CCNx Technical Working Group

Meeting Minutes

1/6/16

Overview

Attendees: Dirk Kutscher, Dave Oran, Ravi Ravindran, Nacho Solis, Mark Stapp, Christian Tschudin, Greg White, Christopher Wood

Scribe: Christopher Wood

Agenda

1. Security, privacy, and trust issues of manifests and nameless objects.
2. Name privacy.
3. Identify last minute tasks that need to be completed 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)
- Some privacy-related papers:
    - Acs, Gergely, et al. "Cache privacy in named-data networking." *2013 IEEE 33rd International Conference on Distributed Computing Systems (ICDCS)*. IEEE, 2013.
    - Chaabane, Abdelberi, et al. "Privacy in content-oriented networking: Threats and countermeasures." *ACM SIGCOMM Computer Communication Review.* Vol. 43 No. 3. ACM, 2013.
    - DiBenedetto, Steven, et al. "ANDaNA: Anonymous Named Data Networking Application."
    - Ion, Mihaela, Jianqing Zhang, and Eve M. Schooler. "Toward content-centric privacy in ICN: attribute-based encryption and routing." *ACM SIGCOMM Computer Communication Review*. Vol. 43. No. 4. ACM, 2013.

1) Security, Privacy, and Trust

- Manifests require channels because observers can just view interests issued from the body of a manifest.
    - Manifest fetching reveals names over a path that might along a different path from the one along which the manifest was fetched.
- Ephemeral communication is needed and that has implications on forwarders (no caching, for example).
    - Encryption might mean there are no nameless objects at all.
- Do forwarders need to parse the body of a manifest? (Either by cleartext or using something like mcTLS.)
- Trusted proxies may not have many uses (banking applications won't fly, but video distribution is a good example).
- Trusted proxies may look like CDNs today
    - We can't do better so why bother trying?
    - We shouldn't do worse than this arrangement today
- Opinion: ICN might not be so much about data -- it has other features as well.
    - Sourceless addresses for example are a good driving feature.
- Manifests and their security (along with channels) should be a stack feature as a service.
- Opinion: maybe map hashes to encrypted variants (in a session) so that the hashes are still hidden and only the locator is revealed
    - Hashes are of encrypted content and each consumer gets a different encrypted representation (and therefore a different manifest) → no caching but better privacy.
- Comment: We all must read Stephen's comments on the security and privacy challenges for ICN.
- Manifests are orthogonal to the privacy question. The real question is if the current CDN paradigm is the best and, if not, how can we do better
    - Better might mean better performance, application independence, or equivalent privacy.
- There needs to be more focus (in the community) on the design of CDNs.
- The spectrum of privacy needs to be explored.

Action Items

- Privacy spectrum exploration. [Anyone interested]
- CDN design revisit. [Anyone interested]

Next Meeting

Date & Time: 1/20/16 at 11am PST

Tentative agenda:

- ICN privacy spectrum
- CDNs and ICN
