Operations Model for Router Keying

draft-ietf-karp-ops-model-05.txt

Sam Hartman, Dacheng Zhang,

IETF 86, March. 2013, Orlando, USA

Status

- Draft-ietf-karp-ops-model-05 published with several updates
- Ready for WG last call

Changes: Alignment with Key Table

- In introduction, note that we give recommendation to protocol spec authors about alignment with key table
- Since the key table draft is stable, include specifics rather than general statements
  - Example: refer to direction column

Changes: Operational Practices

- Implement suggestion from last meeting: keys are just another item of sensitive configuration; existing practices apply
- Lean more towards keys can be stored on central server than other options in sidr-rtr-keying per Russ's comment
- Emphasize higher security practices can be adopted

Subsections for Preshared Keys

- Add sections that commonly get referred to in other documents for easier references:
- Sharing Keys and Zones of Trust
- Key Separation and Protocol Design

Changes: Uncategorized

- Give specific recommendation for VRFs:
  - One key table per VRF
- Discuss randomness of keys especially for group key (thanks Russ)
- Discuss upgrade to AKM for group key management

Open Issues

- Section 3.2: First paragraph is unclear about why management efficiency is important
- Section 4: Rephrase sentence about DH value absent passive attackers
- Easy to fix!

Questions or Comments?