# CCNx Technical Working Group

## Meeting Minutes

12/23/15

# Overview

**Attendees:** Jim Gibson, Dirk Kutscher, Ilya Moiseenko, Greg Rutz, Greg White, Nacho Solis, Mark Stapp, Christian Tschudin, Christopher Wood

**Scribe:** Christopher Wood

# Agenda

1. Give a status update on the CCNx and ccn-lite FLIC implementations.
2. Revisit CCNx nameless objects for clarification.
3. Discuss the manifest security problem raised during the last meeting.
4. Identify tasks that need to be complete before the Paris interim meeting.

# Related Material

- FLIC specification (https://github.com/tschudin/icn-flic-rfc/blob/master/draft-tschudin-icnrg-flic-00.txt)
- CCNx Semantics (https://www.ietf.org/id/draft-irtf-icnrg-ccnxsemantics-00.txt)
- CCNx Messages in TLV Format (https://www.ietf.org/id/draft-irtf-icnrg-ccnxmessages-00.txt)

## 1) FLIC Status Update

- Revisited (minor) ISO and FLIC differences:
    - In ISO: data sizes per pointer.
        - This is useful for amending data (e.g., inserting a byte in the middle of a manifest).
    - In ISO: relative and absolute names are supported.
        - This has implications on nameless and “nameful” objects.
    - Everything else is functionally equivalent.
- We could (should?) test the formats with different data types (streaming video, images, etc.) to see how one format might be better than the other.

    - Differences are small, i.e., they are about saving some bytes here and there.
- Should 2+2 TLV encoding be used for everything? Should we seek for different encodings for different types?
    - Maybe it's not time for this discussion.
    - We should spend time evaluating upper-level use cases (not encoding problems).

## 2) Nameless Objects

- Is the interest name (for a nameless object) used when indexing into the cache?
    - PIT still stores the name (unless you're out of space).
    - Cache is indexed by the hash (assumes an index over the cache that works via hash).
- Protocol updates: header field that includes the hash
    - The field specifies the hash type and the actual payload.
    - Some nodes may compute the hash while others (maybe in the core) may not.
- How is hash agility handled? What if two interests for the same data are issued with with different hash restrictions?
    - They would specify the type of hash (if we supported more than one -- currently we only support SHA256), and the right hash function would be invoked to do the match.
- Root manifest must be named and all children must be nameless.
    - The NDN implementation required some workarounds because nameless objects are not yet supported (see ccn-lite FLIC code for more details).
        - This is the "nameful" mode of the FLIC.
        - The implicit digest covers the name and payload.
    - Sending an interest with a non-complete name you will get the content object whose implicit digest has the "smallest" value.
- For Paris, we should include ideas about security and transitive trust that come with manifests and nameless objects.
- There are three moving parts that all play together: nameless objects, asking by hash value, and manifests.
- If a content object has a name then it *must* match the name of the interest.
- Interest with content object hash will not match a content object with the same computed hash but a *different name*.
    - Scenario:
        - Adv 1 publishes content with /NYT and hash H=1, hosted at /adv1
        - Adv 2 requests content with H=1 and locator (name) /adv1
        - Victim requests /NYT and gets the poisoned content
    - Solution: Enforce the above rule.
    - MarkS: Can't this also be solved by privacy? (No caching, no name collisions, etc.)
        - Answer: Yes.

# Action Items

- Finish CCNx FLIC implementation for January interop test. [Chris]
- Prepare manifest and nameless object security and trust material for the interim meeting. [Chris]
- Collect and organize interop specification documents and drafts to discuss at the interim meeting. [Chris]

# Next Meeting

**Date & Time:** 1/6/16 at 11am PST

**Tentative agenda:**

- Security and trust issues of manifests and nameless objects.
- Name privacy.