

File-Like ICN Collections (FLIC)

draft-irtf-icnrg-flic-06

IETF 121, Dublin

Marc Mosko

Dave Oran

Network Systems Research & Design

Outline

- What FLIC does (super quick recap)
- Updates since -05
- Implementation Status

What FLIC does

- It provides a manifest of hashes that make up all the segments of a piece of application data.
- The manifest is hierarchical – that is the hash pointers can point to application data or to more manifests.
- There is a canonical traversal order. Metadata could provide other traversal hints, such as for video.
- FLIC has its own, extensible, encryption mechanism. Manifest encryption does not need to be related to content encryption.
- FLIC has several Interest construction techniques. The publisher can choose one or more of these naming techniques. More techniques could be added.

Name Constructors

- Hashed Schema
 - The CCNx implementation uses nameless objects for one way of saving the manifest and data. The HashedSchema was defined in the text, but not in the ABNF.
 - Added to the ABNF.

ABNF

- ABNF for Vendor TLVs
 - The PEN was not defined in the ABNF.
 - Added IANA PEN definition.

Salt for AES Nonce

- Using salt with nonce
 - RFCs 5288 and 6655 recommend using a 4-byte salt plus an 8-byte nonce for AES IVs.
 - We updated FLIC to recommend using a pre-shared 4-byte salt with pre-shared symmetric keys.
 - We added a 4-byte salt field to the RSA-OAEP wrapped group key.
 - NOTE: -06 has an error in that the ABNF should be “4OCTET” not “4*OCTET” for the salt.

StartSegmentId

- In the ABNF field definitions list, the description of StartSegmentId was truncated. We filled in the description.

Implementation Status

- We are in the process of updating the ccnpv [1] implementation to the -06 level.
- The previous implementation only used HashedSchema and did not implement name constructors.
- Our reference forwarder is Cefore [2]. Cefore does not support nameless objects and will only work with the SegmentedSchema name constructor.

[1] <https://github.com/mmosko/ccnpv>

[2] <https://github.com/cefore/>

Next Steps

- Possible next steps
 - Implement FLIC natively in Cefore.
 - Implement nameless objects in Cefore.
- SegmentedSchema uses chunked data names. We have re-introduced a draft on chunking data.

Conclusion

- Finalizing FLIC should be soon. Implementing the -06 draft is, in our opinion, the final step to make sure the draft is workable.
- We do not foresee any major changes, just minor fixed based on the implementation.

Q&A