KARP WG

KARP Design Guidelines
draft-ietf-karp-design-guide-01

Gregory Lebovitz, Juniper
Manav Bhatia, Alcatel-Lucent

IETF 79, Beijing

What's changed?

- 3.1 – Consider Asymmetric Keys
  - Refine text about RSA key size
  - Described Elliptic Curve Cryptography (ECC) for shorter key size
  - Still needed: quick reference to utility of HW Security Module for protecting locally, never-moved key pairs (EKR)

3.2 Cryptographic Keys Life Cycle

- Change keys peridically to…
  - REMOVED: … reduce the store of cipher text that can be used to launch an attack
  - Added: … reduce threat against a long lived key associated due to breaches on systems storing the key, or the users entrusted with the key will be subverted.
- Also noted:
  - In general, physical, procedural, and logical access protection considerations often have more impact on the key life than do algorithm and key size factors.

4.1 Design Team Work Phases

On any particular routing protocol

- We need to first fix the manual key management procedures that currently exists within the routing protocols today and then move to a fully automated key management mechanism.
- Mostly text re-organization. Minor text edits

7.4 Key Management Protocol

- Attempted to better describe the different key management techniques that we could use.
  - Out-of-band external configuration vs. Inter-Peer-on-the-wire
  - "Inband" → "Inline" → "Peer-to-Peer" (today's text)
  - Will change it to: "Inter-Peer"

- KARP goal: Inter-Peer key exchange mechanism.
  - More scalable.
  - Moves away from needing to record keys somewhere permanently.
  - Differentiates in-band vs. out-of-band approach KMP approaches, RELATIVE TO THE RTG PROTOCOL.

Not added to document

- Sam Hartman, May 14-
  - What key setup functions belong to KMP and what functions belong to base routing protcol?
- Answer:
  - Karp-framework:
    - architecture of the target solution, it's piece parts, and the boundaries/lines/interactions between them. This is the document that addresses the overall "design" of the system
  - Karp-design-guide:
    - guidance to design teams trying to apply KARP framework to individual routing protocols.
  - Address in Framework document.

What else?

- Fixed many nits
- Tried to cover all comments. Yours missing? Send mail on list, but do so quickly, because…
- Design teams are starting to form and get to work