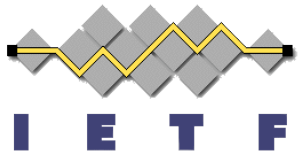
KARP
Design Guide

Draft-ietf-karp-design-guide-00

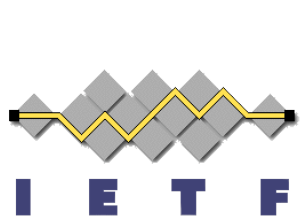


IETF77 Anaheim

Mon, 22 Mar, 2010

Manav Bhatia, Alcatel/Lucent, manav.bhatia@alcatel-lucent.com
Gregory M. Lebovitz, Juniper, gregory.ietf@gmail.com

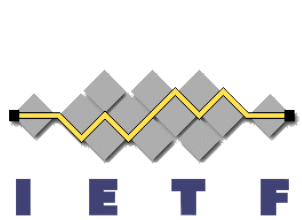
Intellectual Property



- When starting a presentation you MUST say if:
  - There is IPR associated with your draft
  - The restrictions listed in section 5 of RFC 3978/4748 apply to your draft

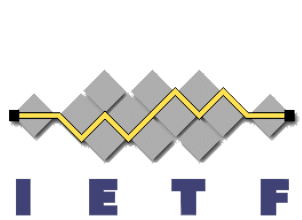
- No IPR that I know of on this document. No restrictions.

Intro



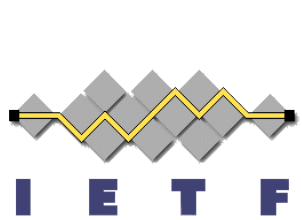
- Should point to the scope, goals, non-goals, audience in -karp-threats-reqs

Categorization



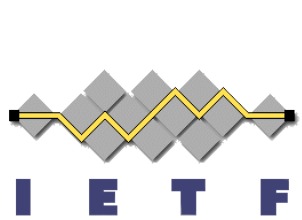
- Communication model
  - One-to-One, e.g. BGP, LDP
    - OSPF & IS-IS in Pt-2-Pt mode may fall here too
  - One-to-Many, e.g. OSPF, IS-IS in BMA modes; RIP
  - Multicast, e.g. PIM
- Keying Model
  - Peer Keying
  - Group Keying

We'll employ a 2 step program



- Step 1 (Sect 4.1, #1)
  - Enhance existing Routing Protocol's current authentication mechanism(s).
    - Usually manual key or OOB management mechanism
    - Strong algorithms, Algo agility, secure use of simple PSKs, Replay protection, mid-session key agility, etc.
    - Get ready for a KMP, or at least don't do anything that would prevent using one.

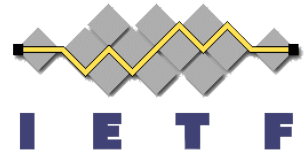
Step 2 of 2 (Sect 4.1, #2)



- Introduce a KMP for operational efficiency gains
  - Use a common Framework for multiple routing protocols

- 2 Step Example: TCP-AO
  - First update manual key mode. Once done…
  - … Introduce a KMP to provide those keys.

But why do we need a KMP?



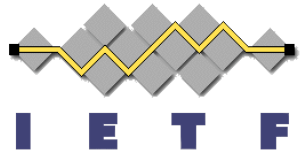
- To address brute force attacks [RFC3562] recommends:
  - frequent key rotation,
  - limited key sharing,
  - key length restrictions, etc.

- Advances in computational power make that management burden untenable for MD5 implementations in today's routing
- Keys must be of a size and composition that makes configuration and maintenance difficult or keys must be rotated with an unreasonable frequency.
- KMPs help A LOT,

  IF

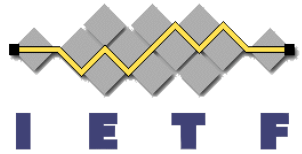
  you can make them operationally usable

Categorizations: Look good?



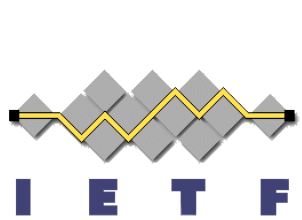
- Re-use as much as possible from common framework
- But not all Routing Protos created equally. Will be uniquenesses for each “grouping”:
  - PIM-SM & -DM
  - BFD – special considerations
  - BGP/LDP/MSDP
  - OSPF/ISIS/RIP – group keying, one-to-many msg
  - RSVP, RSVP-TE
- Dropped the priorities. Add back?

Q: Too much repitition in s6, Gap Analysis?



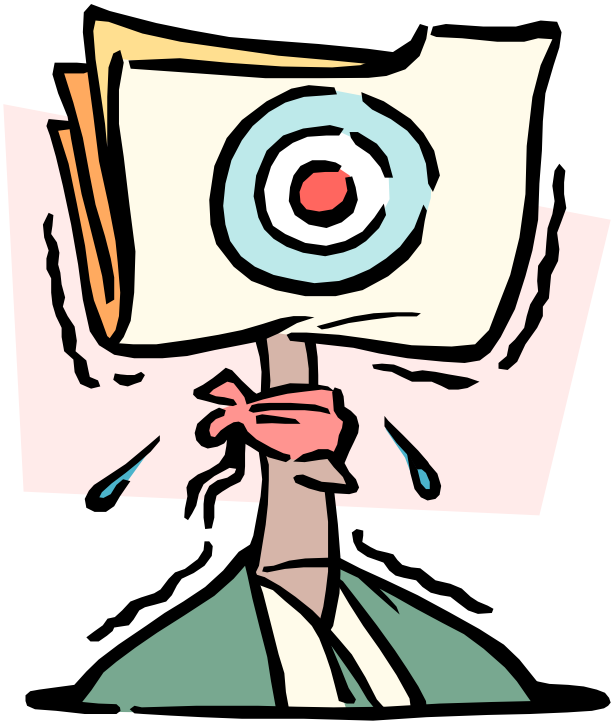
- Seems to have a lot of text that is already in karp-threat-reqs requirements section.
- Suggest sync these two better and cut redundancy. S6 might not be needed at all, just add small bits to work plan section.

Security Considerations, s7



- Use Strong keys – aimed at operators
  - From 3562:
    - (1) key lengths SHOULD be between 12 and 24 bytes (this will vary depending on the MAC/KDF in use),
    - (2) key sharing SHOULD be limited so that keys aren't shared among multiple peering arrangements, and
    - (3) Keys SHOULD be changed at least every 90 days (this could be longer for stronger MAC algorithms, but it is generally a wise idea).
- Internal vs External (to domain of control) operation
- Unique vs. Shared Keys
- OOB vs In-line key management

Feedback?



draft-ietf-karp-design-guide-00