draft-irtf-icnrg-ccnxsemantics-07 draft-irtf-icnrg-ccnxmessages-07 Draft Updates

Marc Mosko

ICNRG @ IETF 101, London

March 20, 2018

Draft Updates & Issues

- We received feedback from IRSG on the semantics -06 Experimental
  - The Security Considerations section needs significant re-write
  - The document did not confirm to IRTF guidelines in regards to certain markings about the document origin, RG consensus around the document, and implementation maturity.
  - 3 structural comments that the draft (semantics) was abrupt and did not provide any background or context for the reader. It also did not cite existing ICNRG RFCs where appropriate.
  - 10 technical comments on style, spelling, or technical content.
- No feedback on the messages draft
  - But many of the above comments apply directly to the messages draft.

Technical Changes

- There are no protocol or encoding changes.

Section	Semantics	Messages
Abstract	Minor text edit, add ICNRG notice	(same updates)
1.0 Intro	(1) Cite RFC 7927 as context (2) Cite Jacobson CCNx 0.x CONEXT paper (3) Cite CICN and CCN Lite as implementations (4) cite NDN (5) Explain NDN/CCNx 1.0 difference as primarily network layer discovery (6) Cite [selectors] draft as example of ULP doing discovery in CCNx 1.0 (7) Add para on ICNRG consensus & that this is experimental protocol (8) Add 4 para w/ high-level walk through of protocol operation	(1) Add quick background on protocol, cite [semantics] (2) Cite RFC 7927 (3) Add para on 2+2 TLV choice (4) Cite our work on header compression as alternate encoding. (5) Add para con ICNRG consensus & exp. protocol.
1.2 Architecture	Add new section with overview of how a typical network looks.	
1.3 Protocol Overview	Re-write as per IRSG comments	

(continued)

Technical Changes (continued)

Section	Semantics	Messages
12 Security Considerations	Completely rewritten (1) Draft is for a layer 3 protocol w/ authentication (not encryption) (2) Usage guidelines on MICs, MACs, Sigs, especially in Interests (3) Does not include how to arrive at keys or trust keys. CCNxKE cited. (4) Discuss [ccnxke] and [esic] for encryption via encapsulation for tunnels (5) Mention broadcast or proxy re-encryption for sharing (6) Discuss encoding (TLV) issues of aliases, schema validation, and efficiency due to per-hop processing. (7) Extended discussion on caching, cache poisoning, and motivation for our rules on cache behavior. (8) Discuss our approach to hash agility. (9) Discuss that name is pure binary matching, so there are case and non-printable phishing attacks if URI normalization or routing protocols admit such things. (10) Referenced to RFC 7927 and 7945 for more background	(same security considerations section with appropriate updates to citations to Semantics document)

Unresolved Issues & Further Discussion

1. Please read the updated Introduction of Semantics.
    1. Suggest other citations
    2. Feedback on the text
    3. Is the NDN comparison appropriate and sufficient? I tried to nail it down to the core difference at layer 3 without getting in to too many weeds.
2. Please read the Security Considerations
    1. Other citations
    2. Feedback on text
    3. Is there any other significant security consideration I missed (for either semantics or messages)?

Future Plans

- Please provide -07 draft feedback, such as on the icnrg mailing list.
- Based on feedback, we will re-submit to IRSG or do an -08 draft.
    - Please provide feedback by Friday April 6. If you need more time, let me know.
    - At that point, we’ll move to re-submit or -08.