CCNx Technical Working Group

Meeting Minutes

1/20/16

Overview

Attendees: Jim Gibson, Dirk Kutscher, Ilya Moiseenko, Marc Mosko, Dave Oran, Ravi Ravindran, Greg Rutz, Glenn Scott, Nacho Solis, Mark Stapp, Christian Tschudin, Greg White, Christopher Wood

Scribe: Christopher Wood

Agenda

1. Discuss network- and application-layer manifest use cases.
2. Examine manifest encryption and privacy requirements and their impact on network-level usage (e.g., prefetching).
3. Revisit private object encryption.

1) Manifest Use Cases

- No new comments or insights.

2) Manifest Encryption

- Encrypting *only* the body of a manifest is useless in the presence of an eavesdropper.
- Standard encryption prevents (i.e., excluding protocols like mcTLS) network elements from using manifests.
- Privacy retrieval of manifests necessitates session-based encryption.
- Comment: maybe we can use random names for manifests in conjunction with per-consumer manifest encryption
    - This seems functionally equivalent to session-based encryption but with more overhead.
    - Session encryption enables the same names to be re-used in the context of a given session -- no refactoring or reconstruction is needed.
- What about multi-consumer (1-n) sessions?
    - CCNxKE is point-to-point but looking at extensions might be worthwhile.
- Broadcast encryption has many nice properties when revocation and privacy are not issues.
- We need to provide tools for different scenarios and applications, e.g., CCNx-KE (or something similar) for session encryption, broadcast encryption for other cases, etc.

- We need to affirmatively answer the question about whether completely private communication is needed for all applications and data.

3) Code Release

- CCNx code will be released with tutorials, videos, and possibly a roadmap soon.
- A presentation for the code would be useful but how and where would that take place?
- A "hello world" example that walks people from the code to a compiled application, with some exercises, would be very useful.

Next Meeting

Date & Time: 2/3/16 at 11am PST

Tentative agenda:

- Application models and privacy requirements (a continuation from Paris).
- Manifests and transport protocols.