KARP, IETF78
Gregory Lebovitz

BASE DOCUMENTS

- Draft-ietf-karp…
  - -threats-reqs
  - -framework – Bill Atwood
  - -design-guide – Manav Bhatia
- Draft-lebovitz-karp-roadmap
  - Will expire, replaced by above 3

Reduce costs for operators

Feedback from Nanog:

"Clearly, both improving security AND key rollover are important. But ultimately, what operators care about is, er, operations. We do need to keep that as a primary focus as we address the same issues."

- Joel Halpern, 16 Jun 2010

Draft-ietf-karp-threats-reqs-00

- Zero reviews
- Zero comments / discussion
- Who will do the work?

Draft-ietf-karp-design-guide

- RSVP? --- doing RSVP-TE
- Open issues
  - Guidance on how frequently need to rotate keys
  - Why need automated KMP?
    - A: this text already exists in –threats-reqs. –design-guide can reference it. Clean up based upon thread “Why automatic key mangement” 05 Apr
  - 3.2 – clean up text on why to rotate keys and how often
- Needs more review. Who will step up?

Draft-ietf-karp-framework

- Separate automated KMP, or tightly integrated per routing protocol
  - Answer: Separate. Rtr vendors said “No way” on per-protocol keying mechanism.
    - Sam H – analysis 11 May –

      “My preliminary conclusion is that the difference between the out-of-bandand in-band approaches is not as much as I had anticipated.If this conclusion holds, it seems that the political advantages of theout-of-band approach will justify its use here.”
  - Routing Protocol should be oblivious to how the keys given it were created
  - Sam H – be more clear about line between keying goo in RoutingProtocol and goo in KMP

-framework (2/3)

- One to serve both 1:1 and group communications?
  - Some idea reuse from MSEC & 802.1x-2010
  - 1:1 becomes a special case of group keying case
  - Algorithm/mechanism for selection of a KeyServer for the link/domain/area. GDOI-like process for authenticaion to KeyServer, returns group SA.
  - Design team working on it (lunch following this)

… -framework (3/3)

- KeyStore
  - required to allow for migration from manually installed SA’s to KMP installed SA’s.
- Update to show multiple base routing protocols
- Needs more review and concrete input