Queries to CFRG

IETF-97
Friday, November 18, 2016

Kyle Rose <krose@krose.org>

- New protocols

- Tcpcrypt offers session ID as primitive to bootstrap endpoint authentication
  - What properties does this session ID need to have?
  - How to precisely phrase them?
  - Email to cfrg on October 2

- ENO can be used to negotiate different encryption protocols
  - What properties of session IDs do these TEPs need to have in common?
  - Computationally indistinguishable from random? Not really.
  - Unpredictability? Not really that either.
  - For privacy: unlinkability? Sure, what does this imply?
  - Other systems want the same properties
  - Email to cfrg on October 26

- Worry: applications will treat interface (e.g., session ID) as a black box with properties of a single TEP
  - Tcpcrypt may not require session IDs to be secret, but what if a different TEP does?
- Do we want:
  - Explicit enumeration of properties that any TEP's session ID must have?
  - Explicit guidance to application authors of baseline, TEP-agnostic treatment of session IDs?
- Straightforward security properties, but would like more eyeballs