CCNx Technical Working Group

Meeting Minutes

10/28/15

Overview

Attendees: Jim Gibson, Ilya Moiseenko, Christian Tschudin, Cedric Westphal, Christopher Wood

Scribe: Christopher Wood

Agenda

1. Quickly review the changes to the discovery document.
2. Assess the Manifest requirements document.
3. Discuss what's missing from the IP security and privacy document. Identify volunteers who can help work on the current version.

Related Material

- CCNx End-host Forwarder Discovery (draft-wood-icnrg-ccnxdiscovery.txt) [this was the bootstrapping document]
- CCNx Manifest Requirements (draft-wood-icnrg-ccnxmanifestreqs.txt)
- IP-Based Security and Privacy Practices (draft-wood-icnrg-ipprivacylandscape.txt)

1) Review changes to the discovery document

- No comments. Will proceed with the current version.

2) Assess the Manifest requirements document

- The motivation for some of the functional requirements was still insufficient.
    - e.g., why is chunking disallowed?
- There is uncertainty about whether these requirements will also be used for future versions or incarnations of the Manifest.
    - Should a "streaming Manifest" also adhere to these requirements?

    - This is unclear, since Ilya's embedding scheme could be applied on top of the static Manifest to enable streaming.
        - The requirements (or design) don't preclude the sequence number-based naming scheme to be applied.
- Should pointers in the body be encrypted?
    - Yes, if we care about privacy.
    - Implication: (untrusted) forwarders can't use encrypted Manifests.
- Concern about the packet type vs message type (R1). Should a Manifest be a type of Content Object or a new message altogether?
    - Treating it as a Content Object makes the parsing simpler (no new states in the parser).
    - Creating a new message may set a dangerous precedent where any new entity is treated as a new message.
        - Response: Manifests that do not carry application data are very distinct from Content Objects, which are vehicles for application data, so a new message type seems alright.
- Requirement R6 has a typo (the second "Manifests" should be "Messages").
- Why is the desire to amortize the cost of signatures not listed as a requirement?
    - Response: That's an error. It probably should be.
- Why are collections of Content Objects not considered in the requirements?
    - Response: The desire was to start small with the static and finite data case.
    - Outcome: Let's handle directories next.
- Requirement R7 ("additional location information") is confusing and could benefit from some examples.
    - e.g., Pointers should be allowed to specify separate "namespace anchors" (locations) for content.
- What happened to metadata?
    - Response: It was pulled out of the Manifest as the expectation is to treat it as new TLVs that can just be added to any CCNx message.
- Should we encode all types of metadata (e.g., application-specific and network-related) the same way?
    - e.g., a metadata field that indicates the "end of a stream" might be useful network metadata but not application-specific.
- (Requirement R8) Why bother saying that Manifests should be loop-free since consumers will perform loop detection anyway?
    - Response: It should be illegal for a producer to create a Manifest that contains loops. We want to limit the burden on consumers parsing Manifests.
    - Implication: We would need to specify the consumer action(s) to take if a loop is detected.
    - Note: We aren't specifying *how* loops are prevented (e.g., via hash-based LINKs). We are only requiring that they do not exist.
- How long should Manifests be expected to live?
    - Group: Their lifetime should be bounded by the data they point to. A Manifest should not outlive the data to which it contains or represents.
- Should the illegality of "broken links" or "non-existent data" be listed as a requirement?
    - Response: Probably not if we specify the lifetime of Manifests.

3) Discuss the IP security and privacy document

- In the "Session Layer" section, the usage of ephemeral keys is a mechanism (i.e., the **how**) to achieve forward secrecy (i.e., the **what**).

Action Items

- Update the Manifest requirements document based on the group discussion and feedback. [Chris]
- Prepare the updated CCNx Manifest design document. [Chris]
- Finalize and distribute the TLV-based metadata specification. [Chris]
- Update and distribute the Manifest use case document. [Chris, time pending]

Next Meeting

Date & Time: 11/11/15 at 11am PST

Tentative agenda:

- IETF 94 recap.
- Discuss the updated static Manifest requirements.
- Review the Manifest use case document.
- Assess the CCNx metadata proposal.