is that a candidate protocol will satisfy this document by doing one of two things
  - Explain how it provides the listed features
  - Explain why it doesn't provide an assurance

Questions

- Is this approach helpful? Does it provide meaningful security guidance?
  - Does architecture reflect reality? Enough?
  - Does the usage concept for requirements make sense?
- Should this document be adopted as a working group item?