GeneRic Autonomic Signaling Protocol
draft-ietf-anima-grasp-01

Brian Carpenter (editor)
Bing Liu (editor)
Carsten Bormann

IETF 94
November 2015
Topics

- Changes since draft-carpenter-anima-gdn-protocol-04
- Open issues
- Discussion, next steps
Changes

• draft-ietf-anima-grasp-00:
  – Changed protocol name
  – Added URL locator type

• draft-ietf-anima-grasp-01:
  – Updated requirements
  – Changed from TLV to CBOR format - many detailed changes, added co-author
  – Tightened up loop count and timeouts
  – Noted that GRASP does not provide transactional integrity
  – Various clarifications and editorial fixes
Change to CBOR (1)

• Required reading:
  – Concise Binary Object Representation [RFC7049]
  – CBOR data definition language (CDDDL) [draft-greevenbosch-appsawg-cbor-cdddl]
Change to CBOR (2)

- Old TLV description of discovery message:
Change to CBOR (3)

- New CBOR description in CDDL:
  
  discovery-message =
  
    [M_DISCOVERY, session-id, objective]
  
  M_DISCOVERY = ; a defined constant
  session-id = 0..16777215
  objective /= ; defined below

- Easy to represent in programming languages and to extend or modify.
- Essentially no change in payload size.
Change to CBOR (4)

• Objective description in CDDL:

    objective /= generic-obj
    generic-obj = [objective-name, objective-flags, loop-count, ?any]
    objective /= vendor-obj
    vendor-obj = [{"PEN":pen}, objective-name, objective-flags, loop-count, ?any]
Open Issues (discovery)

• (No.18) How to handle multiple discovery responses?
  – E.g. GRASP choose by default/random
  – E.g. expose list of responses to ASA; ASA decides according to some criteria

• (24) Do we need "fast withdrawal" of discovery responses?
  – Situation differs: some response might be valid permanently; some might be imperial
  – Consider add TTL for the Response cache?

• (new*) Clarify if/when discovery needs to be repeated.
  – E.g. no response within a certain time (say, 1 min)

• (30) Random delay in discovery responses to mitigate amplification attacks?

* new issues will be numbered in next draft
Open Issues (security)

• (new) Mandatory for running in ACP?
  – Really a challenge to do security without ACP
  – But ACP also needs signalling

• (27) Security of link-local multicasts (Unsolicited Response).
  – If GRASP runs in ACP, no worry about this
  – If not in ACP, then need to handle the authentication and authorization of the flooded information

• (new) Expand discussion of security boundary when running with no ACP.
  – Might rely on the local PKI infrastructure

• (new) State that role-based authorization of ASAs is out of scope for GRASP.
  – GRASP doesn't recognize/handle any “roles”
Open Issues (general 1)

• (29) Private Enterprise Number (PEN) is used to distinguish vendor options. Would a domain name be better?
  – PEN might not make sense for autonomic networking?
  – Domain name might be more beneficial. E.g. for authentication/authorization processing?

• (new) Reconsider CBOR definition for PEN syntax

• (31) Anything else needed for sleeping nodes?
  – Already specified repeats for failed discovery etc.
  – Force to do Sync when awake from sleeping?

• (new) Are URL locators really needed?
  – Renumbering considerations prefer URL
Open Issues (general 2)

• (new) Is Session ID sufficient to identify relayed responses?
  – Isn’t the originator’s address needed too?
• (new) Clarify that a node will contain one GRASP instance supporting multiple ASAs
• (new) Add a “reason” code to the reject option?
  – E.g. “requirement not fulfilled”
  – Might be useful for human auditing/analysis?
• (new) Do we need selective flooding to a subset of nodes? (see draft-liu-anima-grasp-distribution)
  – E.g. flood to nodes support a certain objective
  – E.g. flood to nodes belongs to a specific role or hierarchy
Discussion + next steps

- Next version will settle as many of the open issues as possible.
  - Almost all the “new” issues came from one excellent review by Joel Halpern
- We need more reviews of the draft.
- We need people to think about implementation issues.